CSC | Computer Science and Communications

UNIVERSITY OF LUXEMBOURG

FACULTY OF SCIENCE, TECHNOLOGY AND COMMUNICATION

Computer Science and Communications

Activity Report 2017

CSC | Computer Science and Communications

Computer Science and Communications

Activity Report 2017

Keywords:
Activity Report, University of Luxembourg, Computer Science and Communications, UL, CSC

Computer Science and Communications
Activity Report 2017

Address:

Computer Science & Communications (CSC)
University of Luxembourg
Faculty of Science, Technology and Communication
6, avenue de la Fonte
L-4364 Esch-sur-Alzette
Luxembourg

Administrative Contact:

Danièle Flammang, Isabelle Glemot-Schroeder, Fabienne Schmitz and Nicola Wolters
Email: csc@uni.lu

http://csc.uni.lu

Editor: Christian Glodt
Release date: 2018-06-14
Note: This report was created using LaTeX with a template based on previous work by Sebastien Varrette.

Preface

Dear reader,

This annual report synthesizes the progress and activities of the Computer Science & Communications (CSC) Department in 2017, including our research projects, organized events, awarded papers, visiting researchers and publications.

In 2017 we welcomed our new colleague Prof. Martin Theobald, and Prof. Raymond Bisdorff retired. Moreover, we moved to our new premises in Belval, and we started a new academic bachelor program in computer science (BICS).

We hope that you will find this report stimulating and inspiring. On behalf of the CSC department, we invite you to contact any one of us if you have any questions regarding the research we conduct in the CSC.

Best regards,

Leon van der Torre
Sjouke Mauw

Contents

Chapter 1

Mission

Our vision and mission phrase our long-term view on the relation between ICT and society and our role in shaping it.

CSC vision: A society in which technology and information are seamlessly integrated and in which advanced communicative, intelligent, and secure software systems provide functionality for the benefit of people and society.

CSC mission: To perform groundbreaking fundamental and applied research in computer science, commonly inspired by industrial and societal challenges.

In practice, a clear-cut distinction between fundamental and applied research is unfeasible or artificial. Very often fundamental and applied research interact within the same research project. CSC supports academic freedom and sees the pursuit of long term scientific goals as an important task.

Computer science is a fast moving area. Agility is therefore crucial and consequently we have set up a structure that can deal with a dynamic environment. The multiple research areas and and interests of CSC professors and researchers offer a broad expertise which is readily available. This allows to cope with the high expectations and challenging demands of the local societal and industrial players, but also to participate in new international research programs. This diversity and agility continue to provide a very solid base for visible and relevant research in a changing world.

Chapter 2

Executive Summary

The Computer Science and Communications Department, also known as CSC (http://csc.uni.lu), includes a staff of more than 152 full-time equivalent members involved in both teaching and research activities.

The scope of the lectures in the study programs includes topics covering fundamental aspects of computer science as well as practical ones. The CSC is responsible for two bachelor programs, two master programs, a doctoral program, and a certificate Smart ICT for business innovation.

The CSC (http://csc.uni.lu) is divided into 4 themes:

- Communicative Systems (http://comsys.uni.lu),
- Intelligent and Adaptive Systems (http://ilias.uni.lu),
- Algorithmics, Cryptography and Security (http://lacs.uni.lu).
- Advanced Software Systems (http://lassy.uni.lu).

Many of CSC faculty staff members, as well as their research groups, are involved in the three interdisciplinary research centers of the university, called SnT, C^2DH and LCSB, thus forging a tighter connection between the computer science department and these research centers.

The CSC is cooperating in a large set of international as well as regional projects.

Head

- Leon van der Torre, professor, head of CSC

Vice head

- Sjouke Mauw, professor, head of LACS, vice head of CSC

Academic Staff

- Alex Biryukov, professor
- Raymond Bisdorff, professor
- Pascal Bouvry, professor
- Lionel Briand, professor
- Jean-Sébastien Coron, associate professor
- Thomas Engel, professor, head of COMSYS
- Dov Gabbay, guest professor
- Nicolas Guelfi, professor
- Pierre Kelsen, professor, head of LASSY
- Franck Leprévost, professor
- Sjouke Mauw, professor, head of LACS, vice head of CSC
- Yves Le Traon, professor
- Volker Müller, associate professor
- Nicolas Navet, associate professor
- Björn Ottersten, professor
- Peter Y. A. Ryan, professor
- Steffen Rothkugel, associate professor
- Jürgen Sachau, professor
- Christoph Schommer, associate professor, head of ILIAS
- Ulrich Sorger, professor
- Bernard Steenis, associate professor
- Leon van der Torre, professor
- Denis Zampunieris, professor

Full list of publications: http://orbilu.uni.lu/simple-search?query=CSC

More information: http://csc.uni.lu

Since CSC counts among its major achievements the continued support of the SnT, please look at the SnT 2017 annual report to get a complementary overview of CSC activities in the area of Security, Reliability and Trust. In particular, we invite you to consult the SnT 2017 annual report for information regarding the activities and contributions of professors Briand and Ottersten and their respective groups.

Chapter 3

Research Areas

History

The University of Luxembourg (UL) was created in 2003 by merging several higher-education institutions, notably the Centre Universitaire (CU) (undergraduate level) and the Institut Supérieur de Technologie (IST) (industrial engineering). Accordingly, computer science was initially split between two faculties, resulting within the FDEF faculty in the Laboratory of Algorithmics, Cryptography and Systems (LACS) and the Applied Mathematics Service, and resulting within the FSTC faculty in the Applied Informatics department (DIA).

In 2003, DIA evolved into the Computer Science and Communications Separtment (CSC) including the Communicative Systems Lab (COMSYS), the Interdisciplinary Lab for Intelligent and Adaptive Systems (ILIAS), and the Lab of Advanced Software Systems (LASSY). In 2006, LACS and the Decision Support chair also joined CSC.

The creation of the academic master in 2005 offered a strategic opportunity to recruit new professors and strengthened the existing laboratories, as reflected by the increasing quantity and quality of publications, modulo variable funding opportunities. Since 2012, the doctoral program offers a systematic framework for doctoral education and research.

ICT being a key technology and national priority, local needs and collaboration with industry have played a major role in the development of CSC and of the associated professional bachelor and academic master. Many PhD/research projects have industrial partners. In 2009, CSC spun-off the Interdisciplinary Centre for Security, Reliability and Trust (SnT), whose purpose was to promote and efficiently handle industrial contracts and administrative challenges. Its theme followed the former UL-priority P1 on 'Security and Reliability of Information Technology'. CSC also collaborates with the LCSB and the C^2DH, and supports the computational science initiative.

Research Program

The research program describes, given the relevant side conditions, on which research priorities we work to contribute to our mission. First of all, our research program identifies the four major research fields that we consider essential for achieving our more generic vision and mission (communication, artificial intelligence, software and security).

- Communication: computer systems become more connected,
- Artificial Intelligence: computer systems are used for more complex tasks,
- Security: we increasingly depend on evasive computer systems operating in a hostile environment,
- Software: computer systems become more complex.

Given side conditions like available expertise, interest, funding opportunities, national interests, expected impact, etc, the department has identified within each of the research fields a number of research priorities. This set of research priorities is intended as an evolving program.

At the moment of writing, an important line is 'Security, Trust, Reliability' that is going across labs, but which also forms the key initial target for the first interdisciplinary center, SnT. Moreover, new interdisciplinary research lines are also bundling and fostering together key forces of CSC, such as systems biomedicine (second interdisciplinary center), and FinTech (national priority). In the upcoming years we will further diversify and improve collaborations with other units, notably LCSB, the third interdisciplinary center on digital humanities called C^2DH, and the faculty priority on computational sciences. Moreover, we will invest in upcoming research areas of interest to such domains, such as machine learning.

The top-down cohesion is visible when CSC defines the research profiles for new positions, that strengthen or complete the topics covered by CSC according to this priority. Instead of a top-down overarching cohesion, we have underlying synergies/cohesion within and between labs/themes coming from shared research interests. Another dimension that should not be neglected is cohesion through the elaboration of consistent teaching programs.

Detailed Research Program

The advancements in information and communication technology (ICT) have revolutionised our lives in a way that was unimaginable a few years ago. Today we use ICT in almost all aspects of our daily life. Embracing the end-to-end approach in system design, we focus on integrated research in the areas of Information Transfer and Communicating Systems (COMSYS). Information transfer is concerned with the transmission of information over potentially complex and insecure channels or networks. Communicating systems are compositions of multiple distributed entities employing communication networks to collaboratively achieve a common goal. The rapidly growing demand for information exchange in people's daily life requires technologies such as ubiquitous and pervasive computing to meet the expectations of the information society. The

demand for secure and privacy-friendly communication is growing fast. Our main research focus in communicative systems is the development of novel adaptive concepts tackling the continuing data and societal challenges and providing robust solutions for secure communication, including reliable realtime transfer in embedded signal processing. The resulting problems have already been a key topic for many industrial and governmental projects at national and European level. Current research projects develop and propagate technologies for:

- Privacy and (cyber) security by distribution: privacy in data communications, network traffic analysis and protection, supervisory control and data acquisition (SCADA), information distribution and topology discovery in untrustworthy networks, wireless networks and mobile security, machine learning for big data analysis, malware detection and IT forensics; Energy conversion and electrical power systems;
- Networking: Internet of Things, Quality of Service, IPv6 integration, software-defined networks, vehicular and multimodal traffic management;
- Human Computer Interaction (HCI): games and novel interface technologies and their application to vehicular communication;
- Financial technologies including smart contracts and blockchain.

The Intelligent and Adaptive Systems Research Group (ILIAS; see ilias.uni.lu) is home to 5 Professors, 6 Guest Professors, 16 PostDoc researchers, as well as to 20 Doctoral students. ILIAS investigates the theoretical foundations and algorithmic realisations of Intelligent Systems for complex problem solving and decision making in uncertain and dynamic environments. Our activities include interdisciplinary research that fits to the rapidly growing role of Artificial Intelligence, Big Data, and Robotics.

The collaboration with the Interdisciplinary Centres SnT, LCSB, and C2DH as well as with the Luxembourg School of Finance (LSF), the involvement with the High Performance Computing facility (HPC), and the collaboration with the Computational Sciences initiative reflect ILIAS's significance for Luxembourg's strategic priorities and future.

The research areas are orthogonal and adhere to the following disciplines:

- Big Data: we investigate scalable architectures for the distributed indexing, querying and analysis of large volumes of data. Specific focus areas include information extraction, probabilistic and temporal database models as well as distributed graph and streaming engines.
- Information Theory and Stochastic Inference: the main research topics here are Signal Processing, Error-Correcting Codes, and Probabilistic Graphical Models.
- Knowledge Discovery and Mining: the research areas include fundaments and applications of Machine Learning including Deep Learning, the use of Natural Language Processing for Big data and texts, and Data/Text Mining.
- Knowledge Representation and Reasoning: we concern ourselves with normative reasoning in Multi-Agent Systems, particularly, Logics for Security and Compliance as well as Machine Ethics, Legal Knowledge Representation, Inference under Uncertainty and Inconsistency, Logic-based models for intelligent Agents and Robots, and Computational Choice.

- Parallel Computing and Optimisation: the research on Parallel Computing and Optimisation Techniques, in particular how different species may co-evolve taking local decisions while ensuring global objectives, tackle large and difficult problems. The main application domains are Security, Trust and Reliability, Reliable Scheduling and Routing on new generations of networks, and Sustainable Development and Systems Biomedicine.

Our outreach activities are manifold, diverse, and interdisciplinary, and span collaborations with other departments. We regularly do presentations at schools and student fairs and cooperate with industry, if our expertise for the society is requested. We motivate young students to work with Robots within the RoboLab or with the Robo-Football Team and prepare them for new upcoming disciplines in Artificial Intelligence, Machine Learning, and beyond. The 2017 ILIAS Distinguished Lecture Series of 12 talks, given by international recognized experts from industry, politics, and science, were followed by more than 400 listeners. Since Q4/2017, we are in close contact to the Luxembourgish Ethics Council concerning the questions to Artificial Intelligence and Ethics.

This proliferation of digital communication and the transition of social interactions into cyberspace have raised new concerns in terms of security and privacy. These issues are interdisciplinary in their essence, drawing on several fields: algorithmic number theory, cryptography, network security, signal processing, software engineering, legal issues, and many more. Our work on Information Security (LACS) focuses on:

- Cryptography:
  - Theoretical foundations: study of cryptographic primitives, cryptanalysis, sidechannel analysis, computational number theory.
  - Applications: digital currencies, public key encryption and signatures.
- System and network security: frameworks and tools to analyse security primitives, protocols and systems, the design of novel security protocols and other security controls, human aspects in security, privacy, e.g., in social networks, voting systems.
- Information security management: the development of a methodology and tools to assess system security and to select appropriate security controls.

Our research on Advanced Software and Systems (LASSY) can be structured into five partly overlapping dimensions: modelling, methodology, computing paradigms, dependability (including security) and main application domains.

- Modelling: we investigate the foundations of model-driven engineering (MDE) as well as applications of MDE in fields as diverse as mobile computing, internet of things and the automotive sector, to name just a few.
- Methodology: a new integrated approach has been developed supported by an open-source tool that integrates theories, methods and tools from several software engineering subdisciplines such as requirements, testing and maintenance.
- Computing paradigms: the topic of pro-active computing, which is based on anticipating the user's needs, is investigated.
- Dependability: several research topics deal with dependability. In particular, innovative software testing and debugging techniques are studied. Another research topic within this dimension is the study of software intensive real-time

systems, trying to improve their safety and lower their development costs. This line of investigation is supported by analytic and simulation models as well as by software engineering concepts such as domain-specific languages and system synthesis. Finally, mobile security and reliability are studied using static code analysis and machine learning techniques.

- Application domains: examples are automotive and aerospace embedded systems, enterprise architectures, cyberphysical systems, e-learning and pervasive healthcare systems.

Chapter 4

Research Groups

4.1 Algorithmic Decision Theory (ADT)

Head of research group: Prof. Dr. Raymond Bisdorff

The ADT group is locally part of the ILIAS laboratory and internationally part of the French CNRS founded research group GDRI-Algodec on *Algorithmic Decision Theory* with active support from the FNR. It focuses on developing new decision aiding tools when facing multiple incommensurable performance criteria and big data.

Summary of the group's achievements in 2017

The year 2017 was mainly devoted to organize and host ADT 2017, the 5th International Conference on *Algorithmic Decision Theory, 25-27* October 2017, see https://sma.uni.lu/adt2017/ . About 60 researchers from 13 countries and four continents attended the conference. Main programme topics were: *Preferences and Multi-Criteria Decision Aiding, Decision Making and Voting, Game Theory and Decision Theory,* and *Allocation and Matching*. The proceedings appeared in the Springer LNAI series. A special thank you goes to the sponsors: CNRS (FR), FNR (LU), FSTC/CSC Research Unit (LU), University of Kentucky (US) who hosted the 4th edition of the ADT Conference in 2015, and the EURO Working Group on *Advances in Preference Handling*. The actual conference was preceded by a one day doctoral consortium event where about a dozen doctoral candidates presented and discussed their doctoral ADT projects with the audience.

Main publications and achievements in 2017

- J, Rothe (Ed.) Algorithmic Decision Theory. 5th International Conference, ADT 2017, Luxembourg, Luxembourg, October 25–27, 2017, Proceedings. LNAI

10576 LNCS Springer ISBN 978-3-319-67503-9.

- **R. Bisdorff**, Algorithmic Decision Theory for solving complex decision problems. Distinguished ILIAS Interdisciplinary Lab for Intelligent and Adaptive Systems Lecture IV, FSTC, University of Luxembourg, 3 May, 2017. Abstract: Today's decision makers in fields ranging from engineering to psychology, from medicine to economics and/or homeland security are faced with remarkable new technologies, huge amounts of information to help them in reaching good decisions, and the ability to share information at unprecedented speeds and quantities. These tools and resources should lead to better decisions. Yet, the tools bring with them daunting new problems: the massive amounts of data available are often incomplete, unreliable and/or distributed and there is great uncertainty in them; interoperating/distributed decision makers and decision making devices need to be coordinated; many sources of data need to be fused into a good decision; information sharing under new cooperation/competition arrangements raises security problems. When faced with such issues, there are few highly efficient algorithms available to support decision makers. The objective of Algorithmic Decision Theory (ADT) is to improve the ability of decision makers to perform well when facing these new challenges and problems through the use of methods from theoretical computer science, in particular algorithmic methods. The primary goal of ADT is hence to explore and develop algorithmic approaches for solving decision problems arising in a variety of applications areas. This presentation was more specifically focused on multiple criteria decision aiding methodology, the actual research field of the author.

4.2 Applied Crypto Group (ACG)

Head of research group: Prof. Dr. Jean-Sebastien Coron

The Applied Crypto Group (ACG) is doing research in cryptography, within the Computer Science and Communications (CSC) research unit of the University of Luxembourg.

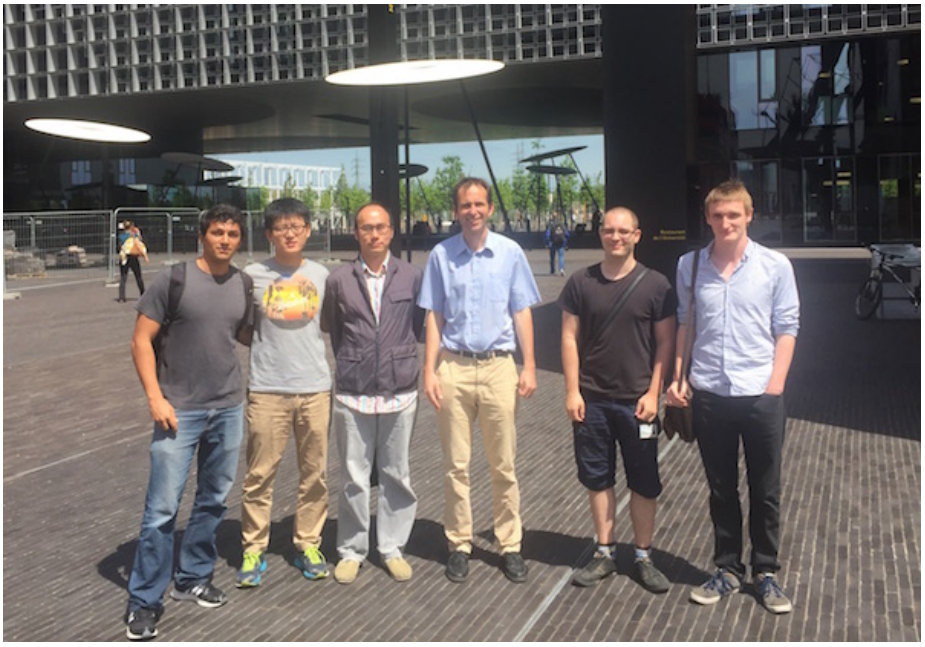
Summary of the group's achievements in 2017

New attack found against a multilinear map cryptographic scheme. The paper has appeared at the PKC 2017 conference. Jean-Sebastien Coron was program co-chair of the EUROCRYPT 2017 conference, one of the two most important conferences in cryptography.

Main publications in 2017

- **Jean-Sébastien Coron**, **Moon Sung Lee**, Tancrède Lepoint, Mehdi Tibouchi: Zeroizing Attacks on Indistinguishability Obfuscation over CLT13. Public Key Cryptography (1) 2017: 41-58. The paper describes a new attack against a multilinear map cryptographic scheme

- **Jean-Sébastien Coron**: High-Order Conversion from Boolean to Arithmetic Masking. CHES 2017: 93-114. The paper describes a more efficient conversion algorithm from Boolean to Arithmetic masking.



4.3 Applied Security and Information Assurance (APSIA)

Head of research group: Prof. Dr. Peter Y A Ryan

The APSIA group is part of the SnT and has strong connections to CSC and the LACS laboratory. The group specializes in the design and analysis of security and privacy mechanisms and protocols. Of particular interest: secure, verifiable voting protocols, authenticated key establishment protocols, both classical and quantum, and including password-based and out of band-based. APSIA has also ventured and developed an interdisciplinary approach to research in security and trust. It collaborates regularly with researchers from various groups and institutions of the University, such as, the experimental soft matter physics (EMPS) of the Physics and Materials Science research unit; the cognitive science and assessment (COSA) of the Education, Culture, Cognition and Society research unit; the research unit in Law (RUL); and the Luxembourg Centre for Systems Biomedicine (LCSB).

APSIA has established a dedicated laboratory to follow these variegate activities: the *laboratory of Interdisciplinary Research in Socio-Technical Cybersecurity* (IRiSC lab, https://wwwfr.uni.lu/snt/research/apsia/irisc_lab).

Summary of the group's achievements in 2017

2017 was a fruitful year for APSIA: three new CORE and Junior-CORE proposals were awarded, as well as an H2020 project FutureTPM. The group grew to around twenty members and is set to grow further in 2018. Two members successfully defended their PhD theses were retained as post-docs. Overall the group published over 40 papers, many in highly prestigious conferences such as Crypto. In addition, the group's output included two edited volumes and a special issue of IEEE Security and Privacy. The Verifiable Voting Workshop in association with Financial Crypto, founded by Ryan in 2016, had its second edition in Malta. The Int. Workshop Socio-Technical Aspects in Security and Trust (STAST) held its 7th edition, hosted by the ACM ACSAC in Orlando, Florida. We have a number of international projects with Poland, Belgium and France, mainly around secure voting systems, and we held a very fruitful workshop in the autumn to bring these collaborations together. Ryan spent a month at the ENS Paris as a Visiting Professor. We also established a sub-group of four members working on quantum information assurance that will be funded by one of the CORE projects just awarded.

Courses taught: Information Security Basics, Security Modelling, Principles of Security Engineering and Theoretical Foundation of Computing. Also contributed to the supervision and evaluation of projects in the new BICS.

The group continues to run the internal "breakfast" talks as well contributing to the SRMs, the joint SATOSS/APSIA seminars: 35 talks featuring speakers from 13 different countries.

Three most interesting publications in 2017

- W. Roscoe, **Peter Y. A. Ryan**: Auditable PAKEs: Approaching Fair Exchange Without a TTP. Security Protocols Workshop2017: Springer LNCS 10576, 278-297. This paper extends Roscoe's notion of "auditability", the ability to distinguish between active attack and network failure, to Password –based Authenticated Key Establishment protocols. This motivated the introduction of a novel flavor of fair exchange: stochastic fair exchange, which is of interest in its own right.
- Zhe Liu, Patrick Longa, Geovandro Pereira, Oscar Reparaz, and Hwajeong Seo: FourQ on Embedded Devices with Strong Countermeasures Against Side-Channel Attacks. In IACR Conference on Cryptographic Hardware and Embedded Systems - CHES 2017. This work presents the state-of-the-art implementation results of elliptic curve scalar multiplication and elliptic curve Diffie-Hellman (ECDH) key exchange on 8, 16 and 32-bit embedded devices using FourQ. We present, to the best of our knowledge, the first publicly-available design and an energy-efficient, high-speed and high-security implementation of elliptic curve-based system that includes defenses against a wide variety of passive attacks. These results demonstrate the potential of deploying FourQ on low-power applications such as protocols for IoT.
- Security in the Shell : An Optical Physical Unclonable Function made of Shells of Cholesteric Liquid Crystals, Lenzini, Gabriele; Samir, Ouchani; Roenne, Peter; **Ryan, Peter**; Geng, Yong; Noh, Junghyun; Lagerwall, Jan in *Proc. of the*

9th IEEE Workshop on Information Forensics and Security (2017, October 02). We define fundamental security properties for physical unclonable functions to be used e.g. in authentication of products, and show that the tags created of shells of Cholesteric Liquid Crystals, recently created by our collaborators from the physics department at the university, fulfill the basic requirement, paving the way for their use in anti-counterfeiting, secure packaging and beyond.

4.4 BigData, Data Science & Databases (BigData)

Head of research group: Prof. Dr. Martin Theobald

The BigData group at the University of Luxembourg is a new research group that has been established in February 2017. The group is headed by Martin Theobald, who previously held positions at the Max-Planck-Institute in Saarbruecken, at the University of Antwerp, and at Ulm University. The group currently consists of one PhD student at the University of Luxembourg, Amal Tawakuli, and one more, jointly supervised PhD student, Maarten Van den Heuvel, at the University of Antwerp. We currently have three open positions, one PhD and two PostDoc positions, which are intended to become filled in early 2018.

Our research activities focus on three main areas:

1. Information Extraction & Knowledge-Base Construction: In collaboration with the Max-Planck-Institute in Saarbrücken, we investigate the full NLP pipeline for information extraction from natural-language sources, including probabilistic-graphical models for named-entity recognition and disambiguation, relation extraction, and knowledge-base construction. We will further intensify our collaboration in the context of a new FNR-CORE project, which recently received funding at the University of Luxembourg, and for which the Max-Planck-Institute kindly serves as external collaborator. Two PhD theses at the Max-Planck-Institute have been defended in 2017 based on this collaboration.

2. Probabilistic & Temporal Databases: A second research focus lies in the development of probabilistic and temporal database models and systems. The team was involved in the development of the Trio probabilistic database system at Stanford University, which was the first principled approach to couple data uncertainty with relational data by using SQL as a query language. Further ongoing research activities (in collaboration with the University of Zurich) are in the context of temporal database models that now also fully support the afore-described probabilistic extensions. One PhD thesis will be defended at the University of Zurich in early 2018 based on this collaboration.

3. Distributed Graph Databases: We recently developed the TriAD distributed graph engine, which is one of the fastest currently available engines for

RDF data and SPARQL queries. TriAD is purely based on in-memory index structures and implements its own custom communication protocol, based on asynchronous message passing, that outperforms MapReduce-based protocols by several orders of magnitude. Recent extensions of TriAD also support more general graph-pattern queries, including the new SPARQL 1.1 specification. We currently investigate the implementation of new streaming extensions based on this architecture.

Our teaching activities focus on Databases, Data Science and Big Data Analytics: We intensively employed the recent Big Data platforms, such as the Apache Hadoop/Pig/HIVE/ HBase software stack, Spark, Giraph, GraphX, as well as MongoDB, for teaching and application development. In particular Spark offers a wealth of constantly updated Machine Learning libraries (MLlib), which we applied to a variety of data collections in the context of different student projects. Two new modules for the MiCS program, namely "Big Data Analytics" and "Advanced Database Topics", will be offered in 2018. In addition, we organize three new modules, "Information Management I-III", in the newly established BiCS program of the University.

Main publications and achievements in 2017

- Dat Ba Nguyen, Abdalghani Abujabal, Khanh Tran, **Martin Theobald**, Gerhard Weikum: Query-Driven On-The-Fly Knowledge Base Construction. PVLDB 11(1): 66-79 (2017)
- Dat Ba Nguyen, **Martin Theobald**, Gerhard Weikum: J-REED: Joint Relation Extraction and Entity Disambiguation. CIKM 2017: 2227-2230
- Rohan Nanda, Giovanni Siragusa, Luigi Di Caro, **Martin Theobald**, Guido Boella, Livio Robaldo, Francesco Costamagna: Concept Recognition in European and National Law. JURIX 2017: 193-198

PhD Defenses in 2017

- Dat Ba Nguyen (Max-Planck-Institute for Informatics/Saarland University): "Joint Models for Information and Knowledge Extraction", Feb. 2017
- Sairam Gurajada (Max-Planck-Institute for Informatics/Saarland University): "Distributed Indexing and Querying of Large, Labeled Graphs", Dec. 2017

4.5 Collaborative and Socio-Technical Systems (COaST)

Head of research group: Assoc.-Prof. Dr. Steffen Rothkugel

As part of the Communicative Systems Laboratory (Com.Sys), the COaST group focuses on distributed collaborative systems, complex networks and self-organization, socio-technical modelling, educational technologies, as well as augmented and virtual reality.

Summary of the group's achievements in 2017

The COaST group counted 5 members (1 professor, 1 senior researcher, 3 PhD students) and 11 publications in 2017. The group's research in the context of the ongoing projects CoCoDA[2], CollaTrEx and Yactul, was published in renowned journals and presented at various international conferences, inclusive of a keynote talk and winning a best paper award. The active and continuous learning environment project Yactul was also awarded the FSTC Teaching and Learning Innovation Grant. Members of the group furthermore received an FHEA fellowship and organized various international scientific events and conferences such as IEEE SASO 2017 and SASOST 2017. The COaST group's teaching activities comprised numerous lectures and seminars in the different bachelor and master programs (BINFO, MICS, BINFO-FC) offered by the University of Luxembourg, as well as guest lecturing abroad. Benjamin Behringer successfully defended his PhD thesis.

Main publications and achievements in 2017

- **Christian Grévisse, Jean Botev, Steffen Rothkugel.** An Extensible and Lightweight Modular Ontology for Programming Education. In Proc. 12th Colombian Conference on Computing, pp.358-371, 2017. Best Paper Award.
  This paper discusses a modular ontology for programming education. Its main purpose is to integrate annotated learning material into Eclipse or other IDEs. The ontology is based on a modular architecture, which is extensible with respect to different programming languages. By aligning language-specific concepts with user-specific tags learning resources for code elements can be suggested in a fine-grained and cross-curricular way. The example implementation establishes relations between learning aspects in Java or C code and related, annotated resources such as articles on online question-and-answer sites.
- Kirstie Bellman, **Jean Botev,** Hanno Hildmann, Peter R. Lewis, Stephen Marsh, Jeremy Pitt, Ingo Scholtes, Sven Tomforde. Socially-Sensitive Systems Design: Exploring Social Potential. In IEEE Technology and Society Magazine, Vol.36, No.3, 2017.
  This article introduces the socially-sensitive systems design framework based on the three core tenets of social organization, social values, and social relations. Explicitly designing these into technical systems allows for better positioning through increased social potential and robustness while exhibiting fewer social pathologies.
- **Johannes Klein, Jean Botev, Steffen Rothkugel.** Concurrency-Based and User-Centric Collaboration for Distributed Compound Document Authoring. In Proc. 21st IEEE International Conference on Computer Supported Cooperative Work in Design, pp.168-173, 2017.
  This paper discusses dedicated data representation and concurrency models for command distribution and application in the collaborative authoring

of complex compound documents. Beyond file-based abstractions, the tight integration of a fine-grained data structure with a highly scalable, priority-based concurrency model helps reducing workflow restrictions and provides increased responsiveness and system-level support users.

4.6 Communication and Information Theory (Cain)

Head of research group: Prof. Dr. Ulrich Sorger

The Cain group is a small research group both in the ILIAS, and the ComSys laboratories. It is a part of the SECAN-Lab, too. There are frequent collaborations and exchanges with researchers from other groups like Bouvry's Parallel Computing and Optimisation Group (PCOG), Engel's Security and Networking Lab (SECAN-Lab), or Biryukov's cryptology research group (CryptoLUX). The group is currently composed of three people; besides the head there is Christian Franck who joined in 2015 as a research scientist and Andrea Capponi who joined in 2016 as a PhD candidate. Our plan is to further grow the group by one or two additional PhD students. The core expertise of the group are mathematical principles behind the efficient encoding of information and the realisation of reliable error-free digital communication systems.

Main publications and achievements in 2017

- C. Fiandrino, **A. Capponi**, G. Cacciatore, D. Kliazovich, **U. Sorger, P. Bouvry**, B. Kantarci, F. Granelli and S. Giordano (Feb 2017), "CrowdSenSim: a Simulation Platform for Mobile Crowdsensing in Realistic Urban Environments" in IEEE ACCESS, 5, pp. 3490-3503. ISSN: 2169-3536, DOI: 10.1109/ACCESS.2017.2671678
- **A. Capponi**, C. Fiandrino, D. Kliazovich, **P. Bouvry** and S. Giordano (Mar 2017), "A Cost-Effective Distributed Framework for Data Collection in Cloud-based Mobile Crowd Sensing Architectures" in IEEE Transactions on Sustainable Computing, 2 (1), pp. 3-16. ISSN: 2377-3782, DOI: 10.1109/TSUSC.2017.2666043
- **C. Franck, J. Großschädl**, "Efficient Implementation of Pedersen Commitments Using Twisted Edwards Curves", Third International Conference on Mobile, Secure, and Programmable Networking (MSPN), 2017

4.7 Critical and Extreme Security and Dependability (CritiX)

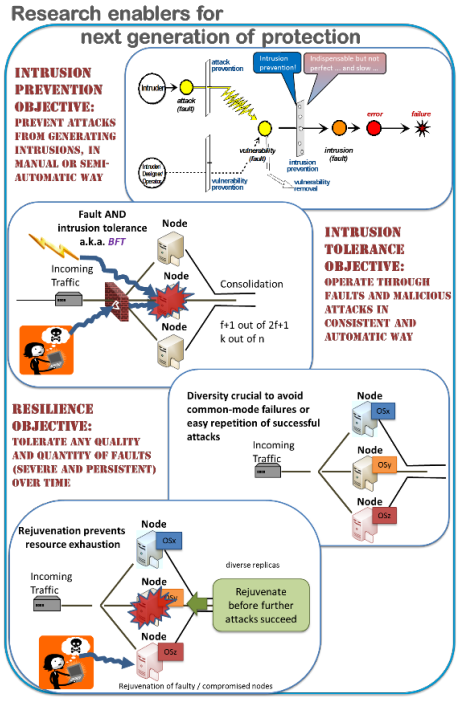
Head of research group: Prof. Dr. Paulo Esteves-Veríssimo

The CritiX lab (https://wwwen.uni.lu/snt/research/critix) was set up in September 2014 at SnT, and its main research activities have reached cruise speed. The group intends to investigate and develop paradigms and techniques for defeating extreme adversary power and sustaining perpetual and unattended opera-

tion, and focusses on four scientific priorities, focal points of the PEARL programme: Resilience of cyber-physical system infrastructures and control; Internet and cloud infrastructures resilience; Security and dependability of embedded components; Data privacy and integrity in highly sensitive sectors. Our mid-term development plan relies on investigating and publishing state-of-the-art advances along the following strategic objectives, which we deploy as research lines: - Ultra-resilient minimal roots-of-trust and enclaves; - Hybridisation-aware distributed algorithms, models, and architectures; - High-confidence vertical verification of mid-sized software; - Privacy- and integrity-preserving decentralised data processing, namely in biomedical and in blockchain fields. To support proof-of-concept prototyping of its discoveries, the group has set up a Private Cloud and a CPS (cyber-physical systems) laboratory.

Summary of the group's achievements in 2017

The increase in manpower focused on PhD students, after the build-up of research associates in previous years. Further to developing results in the scientific areas described, the CritiX research group has been in contact with several companies whose interests match with the research topics of CritiX. Informal collaboration with LCSB (in cooperation with the SnT APSIA group) continues, having good perspectives.



Several papers (reported in Orbilu) have been published, some of which giving visibility to CritiX through presentations in conferences. Members of the group were involved in several events, some selected are: Distinguished Lecture, Univ. Illinois Champaign, US; Keynote, Inter-FORENSICS, Brasília, BR; Keynote, WACC@CCGRID, Madrid, ES; ICRI-CARS Ceremonial Kick-off, Darmstadt, DE; Keynote, Labora & China Portugal Energy R&D Seminar, Lisboa, PT; Keynote, SBESC, TU Curitiba, Curitiba, BR.

Members of the group were involved in several events, some selected are: IFIP WG10.4 Workshop in Aspen-US; participation as a UL element, to the ERC Starting Grants panel; Grande Region Sec. & Reliab. Day workshop; keynote on Cyberdefence at Military Academy International Symposium, Lisbon-PT; Cybersecurity "Made in Lux", REPER Lux, Brussels-BE, with the presence of Rectorate team elements; keynote European Cybersecurity Conference, Lisbon-PT; DSN conference as vice-chair of steering committee, Toulouse-FR; IFIP WG10.4

Workshop in Sorèze-FR; ESORICS conference, Iraklion-GR; address to Brazilian academia, military and information agencies, government and MPs, in the context of advisory to the Brazilian government on cybersecurity and cyberdefense, Brasilia-BR; invited to participate to the (closed) 2nd NATO Cyber Defence Smart Defence Projects Conference, Oeiras-PT; ACM CCS conference, Vienna-AU; keynote at Dagstuhl Seminar on Network Attack Detection and Defense, Dagstuhl-DE; organiser of the 1st CERTS@RTSS, Workshop on Security and Dependability in Critical Embedded Real-time Systems, run very successfully, Porto-PT. PJV was pivot of the participation of UL as founding member of the recent EU ECSO cPPP in cybersecurity.

Focused Research Activity results from 2017 (relevant papers can be found in the group's ORBILU web page):

- CritiX has been invited to partner with Intel in the Intel Collaborative Research Institute on Collaborative Autonomous and Resilient Systems (ICRI-CARS), to perform advanced research focused on vehicles, and autonomous driving safety-security concerns. CARS is formed by invitation only and includes 4 European research groups besides UL: TU Darmstadt (Germany), Aalto University (Finland), Ruhr-Universität Bochum (Germany), TU Wien (Austria).
- Internet and cloud infrastructures resilience: the CritiX team is seeking to continue its privileged position in the international SDN expertise arena (the high impact SDN survey published in January 2015, ramped-up to over 1350 citations (GSC)). A paper introducing a framework for secure communications in SDN was published (KISS), introducing an innovative key distribution and secure channel support (iDVV), expected to give an important contribution both to the robustness and simplification of the authentication and secure communication problems in SDN.
- High-confidence vertical verification of mid-sized software - In a paper recently accepted, we introduced a Coq-based framework to reason about implementations of BFT protocols, and used this framework to provide the first mechanical proof of safety of the seminal Castro/Liskov PBFT protocol.
- Privacy- and integrity-preserving decentralised data processing (biomedical) - We published a paper on the problems (and their mitigation) of SGX enclave-based genome alignment, namely leakage of sensitive genomic information if SGX enclaves accesses reference genome outside the enclave.

4.8 Critical Real-Time Embedded Systems (CRTES)

Head of research group: Assoc.-Prof. Nicolas Navet

The CRTES is part of the LASSY laboratory and studies how to build provably safe critical embedded systems in a time and cost efficient manner. The focus of this group is on software-intensive real-time systems having strong dependability constraints and a significant societal impact, such as transportation systems (road vehicles, aircrafts, etc) and IoT systems.

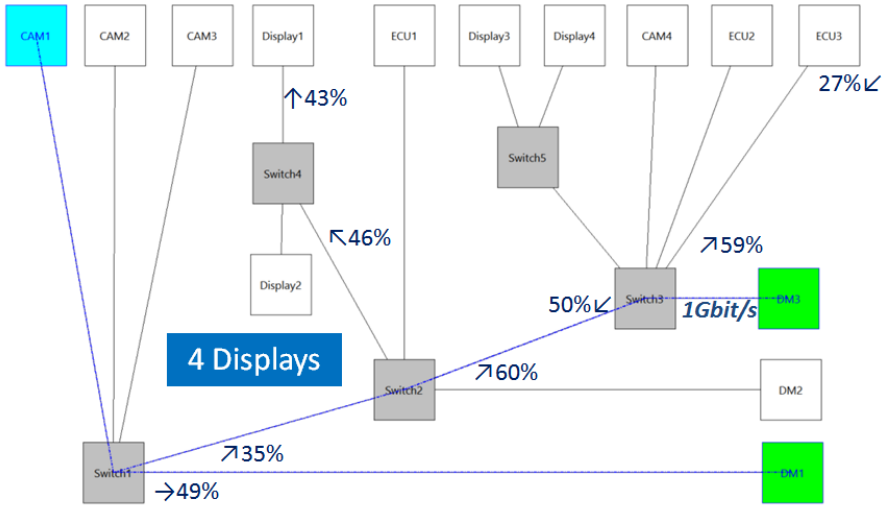
Summary of the group's achievements in 2017

In 2017, the CRTES group was made up of 4 members (1 associate-professor, 1 postdoc, 2 PhD students) and had 9 publications published or accepted. Most of the work was in the field of Model-Driven Engineering (MDE) for Embedded Systems. In particular, we developed an approach based on software patterns for automating the support for software diversity and software fault-injection. We also finalized a framework to systematize and automate the analysis of non-functional properties in MDE. This framework was applied to an avionic case-study combining heterogeneous models, and heterogeneous analyses for the verification. The two latter contributions are outcomes of the Phd thesis of Guillaume Brau, defended in 2017, which was awarded a foundation ISAE-SUPAERO award. Team members including Bachelor students developed two IoT systems: one for logistics (asset tracking) and the other for parking place management in partnership with Ville d'Esch-sur-Alzette. The latter IoT system was successfully field-tested. These IoT systems won the Life Prize, the Logistics Prize and the Special Jury Award at the Morpheus Cup 2017. New results were also obtained in the field of timing analysis, especially in TSN Ethernet networks. Prof. Navet was in the defense board of 3 Phd thesis, and has been involved in the CSC teaching programs especially as the course director of the professional Bachelor in Computer Science.

Main publications and achievements in 2017

- **G. Brau, N. Navet** and J. Hugues, "Towards the Systematic Analysis of Non-Functional Properties in Model-Based Engineering for Real-Time Embedded Systems", accepted for publication in Science of Computer Programming, Elsevier. We present an approach to systematize and automate the analysis of non-functional properties, like timing or safety constraints, in MDE. First, preconditions and postconditions define the applicability of an analysis. Then, contracts specify the analysis interfaces, thereby enabling to reason about the analysis process. We present a proof-of-concept implementation of our approach using a combination of constraint languages and specification languages. We then discuss our practical experience in applying the proposed framework on a real system, the Paparazzi UAV.
- **N. Navet**, J. Villanueva, J. Migge, M. Boyer, "Experimental assessment of QoS protocols for in-car Ethernet networks", 2017 IEEE Standards Association Ethernet & IP @ Automotive Technology Day. The set of TSN standards for Ethernet is re-shaping in-vehicle communications. To the best of our knowledge, this study with Renault Group is the first to assess the QoS that can be expected from the main TSN protocols currently considered in the automotive domain, and to provide insights into the different technological, design and configurations alternatives.
- **T. Hu**, I. Cibrario Bertolotti, **N. Navet**, "Towards Seamless Integration of N-Version Programming in Model-Based Design", in Proc. 22nd IEEE International Conference on Emerging Technologies And Factory Automation (ETFA'2017). We propose a new design pattern to model one of the prominent fault-tolerant techniques, namely N-Nersion Programming (NVP). The design pattern can be integrated seamlessly with existing system models to enhance

them with fault-tolerance feature, while preserving their timing characteristics, in particular the sampling times.



4.9 CryptoLux team

Head of research group: Prof. Dr. Alex Biryukov

The CryptoLux group is part of both LACS and SnT and is concerned with all aspects of symmetric cryptography ranging from design and analysis, efficient and secure implementation to deployment in real-world systems and networks. Detailed information about the group is available at http://cryptolux.org.

Summary of the group's achievements in 2017

In 2017 the CryptoLux group consisted of 8 members (1 professor, 1 senior researcher (shared), 1 postdoc, 4 PhD students, and 1 technical assistant (shared)), who published a total of 10 papers in major international journals and conference proceedings. The group successfully completed the FNR CORE project ACRYPT (Applied Cryptography for the Internet of Things) with 2 Ph.D. students related to this project graduating with excellence in 2017 and with excellent A+ final evaluation. The team got a new FNR CORE research project FinCrypt on future directions in fintech and financial cryptography approved for funding. Research highlights in 2017 include the development of the notions of symmetrically and asymmetrically hard cryptography, side-channel analysis and countermeasures, survey on lightweight cryptography, standardization activities related to the Argon2 password hashing function. Professor Biryukov and other members of the group served on the technical program committee of numerous conferences including top security conferences ACM CCS and NDSS. CryptoLux members taught various courses in the MICS bachelor and master

program and supervised student projects and theses. Last but not least, we have won the smart contract hackathon held in Luxembourg and the Whitebox design challenge by the project ECRYPT CSA.

Main publications and achievements in 2017

- **Alex Biryukov**, Léo Perrin: Symmetrically and Asymmetrically Hard Cryptography. ASIACRYPT (3) 2017. In this paper we present for the first time a unified framework for describing the hardness of a primitive along any of the three axes: code-hardness, time-hardness and memory-hardness. This unified view allows us to present modular block cipher and sponge constructions which can have any of the three forms of hardness and can be used to build any higher level symmetric primitive: hash function, PRNG, etc. We also formalize a new concept: asymmetric hardness.It creates two classes of users: common users have to compute a function with a certain hardness while users knowing a secret can compute the same function in a far cheaper way.
- Win in the Luxblock hackathon in May 2017: CryptoLux team has won shared 1st place in a 2-day smart contract programming event. There were more than 10 international teams with more than 50 coders.
- Win in the WhibOx design challenge run by ECRYPT CSA, September 2017: This was a international white-box design and analysis challenge run by EU project ECRYPT together with Cryptographic hardware (CHES) conference. There were dozens of teams participating, submitting designs and breaking each other's schemes. We have won the design challenge, with our design surviving the longest (almost 1 month), compared to some designs that were broken within minutes. We have also cryptanalyzed several runner up designs.

4.10 Foundations of Model-Driven Engineering (FMDE)

Head of research group: Prof. Dr. Pierre Kelsen

FMDE is a small research group: besides the head (Pierre Kelsen) it comprised 3 members in 2017: Qin Ma (research scientist, half-time), Loïc Gammaitoni (PhD student) and Christian Glodt (research associate). The research group explores fundamental questions in the area of model-driven engineering but also interests itself in concrete applications (eg, enterprise architecture and robotics).

Summary of the group's achievements in 2017

Pierre Kelsen was awarded a Teaching Award at the Rentrée Académique on October 12th as a recognition of excellence in teaching.

Qin Ma collaborated with other group members and colleagues from LIST and the University of Duisburg-Essen in the field of model transformation, enter-

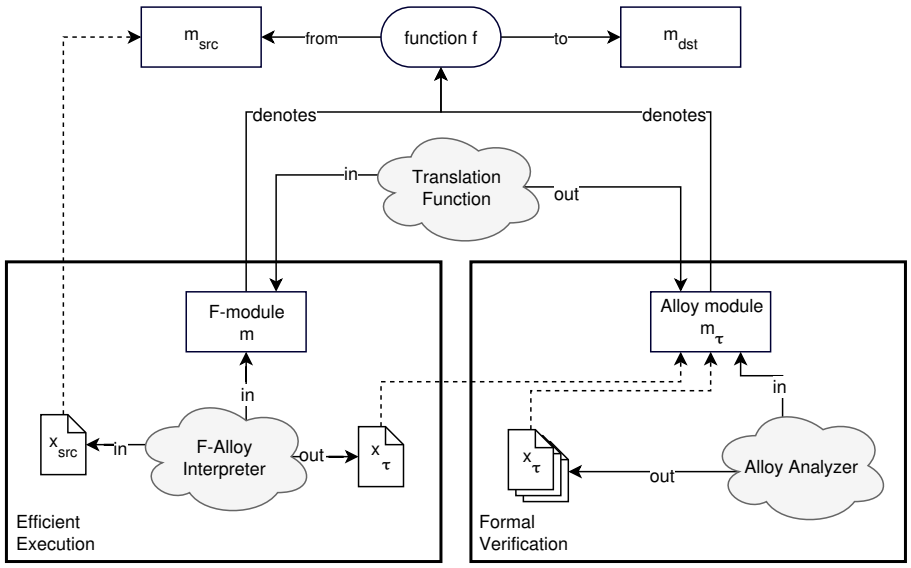
prise architecture, and conceptual modeling, resulting in three publications. Qin Ma also participated in the organisation of lab sessions for the ”Programming Fundamentals 1” course in the new ”Bachelor in Computer Science” degree.

Loïc Gammaitoni wrapped up his PhD thesis entitled ”On the Use of Alloy in Engineering Domain Specific Modeling Languages” and defended it successfully on October 16th with a grade of ”excellent”.

Christian Glodt improved ”Accord”, the research information database used by the CSC. Improvements include support for finer-grained permissions, configurable exports of data to web sites, as well as configurable report generation. He also participated in the organisation of lab sessions for the ”Programming Fundamentals 1” course in the new ”Bachelor in Computer Science” degree.

Most interesting publications in 2017

- **Gammaitoni, Loïc, and Pierre Kelsen**. ”F-Alloy: a relational model transformation language based on Alloy.” Software & Systems Modeling (2017): 1-35. The language F-Alloy is based on the formal language Alloy; it enables the concise expression, in an Alloy-like syntax, of efficiently computable model transformations.
- **Gammaitoni, Loïc, Pierre Kelsen, and Qin Ma**. ”Agile validation of model transformations using compound F-Alloy specifications.” Science of Computer Programming (2017). We propose a domain-specific approach to model transformation validation based on visualization (VBV) and show that such an approach greatly benefits from Hybrid Analysis, i.e., the combined used of Alloy analysis and F-Alloy interpretation.
- S. de Kinderen, M. Kaczmarek-Heß, **Q. Ma**, and I. S. Razo-Zapata. “Towards Meta Model Provenance: a Goal-Driven Approach to Document the Provenance of Meta Models”. In: Lecture Notes in Business Information Processing (LNBIP) 305, pp. 49-64, 2017. We propose a model-based approach to understand, document and trace the origins (provenance) of modelling language specifications, in support of controlled modelling language evolution and informed modelling language (re-)design.



4.11 Individual and Collective Reasoning (ICR)

Head of the research group: Prof. Dr. Leon van der Torre

ICR forms a cornerstone of the Interdisciplinary Lab for Intelligent and Adaptive Systems (ILIAS). Within UL it collaborates with several centres and research units: e.g. the SnT, the Center for Contemporary and Digital History (C2DH), the RU Law, and the Institute of Cognitive Science and Assessment. Its research areas include normative reasoning in multi-agent contexts (deontic logics, AI ethics), logics for intelligent agents/robots, legal knowledge representation and reasoning (also exploiting NLP), formal/computational argumentation, and defeasible reasoning with uncertain/inconsistent information, with applications to AI, law, and formal sciences.

Summary of the group's achievements in 2017

In 2017, ICR hosted 22 researchers: 1 full prof., 1 visiting and 1 guest prof., 1 senior researcher, 6 resident and 3 visiting postdocs, and 9 PhD students. MIREL (Mining and Reasoning with Legal Texts), an H2020-MSCA-RISE network coordinated by ICR, entered its 2nd year and brought a number of fruitful exchange activities with visits (2 weeks - 3 months, overall 8 months) to Tokyo, Stanford, resp. Hangzhou/Zhejiang University by 4 ICR-members, and 2 researchers from Argentina visiting ICR.

The group also organized 2 major conferences: in Luxembourg JURIX 2017 (30th Int. Conf. on Legal Knowledge and Information Systems), strengthening its stance in Law and AI, and in Nice PRIMA 2017 (20th Int. Conf. on Principles and Practice of Multi-Agent Syst.), with a thematic day on Ethics by Design.

Within ILIAS, ICR has supported an interdisciplinary initiative on Ethical Intelligent Systems (EIS), joining forces with groups from FDEF and FLHASE. With a PhD project on argument mining within the DTU Digital History and Hermeneutics, ICR has started a promising cooperation with the C^2DH. ICR continues to be involved in the ERASMUS+ network LAST-JD (Joint International Doctoral Degree in Law, Science, and Technology), which each year involves 9-month visits of several PhD students in Luxembourg, with 4 completed PhDs in 2017. Within ICR, D.A. Ambrossio and M. van Zee obtained their PhD and went for AI-jobs in industry. Theoretical and empirical studies within the CAFA INTER project (with cognitive psychology), which investigate the adequacy of logical models for argumentation in science, have allowed to identify problems with earlier approaches.

On the theoretical side, there have been further insights into the semantic foundations and the logic of defeasible arguments and defeasible obligations. As a reference work for future research, the Handbook of Formal Argumentation was finalized, with two chapters contributed by members of ICR. Research on argumentation was also backed by the the ongoing visits of Prof. B. Liao from Zhejiang University (FNR Mobility), and our long-term collaborator Prof. D. Gabbay from King's College. The CSC Robolab, now led by Dr. F. Lera, supported educational and outreach activities in robotics, an area of growing relevance. It also accompanied our homegrown startup LuxAI (social robots, e.g. for autistic children - FNR proof-of-concept), which collected several awards in 2017, into its 2nd year. The long-term visit of a leading expert in automated theorem proving, Priv.-Doz. Dr. Chr. Benzmueller, provided computational tools for deontic reasoning and the experimental design and evaluation of agent logics.

Three interesting publications (or other achievements) in 2017

- **X. Parent, L. van der Torre.** *Detachment in Normative Systems: Examples, inference Patterns, Properties.* IfCoLog Journal of Logics and their Applications 4 (9), 2295-3039 (2017). There are a variety of ways to reason with normative systems which reflect the various semantics developed for deontic logic, e.g. based on possible worlds, on algebraic methods, on explicit norms, or techniques from non-monotonic logic. The question is how these reasoning methods are related and which ones are appropriate for a particular application. In this paper, we begin by analyzing common benchmark examples at a higher level of abstraction and distinguish different possible interpretations. Next we discuss important logical inference patterns. To conclude, we specify ten more abstract properties around the notion of detachment and explain why they constitute desirable principles for normative reasoning methods.
- M. Dastani, **L. van der Torre,** N. Yorke-Smith. *Commitments and interaction norms in organisations.* Autonomous Agents and Multi-Agent Systems 31 (2), 207-249 (2017). In an organisational setting such as an online marketplace, an entity called the 'organisation' defines interaction protocols, monitors agent interaction, and intervenes to enforce the protocols. In this article we abstract over application-specific protocols and consider commitment lifecycles as generic interaction protocols. We model them by explicitly represented

norms, which allows a logical analysis. We adopt insights and methods from commitment-based approaches to agent interaction as well as from norm-based approaches to agent behaviour governance. We show how to use the norms to model commitment dynamics (lifecycles), introduce an operational semantics for norm enforcement, and logically analyse interaction protocols by means of commitment dynamics and norm enforcement. The model, semantics, and analysis are illustrated by a running example from a vehicle insurance domain.

- **Marcos Cramer, Giovanni Casini.** *Postulates for Revocation Schemes.* POST 2017: International Conference on Principles of Security and Trust, 232-252 (2017). In access control frameworks allowing the delegation of permissions and administrative rights, there can be delegation chains. There are different ways to treat them when revoking rights, which gives rise to different revocation schemes. Hagström et al. proposed a classification framework where these schemes are defined graph-theoretically. We identify however multiple problems with their definition of revocation schemes, which can pose security risks. Our goal is to systematically ensure that improved definitions of the revocation schemes do not lead to similar problems. For this we propose to apply an axiomatic method originating in social choice theory to revocation schemes. This is reminiscent of what is done in belief revision theory. So we define postulates that describe the desirable behaviour of revocation schemes, study which existing revocation frameworks satisfy which postulates, and show how all the postulates can be satisfied by defining the revocation schemes in a novel way.

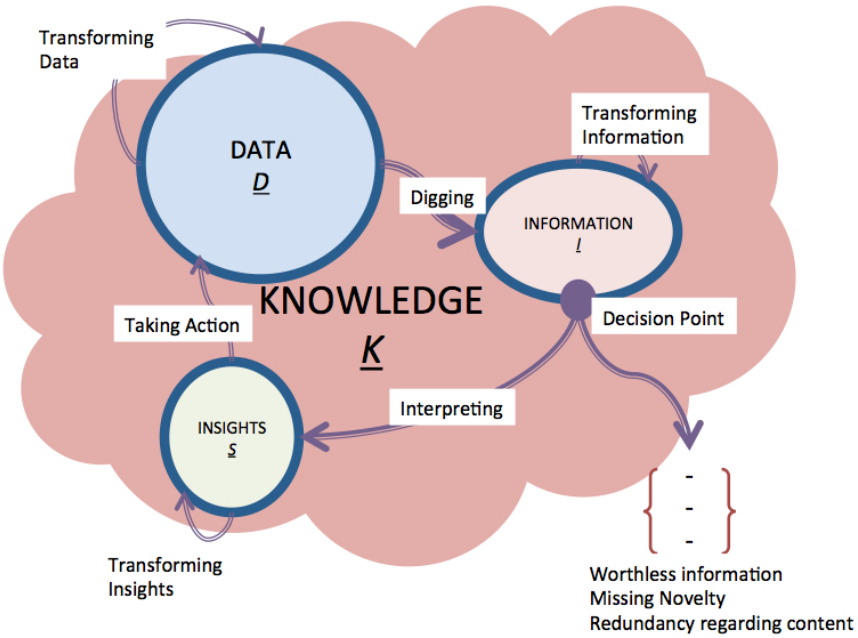
Logo of Legal Informatic Luxembourg (http://www.luxli.lu/): this service of CSC joins interdisciplinary academic research and technology transfer to the industry in order to devise novel cutting-edge legal services.

4.12 Knowledge Discovery and Mining (MINE)

Head of research group: Prof. Dr. Christoph Schommer

The MINE group, as part of the ILIAS research laboratory, follows a strongly interdisciplinary mission, for example, with common research projects with

the Dept of Linguistics and the C2DH Interdisciplinary Centre. MINE demonstrates strong expertise in the education of students on all levels and offers interdisciplinary courses, for example, in cooperation with the Department of Mathematics and the Department of Logistics and Entrepreneurship. Besides, MINE is a member of the Doctoral Training Unit "Digital History and Hermeneutics" (DHH). MINE's research interest focuses on the discovery of knowledge (see the life cycle in Figure) in general and on working in disciplines like Natural Language Processing, Text Analytics, Data Science and Data Mining, Deep Learning, and Artificial Companions in particular. For more information see the MINE group's homepage: http://wiki.uni.lu/mine



Summary of the group's achievements in 2017

Prof Schommer has been the Director of the ILIAS Research Lab and has led a group of more than 40 researchers (professors, guest professors, PostDoc researchers, and PhD students). He has organised the 2017 ILIAS Distinguished Lecture Series, where 12 guest speakers have presented their view on Artificial Intelligence for the Society; furthermore, he has further developed the Artificial Companions Laboratory (see http://acc.uni.lu). Having been a visiting scholar professor at Tshinghua University in 2015 and 2016, Prof Schommer has received an invitation to teach abroad at the University of Lemberg, Ukraine.

Research Projects

- In the research project RAT, we work on automatic solutions to recognize and to understand the content of early printed maps, mainly from the 16th to 19th century, and bring them into a computer-readable format. To reach

this goal a wide range of machine learning algorithms is used, especially related to computer vision tasks. This work enhances the searchability within these historic documents and enables further research like understanding the history of a place name or examining the similarities and differences between maps. Cooperation Partners: C2DH, University of Würzburg.
- In the research project PERSEUS, we aim at discovering individualities in expressing sentiments in text. To study the diversity between individuals and the consistency in each individual, we have build a personalized framework that takes user-related text from social platforms, such as Twitter and Facebook, and investigates and improves sentiment categorization by applying Deep Learning techniques. This project researches beyond purely understanding the meaning of text, and focuses on integrating the preference and tendency of users to provide user-sensitive predictions. Cooperation Partners: Lenovo AI Research Beijing.
- A third research project - as part of the Doctoral Training Unit DHH - concerns text autobiographies with respect to Australian Aborigines. Despite their remarkable value, autobiographies appear to remain one of the most under-utilized historical resources. The proposed research project in digital humanities will apply computational Distant Reading-methods (natural language processing in general and topic modeling in particular) as a complement to traditional "close reading" of Indigenous Australian autobiographies, aiming to identify meaningful language use patterns in the context of social environment and historical events. Cooperation Partners: C^2DH, University of Sydney.

Main publications and achievements in 2017

- **S. Guo, C. Schommer** (2017). *Embedding of the Personalized Sentiment Engine PERSEUS in an Artificial Companion*. International Conference on Companion Technology, Ulm 11-13 September 2017. IEEE.
- **W. Höhn, C. Schommer** (2017). *Geo-referencing of Place Markers in Digitized Early Maps by Using Similar Maps as Data Source*. Digital Humanities 2017, Montréal, Quebec, Canada.
- **W. Höhn, C. Schommer** (2017). *RAT 2.0*. Digital Humanities 2017, Montréal, Quebec, Canada.
- T. van Dijk, T., **C. Schommer** (Eds.,2017). Proceedings of the 2nd International Workshop on *Exploring Old Maps*. Würzburg, Germany: University of Würzburg.
- **C. Schommer**. *Q&A with Data Scientists.* Interview with Christopher Schommer. Operational Database Management Systems.

4.13 Methods and Tools for Scientific Requirements Engineering (MESSIR)

Head of research group: Prof. Dr. Nicolas Guelfi

The MESSIR group is part of the LASSY laboratory. It focuses on introducing model driven engineering approaches in the software development life cycle, in particular for the requirements analysis activity. The group also addresses experimental research in computing education, with special emphasis on software engineering in a global context.

Summary of the group's achievements in 2017

The requirements analysis method called MESSIR and its supporting open source tool (called Excalibur) have been deployed in the context of research and teaching collaboration at Innopolis University (Kazan, Russia) and National University of Rosario (Rosario, Argentina).

The group has played a key role in the setting and launch of the new Bachelor in Computer Science at the University of Luxembourg. It was in the context of this work that a tool has been developed by the team to ease the management of the projects students perform every semester along with either staff of the university or external collaborators.

Last, but not least important is the work being carried out with regards to the BICS Challenge. The aim of this event is twofold: spread the voice about the BICS while attracting motivate and talent students to follow such a educational track.

Main publications and achievements in 2017

- **Guelfi, Nicolas, Benjamin Jahic, and Benoît Ries**. " TESMA: Requirements and Design of a Tool for Educational Programs", Information 2017, Special Issue on "Applications in Information Technology, 8(1), 37; 2017. This paper presents the on-going project called TESMA, whose objective is to provide an open-source tool dedicated to the specification and management (including certification) of teaching programs. The paper also includes an in-depth market analysis regarding related tools and conceptual frameworks of the project is presented.
- **Nicolas Guelfi, Alfredo Capozucca, and Benoit Ries**. "A Product Line of Software Engineering Project Courses", poster at the 30th IEEE Conference on Software Engineering Education and Training, Savannah, Georgia, USA, 2017 This poster presents a method for the derivation of software engineering project courses. It reuses, from a conceptual viewpoint, the product line paradigm for its description, and is strongly based on the SWEBOK.
- In 2017, Prof. Dr. Guelfi, Dr. Ries and Dr. Capozucca were invited as professors at Innopolis University to deliver a course for bachelor and master students on software engineering and development. It was also in 2017, that

Dr. Capozucca spent one full month as visiting professor at the National University of Rosario, where he delivered a course for master and doctoral students about the Messir methodology and performed research activities on verification-related aspects of the Messir methodology.

4.14 Parallel Computing and Optimisation Group (PCOG)

Head of research group: Prof. Dr. Pascal Bouvry

The Parallel Computing and Optimisation group conducts research on parallel computing and optimization techniques, in particular how different species may co-evolve taking local decisions while ensuring global objectives, to tackle large and difficult problems. The main application domains are security, trust and reliability; reliable scheduling and routing on new generations of networks; sustainable development and systems biomedicine; Unmanned autonomous vehicles (UAV), Smart Cities. Detailed information about the group is available at http://pcog.uni.lu/. The head of the team, Prof. Pascal Bouvry acts as special advisor to the rector in matters of high performance computing, member of the editorial board of 4 top international journals (IEEE Cloud Computing magazine, IEEE Transactions on Sustainable Computing, Elsevier Swarm and Evolutionary Computation journal, Springer Scalable Computing and journal) and author of over 300 papers in international peer-reviewed venues.

Summary of the group's achievements in 2017

In 2017, the PCOG team counted 15 members (1 professor, 2 senior researchers, 4 postdocs, 8 PhD students) and produced a total of 22 publications (7 journal articles, 15 conference articles). 2 PhD students successfully defended their thesis in 2017. The group is also involved in the H2020 Erasmus+ LAST-JD "Joint International Doctoral Degree in Law, Science and Technology", with Prof. Bouvry co-supervising 1 PhD student.

The group successfully completed both the ASIMUT (Aid to SItuation Management based on MUtlmodal, MultiUAVs, Multi-level acquisition Techniques) project funded by the European Defense Agency (EDA) and the IShoP (Internet Shopping Optimisation) project funded by the FNR (POLLUX program). In addition, the PCOG started the Digital Trust in Smart ICT research programme in collaboration with the ILNAS.

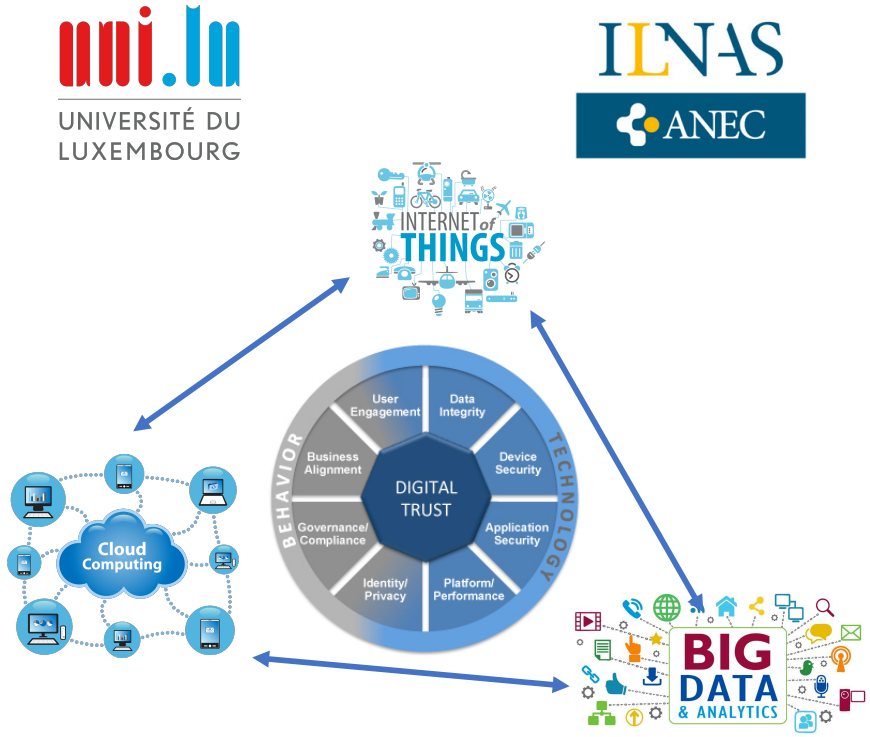
PCOG team members taught in several Bachelor, Master and PhD programs (BINFO, Bachelor en Sciences de la Vie, MICS, Master in Entrepreneurship and Innovation, Doctoral School in Computer Science).

In October 2017, the UL was chosen by the Ministry to represent the country within PRACE (Partnership for Advanced Computing in Europe). The official Country Delegate (Prof. Pascal Bouvry) and Advisor (Dr. Sébastien Varrette)

were present at the 27th PRACE Council meeting where Luxembourg's application received an unanimous approval.

Three most interesting publications (or other achievements) in 2017

- Digital Trust in Smart ICT Project – **https://smartict.gforge.uni.lu/.** Following the successful launch of the University Certificate "Smart ICT for business innovation" in September 2015 and the future creation of a new Master's degree in partnership with the Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS); the four year and 2M€ project "Digital Trust in Smart ICT" aims at developing Luxembourg as a European centre of excellence and innovation for secure, reliable, and trustworthy Smart ICT systems and services. With emphasis on digital trust for smart ICT and the related standardization efforts, the scientific research in the context of this joint program focuses on the three main pillars of, Big Data & Analytics, Internet-of-Things (IoT), Cloud Computing
- The High-Performance Computing platform of the UL managed by **Prof. Bouvry and Dr Varrette**, it is currently the largest facility of this type in Luxembourg (after GoodYear's industrial R&D Center). End of 2017, the HPC platform featured a computational power of 271 TFlops (10132 computing cores) and 7.9 PBytes for storage (incl. 2.1 PB for backups), serving 418 users. In terms of cumulative hardware investments since 2007 (excluding server rooms costs), the UL HPC has reached a total of 8.174 M€.
- Best paper award at IEEE CybConf 2017. **Matthias R. Brust, Grégoire Danoy and Pascal Bouvry** received a best paper award at the 3rd IEEE International Conference on Cybernetics (CYBCONF) for their article "Target Tracking Optimization of UAV Swarms Based on Dual-Pheromone Clustering". This work is also co-authored with three students from the MICS since it is based on their project from the Optmization for Computer Science lecture given by Prof. Bouvry and Dr. Danoy.



4.15 Proactive Computing

Head of research group: Prof. Dr. Denis Zampuniéris

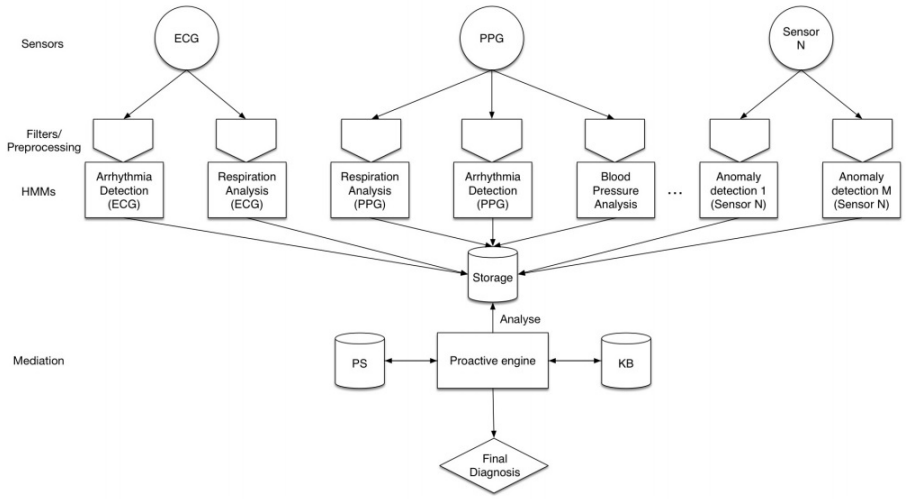
This small group, counting 3 members (1 professor, 1 PhD student, 1 technical assistant) is part of the LASSY research laboratory. It focuses on formalizing and implementing proactive computing principles into the development of innovative, pervasive and/or autonomic software systems for several real-world application fields. The proactive computing paradigm provides us with a new way to make the multitude of computing systems, devices and sensors spread through our modern environment, work for/pro the human beings and be active on our behalf.

Summary of the group's achievements in 2017

Apart from their regular research and publication work and their participation in teaching programmes offered by our Faculty, the group members welcomed and supervised several students (local or from universities abroad) in internship for their Bachelor or Master thesis.

Main publications in 2017

- **Gilles Neyens and Denis Zampuniéris.** Conflict handling for autonomic systems. In Proc. IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO), Tucson (USA), 2017. Technological advances in recent years lead to the miniaturization of a whole arsenal of different sensors. They can be used to offer new services in eHealth applications, smart homes, robotics or smart cities. With the increasing diversity and the cooperation needed between these sensors in order to provide the best possible services to the user the systems that use the data coming from these sensors need to be able to handle conflicting information and thus also conflicting actions. In this paper we propose an approach that uses Hidden Markov Models in a first step to analyse the incoming data and in a second step uses a rule engine in order to handle the occurring conflicts.
- **Gilles Neyens and Denis Zampuniéris.** Using Hidden Markov Models and Rule-based Sensor Mediation on Wearable eHealth Devices. In Proc. International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, Barcelona (Spain), 2017. Improvements in sensor miniaturization allow wearable devices to provide more functionality while also being more comfortable for users to wear. The Samsung Simband©, for example, has 6 different sensors Electrocardiogram (ECG), Photoplethysmogram (PPG), Galvanic Skin Response (GSR), BioImpedance (Bio-Z), Accelerometer and a thermometer as well as a modular sensor hub to easily add additional ones. This increased number of sensors for wearable devices opens new possibilities for a more precise monitoring of patients by integrating the data from the different sensors. This integration can be influenced by failing or malfunctioning sensors and noise. In this paper, we propose an approach that uses Hidden Markov Models (HMM) in combination with a rule-based engine to mediate among the different sensors' data in order to allow the eHealth system to compute a diagnosis on the basis of the selected reliable sensors. We also show some preliminary results about the accuracy of the first stage of the proposed model.



Hidden Markov Models in combination with rule-based Proactive Engine to mediate among data flowing from the different sensors, allowing the eHealth system to compute a diagnosis.

4.16 Security and Networking Lab (SECAN-Lab)

Head of group: Prof. Dr. Thomas Engel

SECAN-Lab addresses both fundamental and applied research in computer networking, privacy, and security, namely in the areas of privacy by distribution, network and system security, SCADA and cyber security, IoT, vehicular communication and multimodal traffic management, and wireless networks and mobile security. Headed by Prof. Dr. Thomas Engel, SECAN-Lab is composed of a balanced team of established high-level research associates, doctoral candidates and research management professionals spanning across a variety of fields, and with many contributing with a significant industry expertise gained at both national and international levels.

Main achievements in 2017:

SECAN-Lab successfully completed four of its 20 externally funded projects and had two new projects starting that focused on the group's core areas, including security and privacy in data communication, vehicular communication for traffic management, and IoT. Moreover, the lab has five ongoing PhD projects and the group head together with senior researchers are involved in supervision of five further external PhD projects. Most notably, SECAN-Lab won Honda HIGE Grant and started cooperation with this car manufacturer on secure car

entry systems. In 2017, SECAN-Lab was involved in various international scientific conferences (published 32 papers) and organized two workshops on smart mobility bringing together about 80 European actors from both industry and academia. Moreover, team members have taught extensively within the University of Luxembourg's BSc and MSc programs and supervised bachelor and master student projects and theses. The annual SECAN-Lab Dagstuhl retreat consolidated the group's activities in collaboration with external guests and partners. During the reporting year, one PhD student (Walter Bronzi) successfully defended his thesis and graduated.

Main publications in 2017

- **A. Panchenko, A. Mitseva**, M. Henze, F. Lanze, K. Wehrle, **T. Engel**. Analysis of Fingerprinting Techniques for Tor Hidden Services. In Proceedings of the 24th ACM Computer and Communications Security (ACM CCS) 16th Workshop on Privacy in the Electronic Society (ACM WPES 2017. The website fingerprinting attack aims to infer the content of encrypted and anonymized connections by analyzing traffic patterns such as packet sizes, their order, and direction. Although it has been shown that no existing fingerprinting method scales in Tor when applied in realistic settings, the case of Tor hidden (onion) services has not yet been considered in such scenarios. Recent works claim the feasibility of the attack in the context of hidden services using limited datasets. In this work, we propose a novel two-phase approach for fingerprinting hidden services that does not rely on malicious Tor nodes. In our attack, the adversary merely needs to be on the link between the client and the first anonymization node. In the first phase, we detect a connection to a hidden service. Once a hidden service communication is detected, we determine the visited hidden service (phase two) within the hidden service universe. To estimate the scalability of our and other existing methods, we constructed the most extensive and realistic dataset of existing hidden services. Using this dataset, we show the feasibility of phase one of the attack and establish that phase two does not scale using existing classifiers. We present a comprehensive comparison of the performance and limits of the state-of-the-art website fingerprinting attacks with respect to Tor hidden services.
- A. Koesdwiady, R. Soua, F. Karray, M. Kamel. Recent Trends in Driver Safety Monitoring Systems: State of the Art and Challenges. In IEEE Transactions on Vehicular Technology (Volume: 66, Issue: 6, June 2017). Driving in busy highways and roads is becoming complex and challenging, as more cars are hitting the roads. Safe driving requires attentive drivers, quality perception of the environment, awareness of the situation, and critical decision making to react properly in emergency situations. This paper provides an overview on driver safety monitoring systems. We study various driver sources of inattention while providing a comprehensive taxonomy. Then, different safety systems that tackle driver inattention are reported. Furthermore, we present the new generation of driver monitoring systems within the context of Internet of Cars. Thus, we introduce the concept of integrated safety, where smart cars collect information from the driver, the car, the road, and, most importantly, the surrounding cars to build an efficient environment for the driver. We conclude by highlighting issues and emerging trends envisioned

by the research community.

- A. Popleteev. Please Stand By: TV-based indoor localization. In Proceedings of the 28th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (IEEE PIMRC 2017). Despite the decades of efforts, indoor positioning remains an open research challenge. While existing solutions already demonstrate high accuracy, their in-building infrastructure — such as Wi-Fi access points or Bluetooth beacons — provides only a limited coverage. This paper investigates feasibility of accurate indoor positioning using broadcast digital TV signals, readily available in populated areas worldwide. We experiment with the classic received signal strength (RSS) fingerprinting, and introduce a novel approach based on channel state information (CSI), which leverages frequency-selective multipath fading of wideband TV signals. The proposed methods are experimentally evaluated on an extensive dataset of DVB-T signals, systematically collected in two large buildings over the course of 8 months. The results show that the proposed approach consistently outperforms RSS fingerprinting and achieves 92–98% localization accuracy. While this study is based on the European DVB-T signals, the proposed method is directly generalizable to other TV standards (such as ATSC, ISDB, DTMB and DMB) and wide-area TV white space (TVWS) networks.

4.17 Security and Trust of Software Systems (SaToSS)

Head of research group: Prof. Dr. Sjouke Mauw

Since its establishment in 2007, the SaToSS group focused on formalizing and applying formal reasoning to real-world security problems. Research in the SaToSS group is carried out on a variety of topics, such as:

- security protocols (e.g. contract signing, distance bounding, e-voting),
- attack trees and threat analysis,
- privacy (e.g. location privacy and privacy in social networks),
- modelling and analysis of biological systems,
- process algebra and model checking,
- data mining and machine learning,
- malware detection and mobile security,
- security of cyber-physical socio-technical systems,
- trust management

SaToSS is part of the LACS and ComSys laboratories and has a strong connection to the Luxembourg Centre for Security, Reliability and Trust (SnT). For more information, please visit our webpage at http://satoss.uni.lu/

Summary of the group's achievements in 2017

In 2017 the SaToSS group counted 18 researchers (1 professor, 1 senior researcher, 8 postdocs, 6 PhD students and 2 technical assistants), which is a record since the group's establishment. In February 2017, SaToSS celebrated 10 years since its foundation. The celebration was marked by a workshop, where 9 former group members gave presentations about their current research. Further, the group published 19 research papers.

In 2017 SaToSS has successfully completed the FNR-funded CORE project (ADT2P on attack trees). The group runs two Junior CORE projects (COMMA on malware analysis and DIST on distance-bounding protocols), one FNR-INTER project (AlgoReCell on models of biological networks), and one UL-funded project (SECPBN on computational modelling in biology). The group also continues to be active in the large Singaporean project Securify. In 2017 the group has secured funding for another Junior CORE project (PrivDA on privacy issues in social networks), which will start in 2018.

The group has contributed to the organization of scientific events (GRSRD 2017, GraMSec 2017). Our regular research seminar SRM co-organized jointly with the APSIA group has featured 35 speakers from 14 countries. SaToSS has been involved in teaching and student supervision for the Bachelor and Master programs in Computer Science (BINFO, BICS, MICS, MSSI). Another highlight of the year was the PhD thesis defense by Qixia Yuan.

Main publications and achievements in 2017

- *Semantics for Specialising Attack Trees based on Linear Logic.* R. Horne, **S. Mauw** and A. Tiu. Fundamenta Informaticae, 153(1-2):57–86, 2017. Attack

trees profile the sub-goals of the proponent of an attack. Attack trees have a variety of semantics depending on the kind of question posed about the attack, where questions are captured by an attribute domain. We observe that one of the most general semantics for attack trees, the multiset semantics, coincides with a semantics expressed using linear logic propositions. The semantics can be used to compare attack trees to determine whether one attack tree is a specialisation of another attack tree. Building on these observations, we propose two new semantics for an extension of attack trees named causal attack trees. Such attack trees are extended with an operator capturing the causal order of sub-goals in an attack. These two semantics extend the multiset semantics to sets of series-parallel graphs closed under certain graph homomorphisms, where each semantics respects a class of attribute domains. We define a sound logical system with respect to each of these semantics, by using a recently introduced extension of linear logic, called MAV, featuring a non-commutative operator. The non-commutative operator models causal dependencies in causal attack trees. Similarly to linear logic for attack trees, implication defines a decidable preorder for specialising causal attack trees that soundly respects a class of attribute domains

- *walk2friends: Inferring social links from mobility profiles.* M. Backes, M. Humbert, **J. Pang** and Y. Zhang. In Proc. 24th ACM International Conference on Computer and Communications Security (CCS'17), ACM Press, pp. 1943-1957, 2017. The development of positioning technologies has resulted in an increasing amount of mobility data being available. While bringing a lot of convenience to people's life, such availability also raises serious concerns about privacy. In this paper, we concentrate on one of the most sensitive information that can be inferred from mobility data, namely social relationships. We propose a novel social relation inference attack that relies on an advanced feature learning technique to automatically summarize users' mobility features. Compared to existing approaches, our attack is able to predict any two individuals' social relation, and it does not require the adversary to have any prior knowledge on existing social relations. These advantages significantly increase the applicability of our attack and the scope of the privacy assessment. Extensive experiments conducted on a large dataset demonstrate that our inference attack is effective, and achieves between 13% to 20% improvement over the best state-of-the-art scheme. We propose three defense mechanisms – hiding, replacement and generalization – and evaluate their effectiveness for mitigating the social link privacy risks stemming from mobility data sharing. Our experimental results show that both hiding and replacement mechanisms outperform generalization. Moreover, hiding and replacement achieve a comparable trade-off between utility and privacy, the former preserving better utility and the latter providing better privacy
- *Should we learn probabilistic models for model checking? A new approach and an empirical study*. J. Wang, J. Sun, **Q. Yuan** and **J. Pang**. In Proc. 20th International Conference on Fundamental Approaches to Software Engineering (FASE'17), Springer-Verlag, Lecture Notes in Computer Science 10202, pp. 3-21, 2017. Many automated system analysis techniques (e.g., model checking, model-based testing) rely on first obtaining a model of the system under analysis. System modeling is often done manually, which is often considered as a hindrance to adopt model-based system analysis and development techniques. To overcome this problem, researchers have proposed to auto-

matically "learn" models based on sample system executions and shown that the learned models can be useful sometimes. There are however many questions to be answered. For instance, how much shall we generalize from the observed samples and how fast would learning converge? Or, would the analysis result based on the learned model be more accurate than the estimation we could have obtained by sampling many system executions within the same amount of time? In this work, we investigate existing algorithms for learning probabilistic models for model checking, propose an evolution-based approach for better controlling the degree of generalization and conduct an empirical study in order to answer the questions. One of our findings is that the effectiveness of learning may sometimes be limited.

4.18 Security, Reasoning and Validation (SerVal)

Head of research group: Prof. Dr. Yves Le Traon

The SerVal – SEcurity, Reasoning and VALidation Research Group is headed by Professor Yves Le Traon and mixes researchers from CSC and SnT. SerVal conducts research on Software Engineering and Software Security, with a focus on data intensive, mobile and complex systems. Researchers in the team leverage various techniques around three main pillars including:

- Software Testing (Mutation Testing, Search-Based Testing, ...)
- Semi-Automated and Fully-Automated Program Repair
- Data Analytics, predictive and prescriptive techniques (Decision Support Services)
- Multi-objective reasoning and optimization
- Model-driven data analytics (on top of Models@run.time)
- Information Retrieval and Data mining to collect knowledge
- Mobile Security, malware detection, prevention and dissection

SerVal strives to be ahead of the challenges of tomorrow's world. The research group builds innovative research solutions for trending and exciting domains such as the Android ecosystem and mobile security, next generations of information systems for banking and public administration, IoT, Fintech, Smart Grid and Smart Home infrastructures, and the latest paradigms of databases.

Summary of the group's achievements in 2017

2017 was a very fruitful year for Serval. The number of members increased to about 30 researchers. They published about 35 papers in top venues such as ICSE, Empirical Software Engineering, ISSTA, IST, IEEE TIFFS, IEEE TSE etc. They acquired industrial projects with BGL and Cebi. Prof. Le Traon acquired a mobility grant to visit UC Berkeley for 8 months: his scientific leave started in August 2017, and he collaborates with Pr. Koushik Sen from UC Berkeley, John Micco from Google and Vadim Kutsyy from Paypal on topics related to software testing and overall system safety and security.

Main publications and achievements in 2017

- Understanding android app piggybacking: A systematic study of malicious code grafting: Li Li, Daoyuan Li, Tegawendé F Bissyandé, Jacques Klein, **Yves Le Traon**, David Lo, Lorenzo Cavallaro, IEEE Transactions on Information Forensics and Security. Short Summary: The Android packaging model offers ample opportunities for malware writers to piggyback malicious code in popular apps, which can then be easily spread to a large user base. Among several findings providing insights analysis techniques should build upon to improve the overall detection and classification accuracy of piggybacked apps, we show that piggybacking operations not only concern app code, but also extensively manipulates app resource files, largely contradicting common beliefs. We also find that piggybacking is done with little sophistication, in many cases automatically, and often via library code.
- (Best Journal Paper award) The next evolution of MDE: a seamless integration of machine learning into domain modeling: T Hartmann, A Moawad, F Fouquet, **Y Le Traon**. Software & Systems Modeling, 1-20. Short Summary: Machine learning algorithms are designed to resolve unknown behaviours by extracting commonalities over massive datasets. In this paper we propose to weave machine learning into domain modeling. More specifically, we suggest to decompose machine learning into reusable, chainable, and independently computable small learning units, which we refer to as micro learning units. These micro learning units are modeled together with and at the same level as the domain data. We show, based on a smart grid case study, that our approach can be significantly more accurate than learning a global behaviour while the performance is fast enough to be used for live learning.
- Comparison of metadata quality in open data portals using the Analytic Hierarchy Process: S Kubler, J Robert, S Neumaier, J Umbrich, **Y Le Traon** - Government Information Quarterly, 2017. Short Summary: The quality of metadata in open data portals plays a crucial role for the success of open data. E-government, for example, have to manage accurate and complete metadata information to guarantee the reliability and foster the reputation of e-government to the public. To address this Multi-Criteria Decision Making (MCDM) problem, this paper develops an Open Data Portal Quality (ODPQ) framework that enables end-users to easily and in real-time assess/rank open data portals. The proposed framework is used to compare over 250 open data portals, powered by organizations across 43 different countries. The findings reveals that today's organizations do not pay sufficient heed to the management of datasets, resources and associated metadata that they are currently publishing on their portal.
- An empirical study on mutation, statement and branch coverage fault revelation that avoids the unreliable clean program assumption: Thierry Titcheu Chekam, **Mike Papadakis**, **Yves Le Traon**, Mark Harman - Proceedings of the 39th International Conference on Software Engineering (ICSE 2017). Short Summary: Many studies suggest using coverage concepts, such as branch coverage, as the starting point of testing, while others as the most prominent test quality indicator. Yet the relationship between coverage and fault-revelation remains unknown, yielding uncertainty and controversy. We present evidence that the Clean Program Assumption does not always hold, thereby raising a critical threat to the validity of previous results. Our findings also re-

vealed that fault revelation starts to increase significantly only once relatively high levels of coverage are attained.

4.19 Signal Processing and Communications (SIGCOM)

Head of research group: Prof. Dr. Björn Ottersten, deputy head: Dr. Symeon Chatzinotas

The SIGCOM department is both part of the SnT Centre for Security, Reliability, and Trust and the CSC research unit. The team focuses on signal processing for satellite/wireless communications, radar signal processing and signal, image and data processing aspects of computer vision.

The research on communications focuses on the formulation, modelling, design, and analysis of future communication networks (5G and beyond) that are capable of supporting new services in a cost efficient manner. This includes transceiver design for linear and non-linear channels, cooperative/cognitive techniques, multi-beam processing, mmWave beamforming, optical communications, MIMO systems, radio resource management, relaying, localization, spectrum monitoring, physical layer security, full duplex systems, wireless power transfer and network performance optimization. These communication activities are supported by a Software Defined Radio Lab for fast prototyping and demonstration.

The computer vision research focuses on 3D sensing and analysis with applications ranging from security and safety to assistive computer vision for health care. Specific research topics include 3D data enhancement, 2D/3D shape modelling, 3D motion analysis, face modelling and recognition. In addition to data modelling and analysis, dedicated techniques are developed for matching, filtering, classification, learning, recognition, detection and estimation. Recently, new activities have started on deep learning for 3D vision exploiting and defining new architecture for learning from 3D data. A well-equipped computer vision laboratory located in Maison du Nombre (MNO), Campus Belval, is dedicated to support these imaging and vision activities, in addition to data collection campaigns that are regularly organized for the needs of the projects.

In radar signal processing with applications in the automotive sector we develop and analyze signal processing techniques for short to mid-range radar sensing and imaging to enhance resolution and localization. Investigations into cognitive radar and their applicability in emerging coexistence scenarios are also being conducted. Recently the group has started research activity on active learning combining data-driven and model-based approaches towards creating an efficient framework for design of complex systems. It investigates the exploration-exploitation trade-offs in acquiring environment cognition and brings together some of the radar and communication activities of the group.

Summary of the group's achievements in 2017

The team recruited 13 PhD candidates and 6 research associates during the year and reached some 45 members. We conduct collaborative research with our partners SES S.A., IEE S.A. and ARTEC 3D. In addition, we are engaged in more than 15 European projects (H2020 and European Space Agency). This year's achievements include **70 publications, 4 patent filings,** and **1 start-up company.** Björn Ottersten received an **ERC Advanced grant** in 2017, the most prestigious award and grant from the European Research Council. **Two SIGCOM PhD students** graduated in 2016.

4.20 Software Verification and Validation (SVV)

Head of research group: Prof. Dr. Lionel Briand

The SVV group is both part of the SnT Centre for Security, Reliability, and Trust and the CSC research unit. The group was founded in 2012 with a FNR PEARL chair. Over the years, SVV has established research collaborations with industry partners in the automotive, satellite, aerospace, financial, and legal domains. It focuses on various aspects of software verification and validation, including requirements engineering, design-based analysis, automated testing, and runtime monitoring. SVV's goals include **both achieving scientific excellence and socio-economic impact** through partnerships. Detailed information about the group is available at svv.lu.

Summary of the group's achievements in 2017

This year's achievements include **45 publications** (excluding accepted papers, in press and to be published in 2018), many in highly reputable software engineering venues, including both conferences and journals. Several members of the department were involved in the program organization or steering committees of major conferences of the field. In addition, Lionel Briand was invited to give **five keynote addresses** (e.g., ECMFA, REFSQ) and distinguished lectures (e.g., Huawei annual STW conference). Though stepping down in 2017, Lionel Briand was until then the co-Editor in Chief of a major software engineering journal edited by Springer (Empirical Software Engineering), which has one of the highest impact factors in the field and focuses on applied, industry-relevant research. Lionel Briand received an **ERC Advanced grant** in September 2016, the most prestigious award and grant from the European Research Council, which is currently under way and is being carried out in collaboration with companies such as IEE, SES, QRA, and LuxSpace. In addition to existing ones, **four new partnerships** were started in 2017 with BGL-Banque Paribas, Clearstream, Escent, and QRA. With the acquisition of **large CORE projects**, our collaborations with SCL – the government division in charge of all legal texts in Luxembourg – and SES, have significantly increased. **Five SVV PhD students** graduated in 2017.

Three important publications in 2017

Thome, Julian; Shar, Lwin Khin; Bianculli, Domenico; Briand, Lionel, Search-driven String Constraint Solving for Vulnerability Detection**,** in Proceedings of the 39th International Conference on Software Engineering (ICSE 2017) (2017, May)

Di Nardo, Daniel; Pastore, Fabrizio; Briand, Lionel, Augmenting Field Data for Testing Systems Subject to Incremental Requirements Changes**,** in ACM Transactions on Software Engineering & Methodology (2017), 26(1), 1-40

Arora, Chetan; Sabetzadeh, Mehrdad; Briand, Lionel; Zimmer, Frank, Automated Extraction and Clustering of Requirements Glossary Terms**,** in IEEE Transactions on Software Engineering (2017), 43(10), 918-945

4.21 Systems and Control Engineering (SCE)

Head of research group: Prof. Dr. Jürgen Sachau

The Systems and Control Engineering group is affiliated to the Computer Science and Communications research unit with common labs with the Electrical Engineering. The group is devoted to systems and control technology development and demonstration for reliable large-scale grid integration of solar power systems, conversion and storage and solar-fed structures for distributed energy systems. Further Informationis available at http://sce.uni.lu/.

Summary of the group's achievements in 2017

In 2017 SCE, counted 4 members (1 professor, 1 PostDoc, 2 PhD students,. The group finished development of the hydrokinetic turbine with RWTH Aachen, and continued cooperation with FZ Jülich and the DerLab association of European laboratories. Furthermore energy economic analysis for the northpool market dynamics and supply curve decomposition came under investigation. The set of three custom-built digital power actuators for parallel grid support inverter with dedicated FPGA hardware control are used in the experimental implementation of PhD Khachatur Torchyan's research on distributed grid support and curtailment. As well, measurable curtailment of Photovoltaic-power inverters has been projected. Cooperation with the Swiss Solar Agency has been reinforced by nomination of Prof. Sachau to Eurosolar Association, awarding the European Solar Prizes at Vienna this year.

Main publications and achievements in 2017

- Haroldo de Faria Jr., DSc, **Khachatur Torchyan**, Harag Z. Margossian, PhD, **Juergen Sachau**, Prof. "Distributed generation with photovoltaic grid connected systems: connection, drivers, and obstacles," in Photovoltaic Systems: Design, Performance and Application; Nova Science Publishers, accepted for

publishing. Connection of a significant amount of photovoltaic generation in distribution networks can cause operational issues such as over-voltages and unnecessary tripping. To overcome these technical obstacles, the grid operator should reinforce the grid by implementing specific voltage and frequency control strategies, as well as protection schemes and grid code changes. A review of available control and protection strategies and grid codes is presented, together with recommendations on possible solutions to operational problems caused by PV integration.

- A.Piskun, A.Seleznev, **J.Sachau** : "Decomposition of Supply Curves in Zonal Day-Ahead Markets for Bid-Scenario Modeling" submission to IEEE Journal. The modeling of price bids submitted by generating companies in day-ahead markets is presented. The proposed algorithm is based on the decomposition of aggregated supply curves published by commercial operators. For the mixed integer optimization, constraints are introduced for capturing the logic of locational marginal pricing as well as the specific bidding behavior of suppliers. In the case study, based on available data from ATS, Russia, we evaluate the accuracy of the decomposition mode, employing reconstructed bids for simulation of day-ahead market. This approach allows for model based investigation of European and Siberian day-ahead markets and, being extendable also to nodal pricing, is showing high relevance for market analysis.
- The European Commission put forward in 2016 the Clean Energy for All Europeans Package, to keep the European Union competitive as the clean energy transition is changing global energy markets, covering energy efficiency, renewable energy, the design of the electricity market, security of electricity supply and governance rules for the Energy Union. Continuing support for implementation and monitoring of EU energy policies and programmes, the JRC Energy Security Systems and Market Unit coordiantes and supports works on energy market design, supply security and system reliability. The sabbatical aims at reinforcement of the techno-scientific progress in energy-security, complementing recent progress financed by the university, Luxembourg's network operator CREOS and the FNR, for sustainable integration in Luxembourg. In order to achieve the energyand climate targets for 2020 and beyond, for Luxemburg the works cope with the long-term energyeconomical needs until mid century:
  - accommodation of large-scale fluctuating electricity feed-in
  - transition to solar-electrical mobility & transport
  - corresponding integration of storage portfolios under techno-economical and supply-security conditions.

4.22 Team Leprévost

Head of research group: Prof. Dr. Franck Leprévost

Summary of the achievements in 2017

During 2017 Research has been conducted on the Elliptic Curve Discrete Logarithm Problem (one of the main mathematical problems underlying Public-Key

Cryptology) over finite fields. Computations were conducted to identify and interpret in an innovative way coefficients of some p-adic expansions that are necessary to address the ECDLP under some conditions. Some refinements of our 2016 results have been performed and included in a joint work between N. Bernard, P. Bouvry & F. Leprévost. The move to Belval has also led to a delay regarding the experimentation of TrueNyms (an unobservability system developed by Nicolas Bernard in the past years, and on which a series of articles were published in the last years). As a consequence, he refocused his scientific interests towards related topics at a more theoretical level. Initially motivated by investigating possible information leaks in a system like TrueNyms, he is now looking for insights on the nature of entropy, information, and uncertainty and how they flow in different kinds of systems, including (but not limited to) "learning" systems where raw information ("data") is distilled to extract meaning ("knowledge"). This direction may also lead to a book in the coming years.

Another direction was to report to the community of academic leaders the experience of the University of Luxembourg, and its fast-growing development. An article has been written and accepted for publication as a chapter of a book, and a thorough update of this chapter has been performed in 2017. The book itself will appear in 2018. In the same line of thoughts, F. Leprévost's experience gained in Russia on the 5-100 program (aiming 5 Russian universities in the top 100 in the world by 2020) has led to an article. However, this article has been expanded during 2017 and continues to be developed currently to what may ultimately become a book. For this reason and although the author has been already invited to submit its first conclusions about Russian universities by different editors, it was decided to wait for the book to gain maturity and decide then whether to publish things separately or not. This book is an on-going work, the outcome of which will be realized in 2018 at the earliest.

The main projects of publications in 2017 are:

- "The University of Luxembourg: A National Excellence Intitiative" (author: F. **Leprévost**). Accepted for publication. This article constitutes the chapter N° 9 of the book "Accelerated Universities – Ideas and Money Combine to Build Academic Excellence. Edited by Philip G. Altbach, Liz Reisberg, Jamil Salmi, and Isak Froumin. To be published by Brill (The Netherlands, http://www.brill.com) in 2018.
- "Computation around ECDLP over Fp" (authors: **F. Leprévost, N. Bernard, P. Bouvry**). Submitted.
- "From Russia with 5-100" (author: **F. Leprévost**).
- "The clash of universities" (author **F. Leprévost**). Book in progress.

4.23 Team Müller

Head of research group: Associate Prof. Dr. Volker Müller

Volker Müller is interested in the application of graph-based techniques for finding new variants of number-theoretic algorithms. He worked on the simul-

taneous Chinese Remainder problem and a possible application to the integer factorization problem. First partial results were achieved in 2017, but these require additional investigations before a possible publication.

After the end of his mandate as "Responsible of the Service Informatique de l'Université (SIU)" on 31.12.2016, he planned for 2017 the constitution of a small research group in the area of algorithmic number theory, which is unfortunately delayed due to the difficult financial situation of the university in 2017.

Since September 2017, Volker Müller is the new study director for the regular and the life-long learning track of the "Bachelor en informatique (professionnel)". Besides the regular duties of a study director, he started in late 2017 with a re-definition of the programme to better clarify the programme vision and its distinction with the new academic Bachelor in Computer Science (BICS) offered by CSC. An even stronger focus on applied and practically relevant technologies will guide the definition of the new BINFO program planned for implementation in September 2018.

Chapter 5

Organizational Structure

In March 2016 we adopted the following organizational structure of CSC.

- The department is meant to be responsible for research and education performed by its members. The head of the department is therefore responsible for both.
- The head is seconded by a vice-head, who is able to take over all the head's responsibilities whenever needed, e.g. due to temporary absence or unavailability of the head. Together, they perform the daily management of the department.
- CSC forms two sub-committees: an *education management committee* and a *research management committee*. The purpose of the education management committee is to coordinate all teaching-related activities of CSC. The purpose of the research management committee is to represent CSC in discussions and decisions with regards to research coordination and its general and financial management.
- The head of CSC is the head of these committees. The vice-head is a regular member of these committees. Further, these committees are formed by the heads of the educational programs (education management committee) and by the lab heads (research management committee).
- Besides these committees, the general CSC professors meeting is the final decision body of CSC.
- The head and vice-head are supported by a secretary and a research facilitator. The secretary supports with administrative tasks and the research facilitator provides support for managerial and financial tasks.
- The head and vice-head of CSC represent CSC at the various UL levels.

The internal communication within CSC is based on an effective communication infrastructure, based e.g. on ULI or Sharepoint. Short summaries of the CSC professors meeting and the meetings of the education management committee and research management committee is made available. Agenda points for the CSC professors meeting is labelled as *Reporting, Decision-making* and *Idea-generation*.

CSC labs organize CSC resources and competencies with a long-term view, and are governed by the following guidelines.

- There are three hierarchical levels within CSC: CSC (all members of CSC) + LAB (a substructure of CSC) + GRP (a research group consisting of a CSC professor and his team members).
  The duties, responsibilities and organization of a department and the tasks and duties of individual professors (and the employees that are hierarchically subordinate to the professor) are (partly) defined in the law and internal UL rules. CSC can delegate responsibilities to other entities (such as the management team, heads of studies, labs, heads of labs, ad-hoc groups, individuals). Research group is named after topic.
- The purpose of a LAB is at least to coordinate and distribute tasks, and to distribute money and share resources (like rooms).
  Moreover, labs can be used for PR and visibility, to represent its members within CSC, to stimulate research cooperation, to organize joint seminars, or to coordinate education in a given domain, etc.
- Labs can determine their own organisational structure.
  Every lab has a *lab head*. The lab professors can delegate responsibilities of the lab to the lab head. The lab professors can define other responsibilities (e.g. vice lab head). The lab head is (s)elected by and from the lab professors. Every lab decides on a set of rules defining the (s)election of the lab head and the internal functioning.
- One can be a member of one primary and one or more secondary LABS.
  A lab should have at least two primary members. Professors, members from their research groups and support staff can be member of a lab. The proposing professors are automatically members of a newly created lab. If a professor wants to join a lab or proposes one of his assistants as a lab member, he may request this to the professors that are currently member of the lab. The lab professors will take a motivated decision on this request. A professor can decide to not become a member of any lab. CSC can allocate resources to professors that are not member of any lab.
- Set of LABS remains stable for long term (e.g. at least 4 years).
  CSC decides on the discontinuation of existing labs and the creation of new labs. A group of professors can propose to CSC to create a new lab.
- A certain percentage of the CSC budget and of the other resources (secretaries, technical assistants, etc.) is assigned to the LABs.
  Each lab decides on how to internally distribute (the use of) the assigned resources. The structural positions for assistants are not assigned to labs, but to professors.
- At the moment, no LAB evaluation procedure is foreseen. Moreover, the guidelines for the creation and discontinuation of labs still need to be defined.

Chapter 6

Education

6.1 Doctoral Programme in Computer Science and Computer Engineering

The Doctoral programme in Computer Science and Computer Engineering (DP-CSCE) is part of the Doctoral School in Science and Engineering (DSSE). The DP-CSCE is the joint doctoral programme of the Computer Science and Communications Research Unit (CSC) and the Interdisciplinary Centre for Security, Reliability and Trust (SnT), which provides an excellent environment for pursuing doctoral studies in computer science and computer engineering at an internationally competitive level and in broad interdisciplinary application.

Candidates successfully terminating doctoral education at the DP-CSCE will be awarded a Doctoral Degree in "Informatique". The main research areas concern: Communicative Systems, Intelligent & Adaptive Systems, Security & Cryptology, and Software & Engineering.

6.2 Master in Information and Computer Sciences (MiCS)

The Master in Information and Computer Sciences (MICS) is a continuation of the Bachelor studies as a first step towards the PhD. The programme started in 2004 and was partly redesigned in 2010 in terms of profiles to provide more flexible specialisation options. The structure is as follows.

The first semester is mandatory for all. It is dedicated to the fundamentals of computer science. By the end of the first semester, the student selects courses based on one or more profiles that she/he would like to pursue. Profiles are similar to specialisations with the added benefit that multiple profiles can be realised. There are currently five profiles offered:

- Adaptive Computing
- Communication Systems
- Information Security
- Intelligent Systems
- Reliable Software Systems

The second and third semester offer specialised courses in the selected field, preparing the candidate for the Master Thesis in the fourth semester. The MICS adheres to the Bologna agreement.

In 2017 there were around 60 students from more than 20 countries in the MICS.

6.3 Master en Management de la Sécurité des Systèmes d'Information

The MSSI (Master en Management de la Sécurité des Systèmes d'Information) allows professionals to increase their knowledge and develop their skills to analyse, interpret and provide adequate solutions in the field of information security.

It is a lifelong learning Master degree programme with a well-established reputation in Luxembourg and the Greater Region. Created in 2007, together with market stakeholders, the MSSI graduates every year between 12 and 18 professionals in the field of security management. Thanks to our teaching team, composed of academics and professionals, we provide the interdisciplinary, applied and academic background (technical, managerial, legal...) required for security officers to face the challenges of nowadays security threats.

In 2017, the MSSI organized the Information Security Education Day (ISED). It is a yearly one-day event co-organized by University of Luxembourg and Luxembourg Institute of Science and Technology and sponsored by CLUSIL, CSC and SnT. ISED provides an ideal forum where academics and practitioners can learn about the different facets of a key-topic, exchange and discuss ideas, and compare experiences. In this spirit, ISED seeks to be an interdisciplinary event, open to all. The speakers have expertise in different areas covering the legal, technical and research-wise facets of the theme. 2017 theme was "Security in the realm of Big Data & Analytics".

6.4 Bachelor in Computer Science (BiCS)

The Computer Science and Communication research unit has set up a completely new academic bachelor program in computer science (BiCS) that welcomed its first promotion in september 2017. The study programme aims at bringing the theoretical and practical skills needed to successfully pursue studies in a Master programme related to Computer Science at the University of Luxembourg or any other world-class university or school.

The main strengths of the BiCS are:

- Programme designed from the international standard ACM / IEEE CS 2013.
- Pedagogy based on acquisition by practice through research and development projects.
- Scientific quality to enhance interest and strengths in science and technology for the future.
- Applied multilingualism for effective integration into the Luxembourgish or international labour market.

The complete programme dedicated to computer science brings:

- Greater focus on key skills needed for computer scientists
- More systematic consideration and implementation of the internationally-recognised standards in computer science education
- Better offer to industry and societal requirements.
- More thoughtful selection of specific types of pedagogies necessary to train highly effective computer science engineers and researchers. It mainly uses project-based learning as a signature pedagogy which is in line with the University's drive for "research-based teaching".

A R&D laboratory for BiCS students has been set up (the BiCSLab). Its objectives are to:

- Support business incubation for selected BiCS students
- Host selected BSP (Bachelor Semester Projects)
- Develop industrial collaborations
- Provide an initial R&D support structure for selected BiCS students

The BiCSLab is financed internally using the BiCS programme budget line and externally using industrial partners registration fees.

The BiCSLab axes are:

- Senseware: Software engineering for intelligent and augmented environments. Interdisciplinary (learning, robotics, virtual & augmented reality)
- Greenware: Systemic approach to resilient ecosystems (permaculture). Software & Hardware (co-)development of IT solutions for permaculture
- Software: General development tools and method for the BicsLab axes. Hosts any project on software development not included in the other axes.

The BiCS organizes an annual Scientific & Digital Challenge targeting secondary school students and secondary school teachers of scientific courses related to mathematics or computer science. Applicants have the opportunity to submit a proposal meeting the challenge objectives. The proposals are evaluated and ranked, and several prizes are distributed to the winning teams. The program is open internationally and submissions can be made in the four languages (English, French, German and Luxembourgish).

The 2017/2018 promotion (named the Alan Turing promotion) is made of 27 students selected among 60 applicants. The application file evaluation average grade was of 15.7/20, 81% have a classic high school degree, 16% are females. The countries in which the 27 accepted students did their last high school year are distributed as follows: LU 17 (63%), LU 17, FR 2, BE 1, BU 1, DE 1, ES 1, GR 1, SE 1, SY 1, US 1.

6.5 Bachelor of Engineering in Computer Science (BINFO)

The “Bachelor en informatique (professionnelle)” (BINFO) offers a practice-oriented study programme that provides the students with necessary professional skills to enter the job market after graduation, be it in the public or the private sector. The BINFO will also give students the set of basic skills and know-hows needed for a continued training and professional development during their career. Beyond technical training in practically relevant IT-related technologies, BINFO is humanly rich and offers a bilingual study programme (French, English) with classmates and instructors from all cultural backgrounds and a mobility semester abroad.

The main learning objectives of the BINFO are the following:

- Be competent in software programming and, more widely, in the methods to develop computer systems;
- Acquire a specialization in one application domain of computer science such as banking information technology or distributed applications;
- Be able to efficiently communicate orally and in writing, in French and English, in cross cultural professional environments;
- Understand how companies operate and be well prepared for professional life, through the end-of-study internship and teaching delivered by experienced practitioners;
- Be able to work autonomously, analyze and anticipate issues, propose solutions in various professional situations.

In the Winter semester 2017-2018, a total of 165 students are registered within the BINFO program (77 in the first year, 36 in the second, and 52 students in the third year). The number of BINFO graduates in 2017 was 22. More information about the programme can be found at http://binfo.uni.lu.

6.6 Certificate Smart ICT for business innovation

The purpose of this certificate is to train in a year’s time, including classes, seminars and an internship, professionals from the ICT sector who want to -further-develop their Smart ICT skills and maybe embrace new career opportunities in positions like Digital Strategy Consultant, Smart ICT Consultant, Innovation Manager, Standards Manager, Head of Innovation, Head of Digital Strategy or Entrepreneur (start-up company). The certificate aims at enhancing the skills of ICT professionals and reinforcing the position of Luxembourg in the field of Smart ICT by offering its students a broad view of Smart ICT concepts and tools at their disposal to develop their sense of innovation.

Students who successfully complete the University certificate will be able to: identify and decode the high potential of Smart ICT concepts for business and innovation; analyse the challenges of digital trust and information security; identify participants and goals in the standardisation process; and cater for the current and future issues and standardisation needs in ICT areas such as dig-

ital intelligence (ICT Governance), smart platforms (Cloud Computing, Smart Cities, Green ICT), and smart interactions (Internet of Things, Smart Cyber Physical Systems & Robotics, Big data and Analytics, Digital Trust).

Appendix A

Publication List

The publications listed in this chapter have been obtained from ORBilu, the official publication record repository of the university.

Publication Category	Quantity	Section
Book	5	A.1 (p.58)
Book Chapter	5	A.2 (p.58)
Journal	78	A.3 (p.59)
Thesis	13	A.4 (p.67)
Conference	136	A.5 (p.68)
Technical Report	8	A.6 (p.82)
Miscellaneous	22	A.7 (p.83)
Unpublished	17	A.8 (p.85)
Total	*284*	

Table A.1: Overview of publications per category

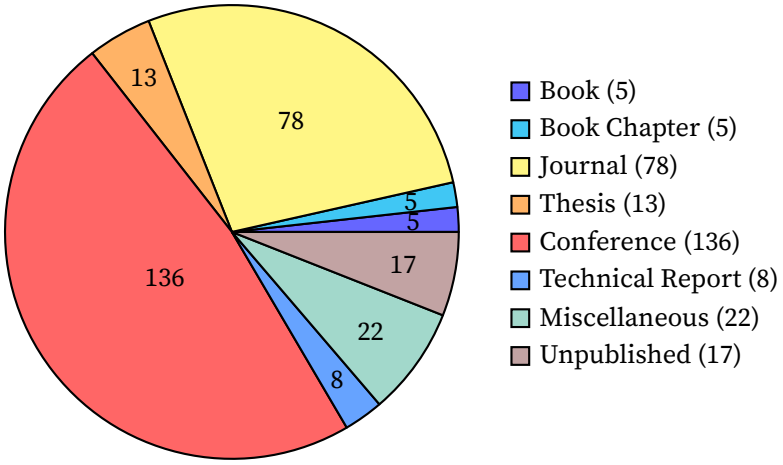


Figure A.1: Distribution of Types of Publications

A.1 Book

[1] Christoph Ewald BENZMÜLLER, Christine Lisetti, and Martin Theobald, eds. *GCAI 2017. 3rd Global Conference on Artificial Intelligence*. EasyChair Proceedings, 2017. URL: http://hdl.handle.net/10993/33610.

[2] Richard Booth, Giovanni CASINI, and Ivan Varzinczak, eds. *DARe-17 - Proceedings of the Fourth International Workshop on Defeasible and Ampliative Reasoning*. CEUR Workshop Proceedings, 2017. URL: http://hdl.handle.net/10993/33519.

[3] Marcello D'Agostino and Dov M. Gabbay. *Feasible Deduction for Realistic Agents*. College Publications, 2017. URL: http://hdl.handle.net/10993/33981.

[4] Thomas van Dijk and Christoph SCHOMMER, eds. *Proceedings of the 2nd International Workshop on Exploring Old Maps*. University of Würzburg, 2017. URL: http://hdl.handle.net/10993/31052.

[5] Adam Wyner and Giovanni CASINI, eds. *Legal Knowledge and Information Systems - JURIX 2017: The Thirtieth Annual Conference*. IOS Press BV, 2017. ISBN: 978-1-61499-837-2. URL: http://hdl.handle.net/10993/33777.

A.2 Book Chapter

[6] Cesare BARTOLINI, Robert Muthuri, and Santos Cristiana. "Using Ontologies to Model Data Protection Requirements in Workflows". In: *New Frontiers in Artificial Intelligence*. Springer International Publishing, 2017, pp. 233–248. ISBN: 978-3-319-50952-5. DOI: 10.1007/978-3-319-50953-2_17. URL: http://hdl.handle.net/10993/33856.

[7] William Derigent, Alexandre Voisin, André Thomas, Sylvain KUBLER, and Jérémy ROBERT. "Application of Measurement-Based AHP to Product-Driven System Control". In: *Service Orientation in Holonic and Multi-Agent Manufacturing*. Springer, 2017, pp. 249–258. ISBN: 978-3-319-51100-9. DOI: 10.1007/978-3-319-51100-9_22. URL: http://hdl.handle.net/10993/31978.

[8] Mike PAPADAKIS, Marinos KINTIS, Jie Zhang, Yue Jia, Yves le TRAON, and Mark Harman. "Mutation Testing Advances: An Analysis and Survey". In: *Advances in Computers*. Elsevier, 2017. URL: http://hdl.handle.net/10993/31612.

[9] Francisco Javier RODRIGUEZ LERA, Camino Fernández Llamas, Ángel Manuel Guerrero, and Vicente Matellán Olivera. "Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety". In: *Robotics - Legal, Ethical and Socioeconomic Impacts*. InTech, 2017. DOI: 10.5772/intechopen.69796. URL: http://hdl.handle.net/10993/33757.

[10] Jiangshan YU and Mark Ryan. "Chapter 7: Evaluating web PKIs". In: *Software Architecture for Big Data and the Cloud, 1st Edition, Chapter 7, June 2017*. Morgan Kaufmann, 2017. URL: http://hdl.handle.net/10993/32516.

A.3 Journal

[11] Gianmaria Ajani, Guido Boella, Luigi Di Caro, Livio ROBALDO, Llio Humphreys, Sabrina Praduroux, Piercarlo Rossi, and Andrea Violato. "The European Legal Taxonomy Syllabus: A multi-lingual, multi-level ontology framework to untangle the web of European legal terminology". In: *Applied Ontology* (2017). URL: http://hdl.handle.net/10993/30225.

[12] F.A. Armenta-Cano, A. Tchernykh, J.M. Cortes-Mendoza, R. Yahyapour, A. Yu. Drozdov, Pascal BOUVRY, D. Kliazovich, A. Avetisyan, and S. Nesmachnow. "Min_c: Heterogeneous concentration policy for energy-aware scheduling of jobs with resource contention". In: *Programming & Computer Software* 3.3 (2017), pp. 204–215. DOI: 10.1134/S0361. URL: http://hdl.handle.net/10993/34044.

[13] Arash ATASHPENDAR, Bernabé Dorronsoro, Grégoire DANOY, and Pascal BOUVRY. "A Scalable Parallel Cooperative Coevolutionary PSO Algorithm for Multi-objective Optimization". In: *Journal of Parallel & Distributed Computing* (2017). DOI: 10.1016/j.jpdc.2017.05.018. URL: http://hdl.handle.net/10993/31731.

[14] Matthias Baaz, Agata Ciabattoni, Dov M. Gabbay, Stefan Hetzl, and Daniel Weller. "Preface". In: *Journal of Logic and Computation* (2017), p. 415. DOI: 10.1093/logcom/exu076. URL: http://hdl.handle.net/10993/33980.

[15] Gabriel Barragan-Ramirez, Alejandro Estrada-Moreno, Yunior RAMIREZ CRUZ, and Juan A. Rodriguez-Velazquez. "The Simultaneous Local Metric Dimension of Graph Families". In: *Symmetry* 9.8 (2017). URL: http://hdl.handle.net/10993/35258.

[16] Giampaolo Bella, Rosario Giustolisi, Gabriele LENZINI, and Peter Y. A. RYAN. “Trustworthy exams without trusted parties”. In: *Computer and Security* 7 (2017), pp. 291–307. DOI: 10.1016/j.cose.2016.12.005. URL: http://hdl.handle.net/10993/33325.

[17] Kirstie Bellman, Jean BOTEV, Hanno Hildmann, Peter R. Lewis, Stephen Marsh, Jeremy Pitt, Ingo Scholtes, and Sven Tomforde. “Socially-Sensitive Systems Design”. In: *IEEE Technology & Society Magazine* 6.3 (2017), pp. 72–80. URL: http://hdl.handle.net/10993/32394.

[18] Christoph Ewald BENZMÜLLER. “Cut-Elimination for Quantified Conditional Logic”. In: *Journal of Philosophical Logic* 6.3 (2017), pp. 333–353. DOI: 10.1007/s10992-016-9403-0. URL: http://hdl.handle.net/10993/33608.

[19] Christoph Ewald BENZMÜLLER and David Fuenmayor. “Computer-assisted Reconstruction and Assessment of E. J. Lowe’s Modal Ontological Argument”. In: *Archive of Formal Proofs* (2017). URL: http://hdl.handle.net/10993/33920.

[20] Christoph Ewald BENZMÜLLER, Leon Weber, and Bruno Woltzenlogel Paleo. “Computer-Assisted Analysis of the Anderson-Hájek Controversy”. In: *Logica Universalis* 1.1 (2017), pp. 139–151. DOI: 10.1007/s11787-017-0160-9. URL: http://hdl.handle.net/10993/33699.

[21] Christoph Ewald BENZMÜLLER and Bruno Woltzenlogel Paleo. “Experiments in Computational Metaphysics: Gödel’s Proof of God’s Existence”. In: *Savijnanam: scientific exploration for a spiritual paradigm. Journal of the Bhaktivedanta Institute* 9 (2017), pp. 43–57. URL: http://hdl.handle.net/10993/33621.

[22] Tarek Besold, Artur d’Avila Garcez, Keith Stenning, Leon van der TORRE, and Michiel van Lambalgen. “Reasoning in Non-probabilistic Uncertainty: Logic Programming and Neural Symbolic Computing as Examples”. In: *Minds and Machines* (2017). URL: http://hdl.handle.net/10993/30739.

[23] Wouter Biesmans, Josep Balasch, Alfredo RIAL DURAN, Bart Preneel, and Ingrid Verbauwhede. “Private Mobile Pay-TV From Priced Oblivious Transfer”. In: *IEEE Transactions on Information Forensics & Security* (2017). URL: http://hdl.handle.net/10993/32011.

[24] Andrea CAPPONI, Claudio FIANDRINO, Dzmitry KLIAZOVICH, Pascal BOUVRY, and Stefano Giordano. “A Cost-Effective Distributed Framework for Data Collection in Cloud-based Mobile Crowd Sensing Architectures”. In: *IEEE Transactions on Sustainable Computing* (2017). DOI: 10.1109/TSUSC.2017.2666043. URL: http://hdl.handle.net/10993/29880.

[25] Angelo de Caro, Vincenzo IOVINO, and Adam O’Neill. “Receiver and Sender Deniable Functional Encryption”. In: *IET Information Security* (2017). DOI: 10.1049/iet-ifs.2017.0040. URL: http://hdl.handle.net/10993/31154.

[26] German CASTIGNANI, Thierry DERRMANN, Raphaël FRANK, and Thomas ENGEL. “Smartphone-based Adaptive Driving Maneuver Detection: A large-scale Evaluation Study”. In: *IEEE Transactions on Intelligent Transportation Systems* (2017). DOI: 10.1109/TITS.2016.2646760. URL: http://hdl.handle.net/10993/29552.

[27] Jeronimo Castrillon, Matthias Lieber, Sascha Klueppelholz, Marcus VOLP, Nils Asmussen, Uwe Assmann, Franz Baader, Christel Baier, Gerhard Fettweis, and Jochen Froehlich. “A Hardware/Software Stack for Heterogeneous Systems”. In: *IEEE Transactions on Multi-Scale Computing Systems* 99 (2017), p. 1. URL: http://hdl.handle.net/10993/33740.

[28] Gianluca Cena, Ivan Cibrario Bertolotti, Tingting HU, and Adriano Valenzano. “CAN With eXtensible In-Frame Reply: Protocol Definition and Prototype Implementation”. In: *IEEE Transactions on Industrial Informatics* 3.5 (2017), pp. 2436–2446. DOI: 10.1109/TII.2017.2714183. URL: http://hdl.handle.net/10993/34022.

[29] Boonyarit CHANGAIVAL, Martin ROSALIE, Grégoire DANOY, Kittichai Lavangnananda, and Pascal BOUVRY. “Chaotic Traversal (CHAT): Very Large Graphs Traversal Using Chaotic Dynamics”. In: *International Journal of Bifurcation and Chaos* 7.14 (2017), p. 1750215. DOI: 10.1142/S0218127417502157. URL: http://hdl.handle.net/10993/34230.

[30] Benoît-Michel COGLIATI, Jooyoung Lee, and Yannick Seurin. “New Constructions of MACs from (Tweakable) Block Ciphers”. In: *IACR Transactions on Symmetric Cryptology* (2017). URL: http://hdl.handle.net/10993/34599.

[31] M. Á. Conde, Lidia Sanchez-Gonzalez, Vicente Matellan-Olivera, and Francisco Javier RODRIGUEZ LERA. “Application of Peer Review Techniques in Engineering Education”. In: *International Journal of Engineering Education* (2017). URL: http://hdl.handle.net/10993/33761.

[32] Jean-Sébastien CORON. “High-Order Conversion from Boolean to Arithmetic Masking”. In: *Proceedings of CHES 2017* (2017). URL: http://hdl.handle.net/10993/34588.

[33] Jean-Sébastien CORON, Moon Sung Lee, Tancrede Lepoint, and Mehdi Tibouchi. “Zeroizing Attacks on Indistinguishability Obfuscation over CLT13”. In: *Proceedings of PKC 2017* (2017). URL: http://hdl.handle.net/10993/34589.

[34] Marcos CRAMER. “Implicit dynamic function introduction and Ackermann-like Function Theory”. In: *The IfCoLog Journal of Logics and their Applications* (2017). URL: http://hdl.handle.net/10993/33831.

[35] Mehdi Dastani, Leon van der TORRE, and Neil Yorke-Smith. “Commitments and interaction norms in organisations”. In: *Autonomous Agents & Multi-Agent Systems* 1.2 (2017), pp. 207–249. URL: http://hdl.handle.net/10993/30684.

[36] Esther David, Dov M. Gabbay, Guy Leshem, and Students of CS Ashkelon. “Logical Analysis of Cyber Vulnerability and Protection”. In: *The IfCoLog Journal of Logics and their Applications* (2017). URL: http://hdl.handle.net/10993/33979.

[37] Naipeng Dong, Hugo Jonker, and Jun PANG. “Formal modelling and analysis of receipt-free auction protocols in applied pi”. In: *Computers & Security* 5 (2017), pp. 405–432. DOI: 10.1016/j.cose.2016.09.002. URL: http://hdl.handle.net/10993/30331.

[38] Joao Duarte, Eirini Kalogeiton, Ridha SOUA, Gaetano Manzo, Maria Rita Palattella, Antonio DI MAIO, Torsten Braun, Thomas ENGEL, Leandro Villas, and Gianluca Rizzo. “A Multi-Pronged Approach to Adaptive and Context Aware Content Dissemination in VANETs”. In: *Mobile Networks and Applications* (2017), pp. 1–13. DOI: 10.1007/s11036-017-0816-y. URL: http://hdl.handle.net/10993/32964.

[39] Fabian Fagerholm, Alejandro SANCHEZ GUINEA, Hanna Mäenpää, and Jürgen Münch. “The RIGHT model for Continuous Experimentation”. In: *Journal of Systems and Software* 3 (2017), pp. 292–305. DOI: 10.1016/j.jss.2016.03.034. URL: http://hdl.handle.net/10993/33062.

[40] Sébastien FAYE, Walter BRONZI, Ibrahim Tahirou, and Thomas ENGEL. “Characterizing User Mobility Using Mobile Sensing Systems”. In: *International Journal of Distributed Sensor Networks* 3.8 (2017). DOI: 10.1177/1550147717726310. URL: http://hdl.handle.net/10993/31971.

[41] C. Fernández-Llamas, M. A. Conde, Francisco Javier RODRIGUEZ LERA, F. J. Rodríguez-Sedano, and F. García. “May I teach you? Students’ behavior when lectured by robotic vs. human teachers”. In: *Computers in Human Behavior* (2017). DOI: 10.1016/j.chb.2017.09.028. URL: http://hdl.handle.net/10993/33760.

[42] Camino Fernández-Llamas, Miguel Ángel Conde, Francisco J. Rodríguez-Sedano, Francisco Javier RODRIGUEZ LERA, and Vicente Matellán-Olivera. “Analysing the Computational Competences Acquired by K-12 Students When Lectured by Robotic and Human Teachers”. In: *International Journal of Social Robotics* (2017). DOI: 10.1007/s12369-017-0440-9. URL: http://hdl.handle.net/10993/33759.

[43] Claudio FIANDRINO, Andrea CAPPONI, Giuseppe CACCIATORE, Dzmitry KLIAZOVICH, Ulrich SORGER, Pascal BOUVRY, Burak Kantarci, Fabrizio Granelli, and Stefano Giordano. “CrowdSenSim: a Simulation Platform for Mobile Crowdsensing in Realistic Urban Environments”. In: *IEEE Access* (2017). DOI: 10.1109/ACCESS.2017.2671678. URL: http://hdl.handle.net/10993/30036.

[44] David Fuenmayor and Christoph Ewald BENZMÜLLER. “Types, Tableaus and Gödel’s God in Isabelle/HOL”. In: *Archive of Formal Proofs* (2017). URL: http://hdl.handle.net/10993/33704.

[45] Dov M. Gabbay and Lydia Rivlin. “HEAL2100: Human Effective Argumentation and Logic for the 21st Century. The next Step in the Evolution of Logic”. In: *The IfCoLog Journal of Logics and their Applications* (2017). URL: http://hdl.handle.net/10993/33976.

[46] Dov M. Gabbay and Gadi Rozenberg. “Reasoning Schemes, Expert Opinions and Critical Questions. Sex Offenders Case Study”. In: *The IfCoLog Journal of Logics and their Applications* (2017). URL: http://hdl.handle.net/10993/33977.

[47] Dov M. Gabbay, Gadi Rozenberg, and Lydia Rivlin. “Reasoning under the Influence of Universal Distortion. Sex Offenders Case Study”. In: *The IfCoLog Journal of Logics and their Applications* (2017). URL: http://hdl.handle.net/10993/33978.

[48] Loïc GAMMAITONI and Pierre KELSEN. “F-Alloy: a relational model transformation language based on Alloy”. In: *Software & Systems Modeling* (2017). URL: http://hdl.handle.net/10993/33261.

[49] Loïc GAMMAITONI, Pierre KELSEN, and Qin Ma. “Agile Validation of Model Transformations using Compound F-Alloy Specifications”. In: *Science of Computer Programming* (2017). URL: http://hdl.handle.net/10993/32533.

[50] Nicolas GUELFI, Benjamin JAHIC, and Benoit RIES. “TESMA: Requirements and Design of a Tool for Educational Programs”. In: *Information* (2017). DOI: 10.3390/info8010037. URL: http://hdl.handle.net/10993/30252.

[51] Ángel Manuel Guerrero-Higueras, Noemí DeCastro-García, Francisco Javier RODRIGUEZ LERA, and Vicente Matellán. “Empirical analysis of cyber-attacks to an indoor real time localization system for autonomous robots”. In: *Computers & Security* (2017), pp. 422–435. DOI: https://doi.org/10.1016/j.cose.2017.06.013. URL: http://hdl.handle.net/10993/33762.

[52] Thomas HARTMANN, Assaad Moawad, François FOUQUET, and Yves le TRAON. “The Next Evolution of MDE: A Seamless Integration of Machine Learning into Domain Modeling”. In: *Software & Systems Modeling* (2017). DOI: 10.1007/s10270-017-0600-2. URL: http://hdl.handle.net/10993/31801.

[53] Ross Horne, Sjouke MAUW, and Alwen Tiu. “Semantics for specialising attack trees based on linear logic”. In: *Fundamenta Informaticae* 3.1 (2017), pp. 57–86. DOI: 10.3233/FI-2017-1531. URL: http://hdl.handle.net/10993/34365.

[54] Vincenzo IOVINO, Qiang Tang, and Karol Zebrowski. “On the power of Public-key Function-Private Functional Encryption”. In: *IET Information Security* (2017). URL: http://hdl.handle.net/10993/33544.

[55] Süleyman Kardaş and Ziya Alper GENÇ. “Security attacks and enhancements to chaotic map-based RFID authentication protocols”. In: *Wireless Personal Communications* (2017). DOI: 10.1007/s11277-017-4912-x. URL: http://hdl.handle.net/10993/33215.

[56] Emmanuel KIEFFER, Grégoire DANOY, Pascal BOUVRY, and Anass Nagih. “A new modeling approach for the biobjective exact optimization of satellite payload configuration”. In: *International Transactions in Operational Research* (2017). URL: http://hdl.handle.net/10993/30386.

[57] Marinos KINTIS, Mike PAPADAKIS, Yue Jia, Nicos Malevris, Yves le TRAON, and Mark Harman. “Detecting Trivial Mutant Equivalences via Compiler Optimisations”. In: *IEEE Transactions on Software Engineering* (2017). DOI: 10.1109/TSE.2017.2684805. URL: http://hdl.handle.net/10993/31623.

[58] Patrick KOBOU NGANI, Jean-Régis HADJI-MINAGLOU, Emmanuel de Jaeger, and Ulrich SORGER. “A New Synchronization Method for Three - phase Grid - tied LC-Filtered Voltage Source Inverters”. In: *International Journal of Emerging Engineering Research and Technology* 5.5 (2017), pp. 7–15. URL: http://hdl.handle.net/10993/32937.

[59] Arief Koesdwiady, Ridha SOUA, Fakhri Karray, and Mohamed said Kamel. “Recent Trends in Driver Safety Monitoring Systems: State of the Art and Challenges”. In: *IEEE Transactions on Vehicular Technology* 6.6 (2017), pp. 4550–4563. DOI: 10.1109/TVT.2016.2631604. URL: http://hdl.handle.net/10993/33108.

[60] Sylvain KUBLER, Jérémy ROBERT, Kary Främling, Ahmed Hefnawy, Chantal Cherifi, and Abdelaziz Bouras. “Open IoT Ecosystem for Sporting Event Management”. In: *IEEE Access* 5.1 (2017), pp. 7064–7079. DOI: 10.1109/ACCESS.2017.2692247. URL: http://hdl.handle.net/10993/31972.

[61] Sylvain KUBLER, Jérémy ROBERT, Jürgen Umbrich, Sebastian Neumaier, and Yves le TRAON. “Comparison of metadata quality in open data portals using the Analytic Hierarchy Process”. In: *Government Information Quarterly* (2017). URL: http://hdl.handle.net/10993/33328.

[62] Jérome Lang, Gabriella Pigozzi, Marija Slavkovik, Leon van der TORRE, and Srdjan Vesic. “A partial taxonomy of judgment aggregation rules and their properties”. In: *Social Choice and Welfare* 8.2 (2017), pp. 327–356. DOI: 10.1007/s00355-016-1006-8. URL: http://hdl.handle.net/10993/33985.

[63] Jean-Luis Laredo, Frédéric Guinand, Olivier Damien, and Pascal BOUVRY. “Load Balancing at the Edge of Chaos: How Can Self-Organized Criticality Lead to Energy-Efficient Computing”. In: *IEEE Transactions on Parallel & Distributed Systems* 8 (2017), pp. 517–529. DOI: 10.1109/TPDS.2016.2582160. URL: http://hdl.handle.net/10993/30183.

[64] Magdalena Lemanska, Alberto Rodríguez-Velázquez, and Rolando TRUJILLO RASUA. “Similarities and Differences Between the Vertex Cover Number and the Weakly Connected Domination Number of a Graph”. In: *Fundamenta Informaticae* 2.3 (2017), pp. 273–287. URL: http://hdl.handle.net/10993/31192%20and%20http://hdl.handle.net/10993/32348.

[65] Li LI, Tegawendé François d Assise BISSYANDE, Mike PAPADAKIS, Siegfried Rasthofer, Alexandre BARTEL, Damien Octeau, Jacques KLEIN, and Yves le TRAON. “Static Analysis of Android Apps: A Systematic Literature Review”. In: *Information and Software Technology* (2017). URL: http://hdl.handle.net/10993/31636.

[66] Li LI, Daoyuan LI, Tegawendé François d Assise BISSYANDE, Jacques KLEIN, Haipeng Cai, David Lo, and Yves le TRAON. “On Locating Malicious Code in Piggybacked Android Apps”. In: *Journal of Computer Science & Technology* (2017). DOI: 10.1007/s11390-017-1786-z. URL: http://hdl.handle.net/10993/33426.

[67] Li LI, Daoyuan LI, Tegawendé François d Assise BISSYANDE, Jacques KLEIN, Yves le TRAON, David Lo, and Lorenzo Cavallaro. “Understanding Android App Piggybacking: A Systematic Study of Malicious Code Grafting”. In: *IEEE Transactions on Information Forensics & Security* (2017). URL: http://hdl.handle.net/10993/29474.

[68] Beishui Liao, Nir Oren, Leon van der TORRE, and Serena Villata. “Prioritized Norms in Formal Argumentation”. In: *Journal of Logic & Computation* 4 (2017). URL: http://hdl.handle.net/10993/33988.

[69] Lemanska Magdalena, Rodríguez-Velázquez Juan Alberto, and Rolando TRUJILLO RASUA. “Similarities and Differences Between the Vertex Cover Number and the Weakly Connected Domination Number of a Graph”. In: *Fundamenta Informaticae* 2.3 (2017), pp. 273–287. URL: http://hdl.handle.net/10993/32348.

[70] Steve Muller, Carlo Harpes, Yves le TRAON, Sylvain Gombault, and Jean-Marie Bonnin. “Efficiently computing the likelihoods of cyclically interdependent risk scenarios”. In: *Computers & Security* 4 (2017), pp. 59–68. DOI: 10.1016/j.cose.2016.09.008. URL: http://hdl.handle.net/10993/33377.

[71] Dat Ba Nguyen, Abdalghani Abujabal, Khanh Tran, Martin THEOBALD, and Gerhard Weikum. “Query-Driven On-The-Fly Knowledge Base Construction”. In: *Proceedings of the VLDB Endowment* 1.1 (2017), pp. 66–79. URL: http://hdl.handle.net/10993/34035.

[72] Xavier PARENT and Leon van der TORRE. “Detachment in Normative Systems: Examples, inference Patterns, Properties”. In: *The IfCoLog Journal of Logics and their Applications* 4.9 (2017), pp. 2295–3039. URL: http://hdl.handle.net/10993/33555.

[73] Célia da Costa Peirera, Andrea G. B. Tettamanzi, Serena Villata, Beishui Liao, Alessandra Malerba, Antonino Rotolo, and Leon van der TORRE. “Handling Norms in Multi-Agent System by Means of Formal Argumentation”. In: *The IfCoLog Journal of Logics and their Applications* (2017). URL: http://hdl.handle.net/10993/34118.

[74] Léo Paul PERRIN and Aleksei UDOVENKO. “Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog”. In: *IACR Transactions on Symmetric Cryptology* 6.2 (2017), pp. 99–124. DOI: 10.13154/tosc.v2016.i2.99-124. URL: http://hdl.handle.net/10993/29887.

[75] Gabriella Pigozzi and Leon van der TORRE. “Multiagent Deontic Logic and its Challenges from a Normative Systems Perspective”. In: *The IfCoLog Journal of Logics and their Applications* (2017), pp. 2929–2993. URL: http://hdl.handle.net/10993/34023.

[76] Maryam Pouryazdan, Claudio Fiandrino, Burak Kantarci, Tolga Soyata, Dzmitry Kliazovich, and Pascal BOUVRY. “Intelligent Gaming for Mobile Crowd-Sensing Participants to Acquire Trustworthy Big Data in the Internet of Things”. In: *IEEE Access* 5 (2017), pp. 22209–22223. DOI: 10.1109/ACCESS.2017.2762238. URL: http://hdl.handle.net/10993/34041.

[77] Vincent RAHLI and Mark Bickford. “Validating Brouwer’s Continuity Principle for Numbers Using Named Exceptions”. In: *Mathematical Structures in Computer Science* (2017). URL: http://hdl.handle.net/10993/33894.

[78] Vincent RAHLI, David Guaspari, Mark Bickford, and Robert Constable. “EventML: Specification, Verification, and Implementation of Crash-Tolerant State Machine Replication Systems”. In: *Science of Computer Programming* (2017). DOI: 10.1016/j.scico.2017.05.009. URL: http://hdl.handle.net/10993/33892.

[79] Alfredo RIAL DURAN. “Issuer-Free Oblivious Transfer with Access Control Revisited”. In: *Information Processing Letters* (2017). URL: http://hdl.handle.net/10993/32010.

[80] Livio ROBALDO and Xin Sun. “On the Complexity of Input/Output Logic”. In: *Journal of Applied Logic* (2017). URL: http://hdl.handle.net/10993/33477.

[81] Livio ROBALDO and Xin Sun. “Reified Input/Output logic: Combining Input/Output logic and Reification to represent norms coming from existing legislation”. In: *Journal of Logic & Computation* (2017). DOI: https://doi.org/10.1093/logcom/exx009. URL: http://hdl.handle.net/10993/31378.

[82] Christoph SCHOMMER. “Q&A with Data Scientists: Christopher Schommer”. In: *Operational Database Management Systems* (2017). URL: http://hdl.handle.net/10993/29518.

[83] Xin Sun and Livio ROBALDO. “Norm-based deontic logic for access control, some computational results”. In: *Future Generation Computer Systems* (2017). URL: http://hdl.handle.net/10993/29859.

[84] Bogdan TOADER, François SPRUMONT, Sébastien FAYE, Francesco VITI, and Mioara Popescu. “Usage of Smartphone Data to Derive an Indicator for Collaborative Mobility between Individuals”. In: *ISPRS International Journal of Geo-Information* 6.3 (2017), p. 62. DOI: 10.3390/ijgi6030062. URL: http://hdl.handle.net/10993/29952.

[85] Leon van der TORRE and Srdjan Vesic. “The Principle-Based Approach to Abstract Argumentation Semantics”. In: *The IfCoLog Journal of Logics and their Applications* (2017). URL: http://hdl.handle.net/10993/33989.

[86] Xinli Yang, David Lo, Li LI, Xin Xia, Tegawendé François d Assise BISSYANDE, and Jacques KLEIN. “Comprehending Malicious Android Apps By Mining Topic-Specific Data Flow Signatures”. In: *Information and Software Technology* (2017). URL: http://hdl.handle.net/10993/31608.

[87] Ilsun You, Gabriele LENZINI, and Alfredo de Santis. *Insider Threats to Information Security, Digital Espionage, and Counter-Intelligence*. 2017. DOI: 10.1109/JSYST.2017.2658258. URL: http://hdl.handle.net/10993/31532.

[88] Jiangshan YU, Mark Ryan, and Cas Cremers. “DECIM: Detecting Endpoint Compromise In Messaging”. In: *IEEE Transactions on Information Forensics & Security* (2017). URL: http://hdl.handle.net/10993/32515.

A.4 Thesis

[89] Javed Ahmed. “Contextual Integrity and Tie Strength in Online Social Networks: Social Theory, User Study, Ontology, and Validation”. PhD thesis. University of Luxembourg, Luxembourg City, Luxembourg, 2017. URL: http://hdl.handle.net/10993/32806.

[90] Diego Agustin AMBROSSIO. “Non-Monotonic Logics for Access Control: Delegation Revocation and Distributed Policies”. PhD thesis. University of Luxembourg, Luxembourg, 2017. URL: http://hdl.handle.net/10993/31864.

[91] Guillaume BRAU. “Integration of the analysis of non-functional properties in Model-Driven Engineering for embedded systems”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2017. URL: http://hdl.handle.net/10993/30827.

[92] Walter BRONZI. “Enhancing Mobility Applications Through Bluetooth Communications”. PhD thesis. University of Luxembourg, Luxembourg, 2017. URL: http://hdl.handle.net/10993/34231.

[93] Massimo CHENAL. “Key-Recovery Attacks Against Somewhat Homomorphic Encryption Schemes”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2017. URL: http://hdl.handle.net/10993/31450.

[94] Afonso DELERUE ARRIAGA. “Private Functional Encryption – Hiding What Cannot Be Learned Through Function Evaluation”. PhD thesis. University of Luxembourg, Luxembourg, 2017. URL: http://hdl.handle.net/10993/29922.

[95] Dumitru-Daniel DINU. “Efficient and Secure Implementations of Lightweight Symmetric Cryptographic Primitives”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2017. URL: http://hdl.handle.net/10993/33803.

[96] Loïc GAMMAITONI. “On the Use of Alloy in Engineering Domain Specific Modeling Languages”. PhD thesis. University of Luxembourg, Luxembourg, 2017. URL: http://hdl.handle.net/10993/33322.

[97] Alessandra Malerba. “Interpretive Interactions among Legal Systems and Argumentation Schemes”. PhD thesis. University of Luxembourg, Luxembourg, 2017. URL: http://hdl.handle.net/10993/32361.

[98] Léo Paul PERRIN. “Cryptanalysis, Reverse-Engineering and Design of Symmetric Cryptographic Algorithms”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2017. URL: http://hdl.handle.net/10993/31195.

[99] Marjan SKROBOT. “On Composability and Security of Game-based Password-Authenticated Key Exchange”. PhD thesis. University of Luxembourg, Luxembourg, 2017. URL: http://hdl.handle.net/10993/30745.

[100] Qixia YUAN. “Computational Methods for Analysing Long-run Dynamics of Large Biological Networks”. PhD thesis. University of Luxembourg, Luxembourg, 2017. URL: http://hdl.handle.net/10993/33749.

[101] Marc van ZEE. *Rational Architecture: Reasoning about Enterprise Dynamics*. 2017. URL: http://hdl.handle.net/10993/32517.

A.5 Conference

[102] Michael Backes, Mathias Humbert, Jun PANG, and Yang Zhang. “walk2friends: Inferring Social Links from Mobility Profiles”. In: *Proceedings of the 24th ACM International Conference on Computer and Communications Security*. ACM Press, 2017, pp. 1943–1957. URL: http://hdl.handle.net/10993/32748.

[103] Thaís Bardini Idalino, Dayana PIERINA BRUSTOLIN SPAGNUELO, and Jean Everson Martina. “Private Verification of Access on Medical Data: An Initial Study”. In: *Private Verification of Access on Medical Data: An Initial Study*. 2017. URL: http://hdl.handle.net/10993/32764.

[104] Cesare BARTOLINI, Andra GIURGIU, Gabriele LENZINI, and Livio ROBALDO. “Towards legal compliance by correlating Standards and Laws with a semi-automated methodology”. In: *Communications in Computer and Information Science*. Springer International Publishing, 2017, pp. 47–62. ISBN: 978-3-319-67467-4. DOI: 10.1007/978-3-319-67468-1_4. URL: http://hdl.handle.net/10993/34476.

[105] Amine Benelallam, Thomas HARTMANN, Ludovic MOULINE, François FOUQUET, Johann Bourcier, Olivier Barais, and Yves le TRAON. “Raising Time Awareness in Model-Driven Engineering”. In: *2017 ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems*. Springer, 2017, pp. 181–188. ISBN: 978-1-5386-3492-9. DOI: 10.1109/MODELS.2017.11. URL: http://hdl.handle.net/10993/32738.

[106] Christoph Ewald BENZMÜLLER. “Recent Successes with a Meta-Logical Approach to Universal Logical Reasoning (Extended Abstract)”. In: *Formal Methods: Foundations and Applications - 20th Brazilian Symposium SBMF 2017, Recife, Brazil, November 29 - December 1, 2017, Proceedings*. Springer, 2017, pp. 7–11. ISBN: 978-3-319-70847-8. DOI: 10.1007/978-3-319-70848-5_2. URL: http://hdl.handle.net/10993/33609.

[107] Christoph Ewald BENZMÜLLER, Alexander Steen, and Max Wisniewski. “Leo-III Version 1.1 (System description)”. In: *IWIL Workshop and LPAR Short Presentations*. EasyChair, 2017, p. 16. URL: http://hdl.handle.net/10993/33703.

[108] Alexei BIRYUKOV, Joan Daemen, Stefan Lucks, and Serge Vaudenay. “Topics and Research Directions for Symmetric Cryptography”. In: *Proceedings of Early Symmetric Crypto workshop, 2017*. University of Luxembourg, 2017, p. 4. ISBN: 978-99959-814-2-6. URL: http://hdl.handle.net/10993/30953.

[109] Alexei BIRYUKOV, Dumitru-Daniel DINU, and Yann le CORRE. “Side-Channel Attacks meet Secure Network Protocols”. In: *Applied Cryptography and Network Security - 15th International Conference, ACNS 2017, Kanazawa, Japan, July 10-12, 2017. Proceedings*. Springer Verlag, 2017, pp. 435–454. DOI: 10.1007/978-3-319-61204-1_22. URL: http://hdl.handle.net/10993/31797.

[110] Gadare Bloom, Gianluca Cena, Ivan Cibrario Bertolotti, Tingting HU, and Adriano Valenzano. “Optimized event notification in CAN through in-frame replies and Bloom filters”. In: *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*. IEEE, 2017, pp. 1–10. ISBN: 978-1-5090-5788-7. DOI: 10.1109/WFCS.2017.7991963. URL: http://hdl.handle.net/10993/34020.

[111] Gedare Bloom, Gianlua Cena, Ivan Cibrario Bertolotti, Tingting HU, and Adriano Valenzano. “Supporting Security Protocols on CAN-Based Networks”. In: *2017 IEEE 18th International Conference on Industrial Technology (ICIT2017)*. 2017, pp. 1334–1339. ISBN: 978-1-5090-5320-9. DOI: 10.1109/ICIT.2017.7915557. URL: http://hdl.handle.net/10993/29920.

[112] Brandon Bohrer, Vincent RAHLI, Ivana VUKOTIC, Marcus VOLP, and Andre Platzer. “Formally Verified Differential Dynamic Logic”. In: *CPP 2017*. 2017. URL: http://hdl.handle.net/10993/29216.

[113] Jean BOTEV and Steffen ROTHKUGEL. “High-Precision Gestural Input for Immersive Large-Scale Distributed Virtual Environments”. In: *Proceedings of the 8th ACM Multimedia Systems Conference (MMSys)*. 2017. DOI: 10.1145/3083207.3083209. URL: http://hdl.handle.net/10993/31478.

[114] Jean BOTEV, Steffen ROTHKUGEL, and Joe Mayer. “Contour Drawing and Detection for Collaborative Context-Aware Mobile Training and Exploration”. In: *Proceedings of the 16th World Conference on Mobile and Contextual Learning (mLearn)*. 2017. DOI: 10.1145/3136907.3136910. URL: http://hdl.handle.net/10993/32871.

[115] Pascal BOUVRY, Serge Chaumette, Grégoire DANOY, Gilles Guerrini, Gilles Jurquet, Achim Kuwertz, Wilmuth Müller, Martin ROSALIE, Jennifer Sander, and Florian Segor. “ASIMUT project: Aid to SItuation Management based on MUltimodal, MUltiUAVs, MUltilevel acquisition Techniques”. In: *DroNet’17 Proceedings of the 3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications*. ACM, 2017, pp. 17–20. ISBN: 978-1-4503-4960-4. DOI: 10.1145/3086439.3086445. URL: http://hdl.handle.net/10993/31477.

[116] Guillaume BRAU, Nicolas NAVET, and Jérôme Hugues. “Heterogeneous models and analyses in the design of real-time embedded systems - an avionic case-study”. In: *25th International Conference on Real-Time Networks and Systems, Grenoble 4-6 October 2017*. ACM, 2017, pp. 168–177. ISBN: 978-1-4503-5286-4. DOI: 10.1145/3139258.3139281. URL: http://hdl.handle.net/10993/34016.

[117] Matthias BRUST, Grégoire DANOY, Pascal BOUVRY, Dren GASHI, Himadri Pathak, and Mike P. Goncalves. “Defending Against Intrusion of Malicious UAVs with Networked UAV Defense Swarms”. In: *42nd IEEE Conference on Local Computer Networks*. IEEE Computer Society, 2017. DOI: 10.1109/LCN.Workshops.2017.71. URL: http://hdl.handle.net/10993/33618.

[118] Matthias BRUST, Maciej ZURAD, Laurent Philippe Hentges, Leandro Gomes, Grégoire DANOY, and Pascal BOUVRY. “Target Tracking Optimization of UAV Swarms Based on Dual-Pheromone Clustering”. In: *CYBCONF 2017-12-13 09:39:53 +0000 2017-12-13 09:39:53 +0000*. IEEE, 2017. URL: http://hdl.handle.net/10993/33615.

[119] Giuseppe Cacciatore, Claudio FIANDRINO, Dzmitry KLIAZOVICH, Fabrizio Granelli, and Pascal BOUVRY. “Cost analysis of Smart Lighting Solutions for Smart Cities”. In: *IEEE International Conference on Communications (ICC), Paris, France, 2017*. 2017. URL: http://hdl.handle.net/10993/29594.

[120] Guido CANTELMO, Francesco VITI, and Thierry DERRMANN. “Effectiveness of the Two-Step Dynamic Demand Estimation model on large networks”. In: *Proceedings of 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)* (2017). DOI: 10.1109/MTITS.2017.8005697. URL: http://hdl.handle.net/10993/32905.

[121] Andrea CAPPONI, Claudio FIANDRINO, Dzmitry KLIAZOVICH, Pascal BOUVRY, and Stefano Giordano. “Energy Efficient Data Collection in Opportunistic Mobile Crowdsensing Architectures for Smart Cities”. In: *3rd IEEE INFOCOM Workshop on Smart Cites and Urban Computing*. 2017. URL: http://hdl.handle.net/10993/30106.

[122] Giovanni CASINI and Thomas Meyer. “Belief Change in a Preferential Non-Monotonic Framework”. In: *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence*. International Joint Conferences on Artificial Intelligence, 2017, pp. 929–935. ISBN: 978-0-9992411-0-3. DOI: 10.24963/ijcai.2017/129. URL: http://hdl.handle.net/10993/31865.

[123] Boonyarit CHANGAIVAL and Martin ROSALIE. “Exploring chaotic dynamics by partition of bifurcation diagram”. In: *Proceeding of Workshop on Advance in Nonlinear Complex Systems and Applications (WANCSA)*. 2017, pp. 7–8. URL: http://hdl.handle.net/10993/31707.

[124] Daewoong Cho, Javid Taheri, Albert Y. Zomaya, and Pascal BOUVRY. “Real-Time Virtual Network Function (VNF) Migration toward Low Network Latency in Cloud Environments”. In: *IEEE 10th International Conference on Cloud Computing (CLOUD), 2017*. IEEE, 2017. DOI: 10.1109/CLOUD.2017.118. URL: http://hdl.handle.net/10993/34040.

[125] Ivan Cibrario Bertolotti, Tingting HU, and Gilda Ghafour Zadeh Kashani. “A Low-Overhead Framework for Inexpensive Embedded Control Systems”. In: *Proc. 12th International Conference on Digital Telecommunications (ICDT2017)*. 2017, pp. 7–12. URL: http://hdl.handle.net/10993/34021.

[126] Ivan Cibrario Bertolotti, Tingting HU, and Nicolas NAVET. “Model-based design languages: A case study”. In: *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*. IEEE, 2017, pp. 1–6. ISBN: 978-1-5090-5788-7. DOI: 10.1109/WFCS.2017.7991964. URL: http://hdl.handle.net/10993/34019.

[127] Vinicius Vielmo Cogo, Alysson Bessani, Francisco M. Couto, Margarida Gama-Carvalho, Maria FERNANDES, and Paulo ESTEVES VERISSIMO. “How can photo sharing inspire sharing genomes?” In: *11th International Conference on Practical Applications of Computational Biology & Bioinformatics 2017*. 2017. URL: http://hdl.handle.net/10993/34970.

[128] Gary Philippe CORNELIUS, Nico HOCHGESCHWENDER, Holger VOOS, Miguel Angel OLIVARES MENDEZ, Patrice Caire, Marcus VOLP, and Paulo ESTEVES VERISSIMO. “A Perspective of Security for Mobile Service Robots”. In: *Iberian Robotics Conference, Seville, Spain, 2017*. 2017. URL: http://hdl.handle.net/10993/32938.

[129] Jorge M. Cortes-Mendoza, Andrei Tchernykh, Alexander Feoktistov, Pascal BOUVRY, and Loïc Didelot. “Load-Aware Strategies for Cloud-Based VoIP Optimization with VM Startup Prediction”. In: *IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), 2017*. IEEE, 2017. DOI: 10.1109/IPDPSW.2017.73. URL: http://hdl.handle.net/10993/34043.

[130] Marcos CRAMER and Giovanni CASINI. “Postulates for Revocation Schemes”. In: *Principles of Security and Trust. Proceedings of the 6th International Conference POST 2017*. Springer, 2017, pp. 232–252. ISBN: 978-3-662-54454-9. URL: http://hdl.handle.net/10993/29413.

[131] Thierry DERRMANN, Raphaël FRANK, Thomas ENGEL, and Francesco VITI. “How Mobile Phone Handovers reflect Urban Mobility: A Simulation Study”. In: *Proceedings of the 5th IEEE Conference on Models and Technologies for Intelligent Transportation Systems.* 2017. URL: http://hdl.handle.net/10993/31772.

[132] Thierry DERRMANN, Raphaël FRANK, Francesco VITI, and Thomas ENGEL. “Estimating Urban Road Traffic States Using Mobile Network Signaling Data”. In: *Abstract book of the 20th International Conference on Intelligent Transportation Systems* (2017). URL: http://hdl.handle.net/10993/31779.

[133] Yvo Desmedt, Vincenzo IOVINO, Giuseppe Persiano, and Ivan Visconti. “Controlled Homomorphic Encryption: Definition and Construction”. In: *FC 2017 International Workshops - WAHC’17 - 5th Workshop on Encrypted Computing and Applied Homomorphic Cryptography*. 2017. URL: http://hdl.handle.net/10993/29852.

[134] Xavier Devroey, Gilles Perrouin, Mike PAPADAKIS, Axel Legay, Pierre-Yves Schobbens, and Patrick Heymans. “Automata Language Equivalence vs. Simulations for Model-based Mutant Equivalence: An Empirical Evaluation”. In: *10th IEEE International Conference on Software Testing, Verification and Validation (ICST 2017)*. 2017. URL: http://hdl.handle.net/10993/29778.

[135] Antonio DI MAIO, Ridha SOUA, Maria Rita Palattella, Thomas ENGEL, and Gianluca Rizzo. “A centralized approach for setting floating content parameters in VANETs”. In: *A centralized approach for setting floating content parameters in VANETs*. 2017. DOI: 10.1109/CCNC.2017.7983220. URL: http://hdl.handle.net/10993/32963.

[136] Maria FERNANDES, Jérémie DECOUCHANT, Francisco M. Couto, and Paulo ESTEVES VERISSIMO. “Cloud-Assisted Read Alignment and Privacy”. In: *11th International Conference on Practical Applications of Computational Biology & Bioinformatics 2017*. 2017. URL: http://hdl.handle.net/10993/34971.

[137] Christian FRANCK and Johann GROSZSCHÄDL. “Efficient Implementation of Pedersen Commitments Using Twisted Edwards Curves”. In: *Mobile, Secure, and Programmable Networking - Third International Conference, {MSPN} 2017, Paris, France, June 29-30, 2017, Revised Selected Papers*. Springer, 2017. ISBN: 978-3-319-67806-1. DOI: 10.1007/978-3-319-67807-8. URL: http://hdl.handle.net/10993/33705.

[138] David Fuenmayor and Christoph Ewald BENZMÜLLER. “Automating Emendations of the Ontological Argument in Intensional Higher-Order Modal Logic”. In: *KI 2017: Advances in Artificial Intelligence 40th Annual German Conference on AI*. Springer International Publishing AG, 2017. ISBN: 978-3-319-67189-5. DOI: 10.1007/978-3-319-67190-1_9. URL: http://hdl.handle.net/10993/33693.

[139] David Fuenmayor, Christoph Ewald BENZMÜLLER, Alexander Steen, and Max Wsinieswki. “The Virtues of Automated Theorem Proving in Metaphysics — A Case Study: E. J. Lowe’s Modal Ontological Argument”. In: *The 2nd World Congress on Logic and Religion – Book of Abstracts*. Instytut Filozofii Uniwersytetu Warszawskiego, 2017, p. 18. ISBN: 978-83-938107-9-6. URL: http://hdl.handle.net/10993/33916.

[140] Olga GADYATSKAYA, Jhawar Ravi, Sjouke MAUW, Rolando TRUJILLO RASUA, and A.C. Willemse Tim. “Refinement-Aware Generation of Attack Trees”. In: *Security and Trust Management - 13th International Workshop*. Springer, 2017, pp. 164–179. ISBN: 978-3-319-68062-0. URL: http://hdl.handle.net/10993/32678.

[141] Jyoti Gajrani, Li LI, Vijay Laxmi, Meenakshi Tripathi, Manoj Singh Gaur, and Mauro Conti. “POSTER: Detection of Information Leaks via Reflection in Android Apps”. In: *The 2017 ACM on Asia Conference on Computer and Communications Security (AsiaCCS 2017)*. 2017. URL: http://hdl.handle.net/10993/31609.

[142] Ziya Alper GENÇ, Süleyman Kardaş, and Kiraz. “Examination of a New Defense Mechanism: Honeywords”. In: *Proceedings of the 11th WISTP International Conference on Information Security Theory and Practice*. Springer, 2017. URL: http://hdl.handle.net/10993/33248.

[143] Ziya Alper GENÇ, Gabriele LENZINI, and Peter Y. A. RYAN. “The Cipher, the Random and the Ransom: A Survey on Current and Future Ransomware”. In: *Advances in Cybersecurity 2017*. University of Maribor Press, 2017. ISBN: 978-961-286-114-8. URL: http://hdl.handle.net/10993/32574.

[144] Sepideh Ghanavati, Marc van ZEE, and Floris Bex. “Argumentation-based Methodology for Goal-oriented Requirements Language (GRL)”. In: *Proceedings of the 10th International i* Workshop co-located with the 29th International Conference on Advanced Information Systems Engineering (CAiSE 2017), Essen, Germany, June 12-13, 2017.* 2017. URL: http://hdl.handle.net/10993/33984.

[145] J. Ginés, F. Martín, V. Matellán, Francisco Javier RODRIGUEZ LERA, and J. Balsa. “Dynamics maps for long-term autonomy”. In: *2017 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC)*. IEEE, 2017. ISBN: 978-1-5090-6233-1. DOI: 10.1109/ICARSC.2017.7964057. URL: http://hdl.handle.net/10993/33756.

[146] Rosario Giustolisi, Vincenzo IOVINO, and Gabriele LENZINI. “Privacy-Preserving Verifiability: A Case for an Electronic Exam Protocol”. In: *Privacy-Preserving Verifiability: A Case for an Electronic Exam Protocol*. SCITEPRESS, 2017. URL: http://hdl.handle.net/10993/31771.

[147] Tobias Gleißner, Alexander Steen, and Christoph Ewald BENZMÜLLER. “Theorem Provers for Every Normal Modal Logic”. In: *LPAR-21. 21st International Conference on Logic for Programming, Artificial Intelligence and Reasoning*. EasyChair, 2017, pp. 14–30. URL: http://hdl.handle.net/10993/33698.

[148] Christian GREVISSE, Jean BOTEV, and Steffen ROTHKUGEL. “An Extensible and Lightweight Modular Ontology for Programming Education”. In: *Advances in Computing - 12th Colombian Conference, CCC 2017, Cali, Colombia, September 19-22, 2017, Proceedings*. Springer, 2017, pp. 358–371. DOI: 10.1007/978-3-319-66562-7_26. URL: http://hdl.handle.net/10993/31932.

[149] Christian GREVISSE, Jean BOTEV, and Steffen ROTHKUGEL. “Integration of Learning Material into an Advanced Project-Based Learning Support Platform”. In: *INTED 2017 Proceedings*. 2017. URL: http://hdl.handle.net/10993/29506.

[150] Christian GREVISSE, Jean BOTEV, and Steffen ROTHKUGEL. “Learning Resource Management through Semantic Annotation Features in Popular Authoring Software”. In: *ICERI 2017 Proceedings*. IATED, 2017. URL: http://hdl.handle.net/10993/33056.

[151] Christian GREVISSE, Jean BOTEV, and Steffen ROTHKUGEL. “Yactul: An Extensible Game-Based Student Response Framework for Active Learning”. In: *Ponencias del XVIII Encuentro Internacional Virtual Educa, Colombia 2017*. 2017. URL: http://hdl.handle.net/10993/31506.

[152] Siwen GUO and Christoph SCHOMMER. “Embedding of the Personalized Sentiment Engine PERSEUS in an Artificial Companion”. In: *International Conference on Companion Technology, Ulm 11-13 September 2017*. IEEE, 2017. URL: http://hdl.handle.net/10993/32525.

[153] Thomas HARTMANN, François FOUQUET, Matthieu JIMENEZ, Romain Rouvoy, and Yves le TRAON. “Analyzing Complex Data in Motion at Scale with Temporal Graphs”. In: *Proceedings of the 29th International Conference on Software Engineering and Knowledge Engineering*. 2017. URL: http://hdl.handle.net/10993/31800.

[154] Ahmed Hefnawy, Taha Elhariri, Abdelaziz Bouras, Chantal Cherifi, Jérémy ROBERT, Sylvain Kubler, and Kary Frmling. “Combined Use of Lifecycle Management and IoT in Smart Cities”. In: *Combined Use of Lifecycle Management and IoT in Smart Cities*. 2017. URL: http://hdl.handle.net/10993/33336.

[155] Winfried HÖHN. “Deep Learning for Place Name OCR in Early Maps”. In: *Proceedings of the 2nd International Workshop on Exploring Old Maps*. 2017. URL: http://hdl.handle.net/10993/31873.

[156] Winfried HÖHN and Christoph SCHOMMER. “Georeferencing of Place Markers in Digitized Early Maps by Using Similar Maps as Data Source”. In: *Digital Humanities 2017: Conference Abstracts*. 2017. URL: http://hdl.handle.net/10993/31874.

[157] Winfried HÖHN and Christoph SCHOMMER. “RAT 2.0”. In: *Digital Humanities 2017: Conference Abstracts*. 2017. URL: http://hdl.handle.net/10993/31875.

[158] Tingting HU, Ivan Cibrario Bertolotti, and Nicolas NAVET. “Towards Seamless Integration of N-Version Programming in Model-Based Design”. In: *22nd IEEE International Conference on Emerging Technologies And Factory Automation (ETFA'2017), Limassol, Cyprus, September 12-15 2017*. IEEE, 2017. ISBN: 978-1-5090-6505-9. DOI: 10.1109/ETFA.2017.8247678. URL: http://hdl.handle.net/10993/34017.

[159] Médéric HURIER, Guillermo Suarez-Tangil, Santanu Kumar Dash, Tegawendé François d Assise BISSYANDE, Yves le TRAON, Jacques KLEIN, and Lorenzo Cavallaro. “Euphony: Harmonious Unification of Cacophonous Anti-Virus Vendor Labels for Android Malware”. In: *MSR 2017*. 2017. URL: http://hdl.handle.net/10993/31441.

[160] Jean-Louis HUYNEN and Gabriele LENZINI. “From Situation Awareness to Action: An Information Security Management Toolkit for Socio-Technical Security Retrospective and Prospective Analysis”. In: *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*. 2017. URL: http://hdl.handle.net/10993/29940.

[161] Vincenzo IOVINO, Alfredo RIAL DURAN, Peter ROENNE, and Peter Y. A. RYAN. “Using Selene to Verify your Vote in JCJ”. In: *Workshop on Advances in Secure Electronic Voting (VOTING'17)*. 2017, p. 17. URL: http://hdl.handle.net/10993/31168.

[162] Sasan JAFARNEJAD, German CASTIGNANI, and Thomas ENGEL. “Towards a Real-Time Driver Identification Mechanism Based on Driving Sensing Data”. In: *20th International Conference on Intelligent Transportation Systems (ITSC)*. 2017, p. 7. URL: http://hdl.handle.net/10993/32359.

[163] Ravi JHAWAR and Sjouke MAUW. “Model-driven situational awareness for moving target defense”. In: *Proc. 16th European Conference on Cyber Warfare and Security*. ACPI, 2017, pp. 184–192. URL: http://hdl.handle.net/10993/33899.

[164] Hugo Jonker and Sjouke MAUW. “A security perspective on publication metrics”. In: *Proc. 25th Security Protocols Workshop*. Springer, 2017, pp. 186–200. URL: http://hdl.handle.net/10993/33830.

[165] Hugo Jonker, Sjouke MAUW, and Tom Schmitz. “Reverse Bayesian poisoning: How to use spam filters to manipulate online elections”. In: *Proc. 2nd International Joint Conference on Electronic Voting*. Springer, 2017, pp. 183–197. ISBN: 978-3-319-68687-5. URL: http://hdl.handle.net/10993/34367.

[166] Emmanuel KIEFFER, Grégoire DANOY, Pascal BOUVRY, and Anass Nagih. "A new Co-evolutionary Algorithm Based on Constraint Decomposition". In: *IPDPS*. IEEE Computer Society, 2017. URL: http://hdl.handle.net/10993/33616.

[167] Emmanuel KIEFFER, Grégoire DANOY, Pascal BOUVRY, and Anass Nagih. "Bayesian Optimization Approach of General Bi-level Problems". In: *Proceedings of the Genetic and Evolutionary Computation Conference Companion*. ACM, 2017, pp. 1614–1621. ISBN: 978-1-4503-4939-0. DOI: 10.1145/3067695.3082537. URL: http://hdl.handle.net/10993/32009.

[168] Sybren de Kinderen, Monika Kaczmarek-Heß, Qin MA, and Iván S. Razo-Zapata. "Towards Meta Model Provenance: a Goal-Driven Approach to Document the Provenance of Meta Models". In: *Lecture Notes in Business Information Processing 305*. Springer, 2017. ISBN: 978-3-319-70240-7. URL: http://hdl.handle.net/10993/33879.

[169] Johannes KLEIN, Jean BOTEV, and Steffen ROTHKUGEL. "Concurrency-Based and User-Centric Collaboration for Distributed Compound Document Authoring". In: *Proceedings of the 2017 IEEE 21st International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. IEEE, 2017, pp. 168–173. DOI: 10.1109/CSCWD.2017.8066689. URL: http://hdl.handle.net/10993/33017.

[170] Johannes KLEIN, Jean BOTEV, and Steffen ROTHKUGEL. "Concurrent Command and Consistency Management for Distributed Compound Document Authoring". In: *Proceedings of the 2017 IEEE 3rd International Conference on Collaboration and Internet Computing*. IEEE, 2017, pp. 34–40. DOI: 10.1109/CIC.2017.00016. URL: http://hdl.handle.net/10993/33022.

[171] Johannes KLEIN, Jean BOTEV, and Steffen ROTHKUGEL. "Distributed Document Authoring for Location-Independent Collaborative Learning". In: *ICERI 2017 Proceedings*. IATED, 2017, pp. 4399–4408. ISBN: 978-84-697-6957-7. URL: http://hdl.handle.net/10993/33024.

[172] Johannes KLEIN, Jean BOTEV, and Steffen ROTHKUGEL. "Enabling Near Real-Time Collaboration in a Distributed Multimedia Editing Environment". In: *Proceedings of the 12th International Workshop on Multimedia Technologies for E-Learning in conjunction with IEEE ISM 2017*. IEEE, 2017, pp. 587–594. DOI: 10.1109/ISM.2017.115. URL: http://hdl.handle.net/10993/33023.

[173] Niklas KOLBE, Sylvain KUBLER, Jérémy ROBERT, Yves le TRAON, and Arkady Zaslavsky. "Towards Semantic Interoperability in an Open IoT Ecosystem for Connected Vehicle Services". In: *2017 IEEE Global Internet of Things Summit (GIoTS) Proceedings*. 2017. URL: http://hdl.handle.net/10993/31791.

[174] Niklas KOLBE, Jérémy ROBERT, Sylvain Kubler, and Yves le TRAON. "PROFICIENT: Productivity Tool for Semantic Interoperability in an Open IoT Ecosystem". In: *Proceedings of the 14th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. 2017. DOI: 10.1145/3144457.3144479. URL: http://hdl.handle.net/10993/32960.

[175] Niklas KOLBE, Arkady Zaslavsky, Sylvain KUBLER, Jérémy ROBERT, and Yves le TRAON. “Enriching a Situation Awareness Framework for IoT with Knowledge Base and Reasoning Components”. In: *Modeling and Using Context*. 2017. URL: http://hdl.handle.net/10993/31792.

[176] Sylvain KUBLER, William Derigent, Alexandre Voisin, Jérémy ROBERT, and Yves le TRAON. “Knowledge-based Consistency Index for Fuzzy Pairwise Comparison Matrices”. In: *Knowledge-based Consistency Index for Fuzzy Pairwise Comparison Matrices*. 2017. URL: http://hdl.handle.net/10993/31973.

[177] Thomas Laurent, Mike PAPADAKIS, Marinos KINTIS, Christopher HENARD, Yves le TRAON, and Anthony Ventresque. “Assessing and Improving the Mutation Testing Practice of PIT”. In: *10th IEEE International Conference on Software Testing, Verification and Validation*. 2017. URL: http://hdl.handle.net/10993/29779.

[178] Gabriele LENZINI, Ouchani Samir, Peter ROENNE, Peter Y. A. RYAN, Yong Geng, JungHyun NOH, and Jan LAGERWALL. “Security in the Shell : An Optical Physical Unclonable Function made of Shells of Cholesteric Liquid Crystals”. In: *Proc. of the 9th IEEE Workshop on Information Forensics and Security*. 2017. URL: http://hdl.handle.net/10993/32518.

[179] Daoyuan LI, Tegawendé François d Assise BISSYANDE, Jacques KLEIN, and Yves le TRAON. “Sensing by Proxy in Buildings with Agglomerative Clustering of Indoor Temperature Movements”. In: *The 32nd ACM Symposium on Applied Computing (SAC 2017)*. 2017. DOI: 10.1145/3019612.3019699. URL: http://hdl.handle.net/10993/29473.

[180] Li LI. “Mining AndroZoo: A Retrospect”. In: *The International Conference on Software Maintenance and Evolution (ICSME)*. 2017. URL: http://hdl.handle.net/10993/31868.

[181] Li LI, Tegawendé François d Assise BISSYANDE, and Jacques KLEIN. “SimiDroid: Identifying and Explaining Similarities in Android Apps”. In: *Abstract book of the 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (2017). URL: http://hdl.handle.net/10993/31644.

[182] Li Li, Naipeng Dong, Jun PANG, Jun Sun, Guandong Bai, Yang Liu, and Jin Song Dong. “A verification framework for stateful security protocols”. In: *Proceedings of the 19th International Conference on Formal Engineering Methods*. Springer Science & Business Media B.V., 2017, pp. 262–280. URL: http://hdl.handle.net/10993/32657.

[183] Li LI, Daoyuan LI, Tegawendé François d Assise BISSYANDE, Jacques KLEIN, Haipeng Cai, David Lo, and Yves le TRAON. “Automatically Locating Malicious Packages in Piggybacked Android Apps”. In: *Abstract book of the 4th IEEE/ACM International Conference on Mobile Software Engineering and Systems (MobileSoft 2017)* (2017). URL: http://hdl.handle.net/10993/30028.

[184] Zhe LIU, Kimmo Järvinen, Weiqiang Liu, and Hwajeong Seo. “Multiprecision Multiplication on ARMv8”. In: *IEEE 24th Symposium on Computer Arithmetic - ARITH24*. 2017, pp. 10–17. URL: http://hdl.handle.net/10993/34104.

[185] Zhe LIU, Patrick Longa, Geovandro Pereira, Oscar Reparaz, and Hwajoneg Seo. “FourQ on Embedded Devices with Strong Countermeasures Against Side-Channel Attacks”. In: *International Conference on Cryptographic Hardware and Embedded Systems - CHES2017*. 2017, pp. 665–686. URL: http://hdl.handle.net/10993/34103.

[186] Thomas Loise, Xavier Devroey, Gilles Perrouin, Mike PAPADAKIS, and Patrick Heymans. “Towards Security-aware Mutation Testing”. In: *The 12th International Workshop on Mutation Analysis (Mutation 2017)*. 2017. URL: http://hdl.handle.net/10993/29780.

[187] José Miguel LOPEZ BECERRA, Vincenzo IOVINO, Dimiter OSTREV, Petra SALA, and Marjan SKROBOT. “Tightly-Secure PAK(E)”. In: *Cryptology and Network Security*. Springer, 2017. URL: http://hdl.handle.net/10993/33788.

[188] José Miguel LOPEZ BECERRA, Vincenzo IOVINO, Dimiter OSTREV, and Marjan SKROBOT. “On the Relation Between SIM and IND-RoR Security Models for PAKEs”. In: *Proceedings of the International Conference on Security and Cryptography*. SCITEPRESS, 2017, p. 12. URL: http://hdl.handle.net/10993/31655.

[189] Gaetano Manzo, Ridha SOUA, Antonio DI MAIO, Thomas ENGEL, Maria Rita Palattella, and Gianluca Rizzo. “Coordination Mechanisms for Floating Content in Realistic Vehicular Scenario”. In: *Coordination Mechanisms for Floating Content in Realistic Vehicular Scenario*. 2017. URL: http://hdl.handle.net/10993/32906.

[190] Weizhi Meng, Wanghao Lee, Man ho Au, and Zhe LIU. “Exploring Effect of Location Number on Map-Based Graphical Password Authentication”. In: *22nd Australasian Conference on Information Security and Privacy - ACISP2017*. 2017. URL: http://hdl.handle.net/10993/34111.

[191] Weizhi Meng, Wanghao Lee, Zhe LIU, Chunhua Su, and Yan Li. “Evaluating the Impact of Juice Filming Charging Attack in Practical Environments”. In: *The 20th Annual International Conference on Information Security and Cryptology - ICISC2017*. 2017. URL: http://hdl.handle.net/10993/34109.

[192] Kevin Milner, Cas Cremers, Jiangshan YU, and Mark Ryan. “Automatically Detecting the Misuse of Secrets: Foundations, Design Principles, and Applications”. In: *30th IEEE Computer Security Foundations Symposium*. 2017. URL: http://hdl.handle.net/10993/32513.

[193] Andrzej Mizera, Jun PANG, Hongyang Qu, and Qixia YUAN. “A new decomposition method for attractor detection in large synchronous Boolean networks”. In: *Proceedings of the 3rd International Symposium on Dependable Software Engineering: Theories, Tools, and Applications*. Springer Science & Business Media B.V., 2017, pp. 232–249. URL: http://hdl.handle.net/10993/32656.

[194] Ludovic MOULINE, Thomas HARTMANN, François FOUQUET, Yves le TRAON, Johann Bourcier, and Olivier Barais. “Weaving Rules into Models@run.time for Embedded Smart Systems”. In: *Programming ’17 Companion to the first International Conference on the Art, Science and*

Engineering of Programming. ACM, 2017. ISBN: 978-1-4503-4836-2. DOI: 10.1145/3079368.3079394. URL: http://hdl.handle.net/10993/31647.

[195] Rohan Nanda, Luigi Di Caro, Guido Boella, Hristo Konstantinov, Tenyo Tyankov, Daniel Traykov, Hristo Hristov, Francesco Costamagna, Llio Humphreys, Livio ROBALDO, and Michele Romano. "A Unifying Similarity Measure for Automated Identification of National Implementations of European Union Directives". In: *A Unifying Similarity Measure for Automated Identification of National Implementations of European Union Directives*. 2017. URL: http://hdl.handle.net/10993/31850.

[196] Rohan Nanda, Giovanni Siragusa, Luigi Di caro, Martin THEOBALD, Guido Boella, Livio ROBALDO, and Francesco Costamagna. "Concept Recognition in European and National Law". In: *proc. of The 30th international conference on Legal Knowledge and Information Systems (JURIX 2017)*. 2017. URL: http://hdl.handle.net/10993/34087.

[197] Nicolas NAVET, Ivan Cibrario Bertolotti, and Tingting HU. "Software patterns for fault injection in CPS engineering". In: *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2017, pp. 1–6. ISBN: 978-1-5090-6505-9. DOI: 10.1109/ETFA.2017.8247701. URL: http://hdl.handle.net/10993/34018.

[198] Gilles NEYENS and Denis ZAMPUNIERIS. "Conflict handling for autonomic systems". In: *Procedings of the 11th IEEE International Conference on Self-Adaptive and Self-Organizing Systems, Tucson, AZ, USA 18-22 September 2017*. IEEE Computer Society Publications, 2017, pp. 369–370. ISBN: 978-1-5090-6558-5. DOI: 10.1109/FAS*W.2017.81. URL: http://hdl.handle.net/10993/33263.

[199] Gilles NEYENS and Denis ZAMPUNIERIS. "Using Hidden Markov Models and Rule-based Sensor Mediation on Wearable eHealth Devices". In: *Procedings of the 11th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, Barcelona, Spain 12-16 November 2017*. IARIA, 2017. ISBN: 978-1-61208-598-2. URL: http://hdl.handle.net/10993/33264.

[200] Dat Ba Nguyen, Martin THEOBALD, and Gerhard Weikum. "J-REED: Joint Relation Extraction and Entity Disambiguation". In: *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management, CIKM 2017, Singapore, November 06 - 10, 2017*. 2017, pp. 2227–2230. URL: http://hdl.handle.net/10993/34048.

[201] Andriy PANCHENKO, Asya MITSEVA, Martin Henze, Fabian LANZE, Klaus Wehrle, and Thomas ENGEL. "Analysis of Fingerprinting Techniques for Tor Hidden Services". In: *Proceedings of the 24th ACM Computer and Communications Security (ACM CCS) 16th Workshop on Privacy in the Electronic Society (ACM WPES 2017)*. 2017. URL: http://hdl.handle.net/10993/32522.

[202] Jun PANG and Yang Zhang. "DeepCity: A Feature Learning Framework for Mining Location Check-Ins". In: *Proceedings of the 11th International Conference on Web and Social Media (ICWSM'17)*. AAAI, 2017, pp. 652–655. URL: http://hdl.handle.net/10993/31237.

[203] Jun PANG and Yang Zhang. “Quantifying location sociality”. In: *Proc. 28th ACM Conference on Hypertext and Social Media - HT'17*. ACM Press, 2017, pp. 145–154. DOI: 10.1145/3078714.3078729. URL: http://hdl.handle.net/10993/31597.

[204] Xavier PARENT and Leon van der TORRE. “The pragmatic oddity in a norm-based semantics”. In: *16th International Conference on Artificial Intelligence & Law (ICAIL-17)*. ACM, 2017. URL: http://hdl.handle.net/10993/31638.

[205] Balazs PEJO and Qiang Tang. “To Cheat or Not to Cheat - A Game-Theoretic Analysis of Outsourced Computation Verification”. In: *Fifth ACM International Workshop on Security in Cloud Computing, Abu Dhabi 2 April 2017*. ACM, 2017. ISBN: 978-1-4503-4970-3. DOI: 10.1145/3055259.3055262. URL: http://hdl.handle.net/10993/30691.

[206] Dayana PIERINA BRUSTOLIN SPAGNUELO, Cesare BARTOLINI, and Gabriele LENZINI. “Modelling Metrics for Transparency in Medical Systems”. In: *Proceedings of TrustBus 2017*. 2017. URL: http://hdl.handle.net/10993/31943.

[207] Andrei POPLETEEV. “AmbiLoc: A year-long dataset of FM, TV and GSM fingerprints for ambient indoor localization”. In: *8th International Conference on Indoor Positioning and Indoor Navigation (IPIN-2017)*. 2017. URL: http://hdl.handle.net/10993/32587.

[208] Andrei POPLETEEV. “Indoor localization using ambient FM radio RSS fingerprinting: A 9-month study”. In: *17th IEEE International Conference on Computer and Information Technology (CIT-2017)*. 2017. DOI: 10.1109/CIT.2017.57. URL: http://hdl.handle.net/10993/32586.

[209] Andrei POPLETEEV. “Please Stand By: TV-based indoor localization”. In: *28th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC-2017)*. 2017. URL: http://hdl.handle.net/10993/32588.

[210] Andrei POPLETEEV. “Wi-Fi butterfly effect in indoor localization: The impact of imprecise ground truth and small-scale fading”. In: *14th IEEE Workshop on Positioning, Navigation and Communications (WPNC-2017)*. 2017. URL: http://hdl.handle.net/10993/32589.

[211] Ila Radhakrishnan, Ridha SOUA, Maria Rita PALATTELLA, and Thomas ENGEL. “An Efficient Service Channel Allocation Scheme in SDN-enabled VANETs”. In: *An Efficient Service Channel Allocation Scheme in SDN-enabled VANETs*. 2017. DOI: 10.1109/MedHocNet.2017.8001644. URL: http://hdl.handle.net/10993/33107.

[212] Vincent RAHLI, Mark Bickford, and Robert Constable. “Bar Induction: The Good, the Bad, and the Ugly”. In: *Thirty-Second Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*. 2017. DOI: 10.1109/LICS.2017.8005074. URL: http://hdl.handle.net/10993/31268.

[213] Iván S. Razo-Zapata, Qin MA, Monika Kaczmarek-Heß, and Sybren de Kinderen. "The Conjoint Modeling of Value Networks and Regulations of Smart Grid Platforms: A Luxembourg Case Study". In: *19th IEEE Conference on Business Informatics, CBI 2017, Thessaloniki, Greece, July 24-27, 2017, Volume 2: Workshop Papers*. 2017, pp. 83–88. URL: http://hdl.handle.net/10993/33878.

[214] Francisco Javier RODRIGUEZ LERA, Francisco Martín Rico, and Vicente Matellán Olivera. "Context Awareness in shared human-robot Environments: Benefits of Environment Acoustic Recognition for User Activity Classification". In: *8th International Conference of Pattern Recognition Systems (ICPRS 2017), Madrid (Spain), 11-13 July 2017*. Institution of Engineering and Technology, 2017, ISBN: 978-1-78561-652-5. URL: http://hdl.handle.net/10993/33755.

[215] Francisco Javier RODRIGUEZ LERA, Francisco Martín Rico, and Vicente Matellán. "Deep Learning and Bayesian Networks for Labelling User Activity Context Through Acoustic Signals". In: *Biomedical Applications Based on Natural and Artificial Computing: International Work-Conference on the Interplay Between Natural and Artificial Computation, IWINAC 2017, Corunna, Spain, June 19-23, 2017, Proceedings, Part II*. Springer International Publishing, 2017, pp. 213–222. ISBN: 978-3-319-59773-7. DOI: 10.1007/978-3-319-59773-7_22. URL: http://hdl.handle.net/10993/33758.

[216] Martin ROSALIE, Matthias BRUST, Grégoire DANOY, Serge Chaumette, and Pascal BOUVRY. "Coverage optimization with connectivity preservation for UAV swarms applying chaotic dynamics". In: *IEEE International Conference on Autonomic Computing (ICAC), Columbus 17-21 July 2017*. 2017, pp. 113–118. DOI: 10.1109/ICAC.2017.26. URL: http://hdl.handle.net/10993/31935.

[217] Martin ROSALIE, Grégoire DANOY, Serge Chaumette, and Pascal BOUVRY. "Impact du mécanisme chaotique sur l'optimisation d'un modèle de mobilité pour un essaim de drones devant réaliser une couverture de zone". In: *Comptes-rendus de la 20e Rencontre du Non Linéaire*. Non-Linéaire Publications, 2017, pp. 79–84. ISBN: 978-2-9538596-6-9. URL: http://hdl.handle.net/10993/30979.

[218] Martin ROSALIE, Jan Eric DENTLER, Grégoire DANOY, Pascal BOUVRY, Somasundar KANNAN, Miguel Angel OLIVARES MENDEZ, and Holger VOOS. "Area exploration with a swarm of UAVs combining deterministic Chaotic Ant Colony Mobility with position MPC". In: *2017 International Conference on Unmanned Aircraft Systems (ICUAS)*. 2017, pp. 1392–1397. ISBN: 978-1-5090-4495-5. DOI: 10.1109/ICUAS.2017.7991418. URL: http://hdl.handle.net/10993/31476.

[219] Arianna Rossi and Monica Palmirani. "A Visualization Approach for Adaptive Consent in the European Data Protection Framework". In: *Proceedings of the 7th International Conference for E-Democracy and Open Government*. 2017, pp. 159–170. ISBN: 978-1-5090-6718-3. URL: http://hdl.handle.net/10993/33525.

[220] Alban ROUSSET, Abdoul Wahid MAINASSARA CHEKARAOU, Yu-Chung LIAO, Xavier BESSERON, Sébastien VARRETTE, and Bernhard PETERS. "Comparing Broad-Phase Interaction Detection Algorithms for Multi-physics DEM Applications". In: *AIP Conference Proceedings ICNAAM 2017*. American Institute of Physics, 2017. URL: http://hdl.handle.net/10993/32261.

[221] Hwajeong Seo, Zhe LIU, Taehwan Park, Hyeokchan Kwon, Sokjoon Lee, and Howon Kim. "Secure Number Theoretic Transform and Speed Record for Ring-LWE Encryption on Embedded Processors". In: *The 20th Annual International Conference on Information Security and Cryptology - ICISC2017*. 2017. URL: http://hdl.handle.net/10993/34108.

[222] Adi Shamir, Alexei BIRYUKOV, and Léo Paul PERRIN. "Summary of an Open Discussion on IoT and Lightweight Cryptography". In: *Proceedings of Early Symmetric Crypto workshop, 2017*. University of Luxembourg, 2017. ISBN: 978-99959-814-2-6. URL: http://hdl.handle.net/10993/30955.

[223] Alexander Steen, Max Wisniewski, and Christoph Ewald BENZMÜLLER. "Going Polymorphic - TH1 Reasoning for Leo-III". In: *IWIL Workshop and LPAR Short Presentations*. EasyChair, 2017, p. 13. URL: http://hdl.handle.net/10993/33702.

[224] Alexander Steen, Max Wisniewski, Hans-Jörg Schurr, and Christoph Ewald BENZMÜLLER. "Capability Discovery for Automated Reasoning Systems". In: *IWIL Workshop and LPAR Short Presentations*. EasyChair, 2017, p. 6. URL: http://hdl.handle.net/10993/33701.

[225] Thierry TITCHEU CHEKAM, Mike PAPADAKIS, Yves le TRAON, and Mark Harman. "An Empirical Study on Mutation, Statement and Branch Coverage Fault Revelation that Avoids the Unreliable Clean Program Assumption". In: *International Conference on Software Engineering (ICSE 2017)*. 2017. URL: http://hdl.handle.net/10993/30694.

[226] Leon van der TORRE and Marc van ZEE. "Rational Enterprise Architecture". In: *Advances in Artificial Intelligence: From Theory to Practice - 30th International Conference on Industrial Engineering and Other Applications of Applied Intelligent Systems, IEA/AIE 2017, Arras, France, June 27-30, 2017, Proceedings, Part I*. 2017. DOI: 10.1007/978-3-319-60042-0_2. URL: http://hdl.handle.net/10993/33982.

[227] Marcus VOLP, Francisco Rocha, Jérémie DECOUCHANT, Jiangshan YU, and Paulo ESTEVES VERISSIMO. "Permanent Reencryption: How to Survive Generations of Cryptanalysts to Come". In: *Twenty-fifth International Workshop on Security Protocols*. 2017. URL: http://hdl.handle.net/10993/32521.

[228] Jingyi Wang, Jun Sun, Qixia YUAN, and Jun PANG. "Should We Learn Probabilistic Models for Model Checking? A New Approach and An Empirical Study". In: *Proceedings of 20th International Conference on Fundamental Approaches to Software Engineering*. Springer, 2017, pp. 3–21. URL: http://hdl.handle.net/10993/30332.

[229] Jun WANG and Qiang Tang. "Differentially Private Neighborhood-based Recommender Systems". In: *IFIP Information Security & Privacy Conference*. Springer, 2017, p. 14. URL: http://hdl.handle.net/10993/30114.

[230] Yan Wang, Zongxu Qin, Jun PANG, Yang Zhang, and Xin Jin. “Semantic annotation for places in LBSN through graph embedding”. In: *Proceedings of the 26th ACM International Conference on Information and Knowledge Management - CIKM'17*. ACM Press, 2017, pp. 2343–2346. URL: http://hdl.handle.net/10993/32879.

[231] Peerasak Wangsom, Kittichai Lavangnananda, and Pascal BOUVRY. “Measuring data locality ratio in virtual MapReduce cluster using WorkflowSim”. In: *Proceedings of the 14th International Joint Conference on Computer Science and Software Engineering (JCSSE), 2017 14th*. IEEE, 2017. DOI: 10.1109/JCSSE.2017.8025944. URL: http://hdl.handle.net/10993/34042.

[232] Muhammad Umer WASIM, Abdallah Ali Zainelabden Abdallah IBRAHIM, Pascal BOUVRY, and Tadas Limba. “Law as a Service (LaaS): Enabling Legal Protection over a Blockchain Network”. In: *14th International Conference on Smart Cities: Improving Quality of Life using ICT & IoT (HONET-ICT 17), October 09-11, Irbid Jordan*. 2017. URL: http://hdl.handle.net/10993/32616.

[233] Muhammad Umer WASIM, Abdallah Ali Zainelabden Abdallah IBRAHIM, Pascal BOUVRY, and Tadas Limba. “Self-Regulated Multi-criteria Decision Analysis: An Autonomous Brokerage-Based Approach for Service Provider Ranking in the Cloud”. In: *9th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2017), December 11-14, Hong Kong China*. 2017. URL: http://hdl.handle.net/10993/32617.

[234] Gao Xinwei, Lin Li, Ding Jintai, Liu Jiqiang, Saraswathy Rv, and Zhe LIU. “Fast Discretized Gaussian Sampling and Post-quantum TLS Ciphersuite”. In: *The 13th International Conference on Information Security Practice and Experience - ISPEC 2017*. 2017. URL: http://hdl.handle.net/10993/34110.

[235] Jiangshan YU, Mark Ryan, and Liqun Chen. “Authenticating compromisable storage systems”. In: *The 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. 2017. URL: http://hdl.handle.net/10993/32514.

[236] Yang zhang, Minyue Ni, Weili Han, and Jun PANG. “Does #like4like indeed provoke more likes?” In: *Proceedings of the 16th IEEE/WIC/ACM International Conference on Web Intelligence (WI'17)*. ACM, 2017, pp. 179–186. URL: http://hdl.handle.net/10993/32089.

[237] Cong Zuo, Jun Shao, Zhe LIU, Yun Ling, and Guiyi Wei. “Hidden-Token Searchable Public-Key Encryption”. In: *The 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications - IEEE TrustCom-17*. 2017. URL: http://hdl.handle.net/10993/34112.

A.6 Technical Report

[238] Alexei BIRYUKOV, Daniel FEHER, and Dmitry KHOVRATOVICH. *Guru: Universal Reputation Module for Distributed Consensus Protocols*. University of Luxembourg > Faculty of Science, Technology et al., 2017. URL: http://hdl.handle.net/10993/31586.

[239] Richard Booth, Giovanni CASINI, Thomas Meyer, and Ivan Varzinczak. *Extending Typicality for Description Logics*. Cardiff University > School of Computer Science et al., 2017. URL: http://hdl.handle.net/10993/32165.

[240] Marcos CRAMER. *Modelling argumentation on Axiom of Choice in ASPIC-END – Technical report*. University of Luxembourg > Faculty of Science, Technology, Communication (FSTC) > Computer Science, and Communications Research Unit (CSC), 2017. URL: http://hdl.handle.net/10993/33709.

[241] Marcos CRAMER and Deepak Garg. *Kripke Semantics for BL0 and BL – Technical report*. University of Luxembourg > Faculty of Science, Technology, Communication (FSTC) > Computer Science, and Communications Research Unit (CSC), 2017. URL: http://hdl.handle.net/10993/31269.

[242] Sébastien FAYE, Nicolas LOUVETON, Sasan JAFARNEJAD, Roman Kryvchenko, and Thomas ENGEL. *An Open Dataset for Human Activity Analysis using Smart Devices*. University of Luxembourg > Interdisciplinary Centre for Security, Reliability et al., 2017. URL: http://hdl.handle.net/10993/32355.

[243] Diego Luis KREUTZ, Paulo ESTEVES VERISSIMO, Catia Magalhaes, and Fernando M. V. Ramos. *The KISS principle in Software-Defined Networking: An architecture for Keeping It Simple and Secure*. University of Luxembourg > Interdisciplinary Centre for Security, Reliability and Trust (SNT), 2017. URL: http://hdl.handle.net/10993/34585.

[244] Daoyuan LI, Tegawendé François d Assise BISSYANDE, Jacques KLEIN, Yves le TRAON, Paul Schummer, Ben Muller, and Anne-Marie Solvi. *Towards a Plug-and-Play and Holistic Data Mining Framework for Understanding and Facilitating Operations in Smart Buildings*. University of Luxembourg > Interdisciplinary Centre for Security, Reliability et al., 2017. URL: http://hdl.handle.net/10993/32961.

[245] Raphael Sirres, Tegawendé François d Assise BISSYANDE, Dongsun KIM, David Lo, Jacques KLEIN, and Yves le TRAON. *Augmenting and Structuring User Queries to Support Efficient Free-Form Code Search*. University of Luxembourg > Interdisciplinary Centre for Security, Reliability et al., 2017. URL: http://hdl.handle.net/10993/30408.

A.7 Miscellaneous

[246] Arash ATASHPENDAR, Peter ROENNE, Dimiter OSTREV, and Peter Y. A. RYAN. *Deniability in Quantum Cryptography*. 2017. URL: http://hdl.handle.net/10993/34161.

[247] Cesare BARTOLINI and Gabriele LENZINI. *Human Rights in the era of Information and Communication Technology*. 2017. URL: http://hdl.handle.net/10993/33857.

[248] Christoph Ewald BENZMÜLLER. *Universal Reasoning, Rational Argumentation and Human-Machine Interaction*. 2017. URL: http://hdl.handle.net/10993/33919.

[249] Alexei BIRYUKOV and Léo Paul PERRIN. *State of the Art in Lightweight Symmetric Cryptography*. 2017. URL: http://hdl.handle.net/10993/31319.

[250] Raymond Joseph BISDORFF. *Algorithmic Decision Theory for solving complex decision problems*. 2017. URL: http://hdl.handle.net/10993/31196.

[251] Thierry DERRMANN, Raphaël FRANK, and Francesco VITI. *Towards Estimating Urban Macroscopic Fundamental Diagrams From Mobile Phone Signaling Data: A Simulation Study*. 2017. URL: http://hdl.handle.net/10993/28802.

[252] Sébastien FAYE, Guido CANTELMO, Ibrahim Tahirou, Thierry DERRMANN, Francesco VITI, and Thomas ENGEL. *Demo: MAMBA: A Platform for Personalised Multimodal Trip Planning*. 2017. URL: http://hdl.handle.net/10993/33307.

[253] Sébastien FAYE, Sasan JAFARNEJAD, Juan COSTAMAGNA, German CASTIGNANI, and Thomas ENGEL. *Poster: Characterizing Driving Behaviors Through a Car Simulation Platform*. 2017. URL: http://hdl.handle.net/10993/32908.

[254] Christian FRANCK. *A Decoder for a Symbol-Constrained Code (preliminary version)*. 2017. URL: http://hdl.handle.net/10993/33707.

[255] Christian FRANCK. *Mapping Combinational Circuits to Homogenous Trellis-Constrained Codes*. 2017. URL: http://hdl.handle.net/10993/31646.

[256] Nicolas GUELFI, Alfredo CAPOZUCCA, and Benoit RIES. *A Product Line of Software Engineering Project Courses*. 2017. URL: http://hdl.handle.net/10993/34094.

[257] Matthieu JIMENEZ, Maxime Cordy, Marinos KINTIS, Thierry TITCHEU CHEKAM, Yves le TRAON, and Mike PAPADAKIS. *On the Naturalness of Mutants*. 2017. URL: http://hdl.handle.net/10993/35014.

[258] Daniel Kirchner, Christoph Ewald BENZMÜLLER, and Edward N. Zalta. *Mechanizing Principia Logico-Metaphysica in Functional Type Theory*. 2017. URL: http://hdl.handle.net/10993/33700.

[259] Diego Luis KREUTZ, Jiangshan YU, Fernando M. V. Ramos, and Paulo ESTEVES VERISSIMO. *ANCHOR: logically-centralized security for Software-Defined Networks*. 2017. URL: http://hdl.handle.net/10993/34586.

[260] Li LI, Tegawendé François d Assise BISSYANDE, Alexandre BARTEL, Jacques KLEIN, and Yves le TRAON. *The Multi-Generation Repackaging Hypothesis*. 2017. URL: http://hdl.handle.net/10993/30111.

[261] Li LI, Daoyuan LI, Tegawendé François d Assise BISSYANDE, Jacques KLEIN, Yves le TRAON, David Lo, and Lorenzo Cavallaro. *Understanding Android App Piggybacking*. 2017. URL: http://hdl.handle.net/10993/30027.

[262] Beishui Liao and Leon van der TORRE. *Defense semantics of argumentation: encoding reasons for accepting arguments*. 2017. URL: http://hdl.handle.net/10993/33983.

[263] José Miguel LOPEZ BECERRA, Vincenzo IOVINO, and Marjan SKROBOT. *On the Relation Between SIM and IND-RoR Security Models for PAKEs*. 2017. URL: http://hdl.handle.net/10993/35015.

[264] Andrei POPLETEEV. *Poster: Impact of ground truth errors on Wi-Fi localization accuracy*. 2017. DOI: 10.1145/3081333.3089310. URL: http://hdl.handle.net/10993/32585.

[265] Muhammad Umer WASIM. *Attacks and protection for Intellectual Property Rights, Privacy, and Contracts in the Cloud*. 2017. URL: http://hdl.handle.net/10993/32625.

[266] Muhammad Umer WASIM. *Communication Strategies for Next-Generation of University based Science Parks*. 2017. URL: http://hdl.handle.net/10993/32626.

[267] Muhammad Umer WASIM. *Intellectual Property Rights infringement in the Cloud*. 2017. URL: http://hdl.handle.net/10993/32627.

A.8 Unpublished

[268] Bo An, Ana L. C. Bazzan, João Leite, Serena Villata, and Leon van der TORRE. "PRIMA 2017: Principles and Practice of Multi-Agent Systems - 20th International Conference, Nice, France, October 30 - November 3, 2017 Proceedings". 2017. URL: http://hdl.handle.net/10993/33986.

[269] Cesare BARTOLINI and Gabriele LENZINI. "Law and the software development life cycle". 2017. URL: http://hdl.handle.net/10993/34145.

[270] Christoph Ewald BENZMÜLLER, Ali FARJAMI, Xavier PARENT, and Leon van der TORRE. "Implementation of Carmo and Jones Dyadic Deontic Logic in Isabelle/HOL". 2017. URL: http://hdl.handle.net/10993/33607.

[271] Christoph Ewald BENZMÜLLER, Christine Lisetti, and Martin THEOBALD. "GCAI 2017: 3rd Global Conference on Artificial Intelligence, Miami, FL, USA, 18-22 October 2017". 2017. URL: http://hdl.handle.net/10993/34073.

[272] Alexei BIRYUKOV, Dmitry KHOVRATOVICH, and Sergei TIKHOMIROV. "Findel: Secure Derivative Contracts for Ethereum". 2017. URL: http://hdl.handle.net/10993/30975.

[273] Walter BRONZI, Sébastien FAYE, Raphaël FRANK, and Thomas ENGEL. "Characterizing Driving Environments Through Bluetooth Discovery". 2017. URL: http://hdl.handle.net/10993/32185.

[274] Tim van der Heijden, Eva Andersen, Jakub Bronec, Marleen de Kramer, Thomas Durlacher, Antonio Maria FISCARELLI, Shohreh HADDADAN, Ekaterina KAMLOVSKAYA, Jan Lotz, Sam Mersch, Christopher Morse, Kaarel Sikk, and Sytze van Herck. "Presentation of the Luxembourg Centre for Contemporary and Digital History – C2DH Doctoral Training Unit". 2017. URL: http://hdl.handle.net/10993/34187.

[275] ANIL KOYUNCU, Tegawendé François d Assise BISSYANDE, Dongsun KIM, Jacques KLEIN, Martin Monperrus, and Yves le TRAON. "Impact of Tool Support in Patch Construction". 2017. URL: http://hdl.handle.net/10993/31858.

[276] Kristin Krüger, Gerhard Fohler, and Marcus VOLP. “Improving Security for Time-Triggered Real-Time Systems against Timing Inference Based Attacks by Schedule Obfuscation”. 2017. URL: http://hdl.handle.net/10993/33739.

[277] Martin Küttler, Michael Roitzsch, Claude-Joachim Hamann, and Marcus VOLP. “Probabilistic Analysis of Low-Criticality Execution”. 2017. URL: http://hdl.handle.net/10993/33738.

[278] Nicolas NAVET, Josetxo Villanueva, Jörn Migge, and Marc Boyer. “Insights on the performance and configuration of AVB and TSN in automotive applications”. 2017. URL: http://hdl.handle.net/10993/34053.

[279] Andreia Pinto Costa, Georges Steffgen, Francisco Javier RODRIGUEZ LERA, Aida Nazarikhorram, and Pouyan Ziafati. “Socially assistive robots for teaching emotional abilities to children with autism spectrum disorder”. 2017. URL: http://hdl.handle.net/10993/30210.

[280] Michael Raitza, Akash Kumar, Marcus VOLP, Dennis Walter, Jens Trommer, Thomas Mikolajick, and Walter M. Weber. “Exploiting Transistor-Level Reconfiguration to Optimize Combinational Circuits on the Example of a Conditional Sum Adder”. 2017. URL: http://hdl.handle.net/10993/28999.

[281] Bogdan TOADER, Assaad MOAWAD, François FOUQUET, Thomas HARTMANN, Mioara Popescu, and Francesco VITI. “A New Modelling Framework over Temporal Graphs for Collaborative Mobility Recommendation Systems”. 2017. URL: http://hdl.handle.net/10993/32959.

[282] Marcus VOLP, Jérémie DECOUCHANT, Christoph LAMBERT, Maria FERNANDES, and Paulo ESTEVES VERISSIMO. “Enclave-Based Privacy-Preserving Alignment of Raw Genomic Information”. 2017. URL: http://hdl.handle.net/10993/34058.

[283] Marcus VOLP, David KOZHAYA, and Paulo ESTEVES VERISSIMO. “Facing the Safety-Security Gap in RTES: the Challenge of Timeliness”. 2017. URL: http://hdl.handle.net/10993/34057.

[284] Pouyan Ziafati, Francisco Javier RODRIGUEZ LERA, Andreia Pinto Costa, Aida Nazarikhorram, and Leon van der TORRE. “ProCRob Architecture for Personalized Social Robotics”. 2017. URL: http://hdl.handle.net/10993/33763.

Appendix B

Research Projects

This chapter lists research projects that were ongoing during 2017, and whose principal investigator is a CSC member. It is structured to summarize the projects by funding source.

- European Commission
- European Defence Agency
- European Space Agency
- European Union
- External Organisation Funding
- Fonds National de la Recherche
- Fonds National de la Recherche and Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services
- Fonds National de la Recherche
- Fonds National de la Recherche and Narodowe Centrum Badań i Rozwoju
- Fonds National de la Recherche
- University of Luxembourg

B.1 European Commission Projects

Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures

https://www.atena-h2020.eu/

Acronym:	ATENA
Reference:	R-AGR-3026
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	6,889,925.00 €
Duration:	1 May 2016 – 30 Apr 2019
Members:	• Thomas ENGEL (Principal Investigator) • Florian ADAMSKY (Researcher) • Ridha SOUA (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Latif LADID (Program Coordinator) • Andriy PANCHENKO (Scientific Contact)
Area:	Communicative Systems
Partners:	• Crat • CREOS • Enea • Iec • Institute of Baltic Studies • itrust Luxembourg • Multitel • Sapienza SL • SES Spa • Swde • Uniroma3 • University of Coimbra

Description

Over recent years, Industrial and Automation Control Systems (IACS) adopted in Critical Infrastructures (CIs) have become more complex due to the increasing number of interconnected devices, and to the large amount of information

exchanged among system components. With the emergence of such an "Internet of Things" generation of IACS, the boundaries to be protected have grown well beyond that of the single or aggregated-plant, typical of the mono-operator or silos vision. That poses new challenges, as more operators become involved in a scenario that naturally demands the introduction of multitenancy mechanisms. New ICT paradigms, where virtualization is playing an important role, provide innovative features for flexible and efficient management, monitoring and control of devices and data traffic. With the OT/IT convergence, OT (Operation Technologies) will benefit from IT innovation, but at the same time, they will also inherit new IT threats that can potentially impact CIs.

ATENA project, with reference to the above-mentioned interdependent scenario, aims at achieving the desired level of Security and Resilience of the considered CIs, while preserving their efficient and flexible management. ATENA, leveraging the outcomes of previous European Research activities, particularly the CockpitCI and MICIE EU projects, will remarkably upgrade them by exploiting advanced features of ICT algorithms and components, and will bring them at operational industrial maturity level; in this last respect, ATENA outcomes will be tailored and validated in selected Use Cases. In particular, ATENA will develop a Software Defined Security paradigm combining new anomaly detection algorithms and risk assessment methodologies within a distributed environment, and will provide a suite of integrated market-ready ICT networked components and advanced tools embedding innovative algorithms both for correct static CI configuration and for fast dynamic CI reaction in presence of adverse events.

Results

The main activities carried out during 2017 were related to 1) the definition of ATENA System requirements and architecture, 2) analysis of security metrics and critical infrastructure vulnerabilities, and finally 3) distributed awareness.

In the first activity, we have contributed to the overall ATENA Intrusion and Anomaly Detection System (IADS) architecture and the requirements that are necessary to protect critical infrastructure (CI) against cyber attacks. We have included Software-Defined Networking (SDN) and network function virtualization (NFV) components to the IADS architecture and outlined how this can improve the overall detection rate. The results of the first research topic were submitted in the *International Journal of Critical Infrastructure Protection* where ATENA architecture and its key features were highlighted.

After studying the different vulnerabilities of SCADA systems specifically in the level of communication protocols (Modbus, DNP3), we were focused on the distributed intrusion and anomaly detection strategies for industrial automation and control systems. The objective was the analysis and evaluation of the best techniques that suit the needs of the ATENA Intrusion and Anomaly Detection System (IADS). Therefore, we have assessed Machine Learning techniques for intrusion detection in SCADA systems using a real data set collected from a gas pipeline system. The contribution was two-fold: 1) the evaluation of four techniques for missing data estimation and two techniques for data nor-

malization, 2) The performances of Support Vector Machine (SVM), Random Forest (RF), Long Short Term Memory (LSTM) are assessed in terms of accuracy, precision, recall and F_1 score for intrusion detection. Two cases were differentiated: binary and categorical classifications. Our experiments reveal that RF and LSTM detect intrusions effectively, with a F_1 score of respectively >99% and >96%. The results of these studies were submitted to the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).

Furthermore, distributed awareness requires the design of several agents. To this end, we designed several security components (e.g. IDS detection agents/probes) which fulfil both intrusion detection and functional requirements. Specifically, we have provided a detailed description of network signature, statistical, SDN–assisted, multi-antivirus, rule based agents, and honeypots agents. This plethora of agents will operate in complex deployments. Hence, it is crucial to control each device (or a group) in a homogeneous way.

Building an IoT OPen innovation Ecosystem for connected smart objects

http://biotope-h2020.eu/

Acronym:	bIoTope
PI:	Yves LE TRAON
Funding:	European Commission - Horizon 2020
Budget:	598,750.00 €
Duration:	1 Jan 2016 – 31 Dec 2019
Member:	Yves LE TRAON (Principal Investigator)

Description

bIoTope is a RIA (Research and Innovation action) project funded by the Horizon 2020 programme, Call ICT30: Internet of Things and Platforms for Connected Smart Objects.

bIoTope lays the foundation for open innovation ecosystems, where companies can innovate by creating new Systems-of-Systems (SoS) platforms for connected smart objects (based on standardised Open APIs). bIoTope develops a dozen of smart city proofs-of-concept/pilots (visit the USE CASES page), implemented in three distinct cities/regions (Helsinki, Grand Lyon, Brussels Region).2

EU-China study on IoT and 5G

https://euchina-iot5g.eu/

Acronym:	EXCITING
Reference:	R-AGR-3109
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	999,547.00 €
Duration:	1 Nov 2016 – 31 Oct 2018
Members:	• Thomas ENGEL (Principal Investigator) • Detlef FUEHRER (Researcher) • Stefanie OESTLUND (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Latif LADID (Scientific Contact)
Area:	Communicative Systems
Partners:	• BII Group Holdings • Bupt • Caict • Cas • Huawei • Hust • Inno AG • Interinnov • Mandat International • Martel Consulting • Spi • UNIS • Upmc

Description

Europe and China are at the forefront of technological advances in areas related to the Future Internet (especially 5G and IoT). While both parties share common technological objectives, there is still room for improvement in what concerns bilateral co-operation. As a result, the main purpose of EXCITING is to support the creation of favourable conditions for cooperation between the European and Chinese research and innovation ecosystems, mainly related to the key strategic domains of IoT and 5G. EXCITING will study the research and innovation ecosystem for IoT and 5G in China and compare it with the European model.

EXCITING will identify and document the key international standards bodies for IoT and 5G, as well as other associations and fora where discussions take place and implementation decisions are made. Going beyond standardisation, interoperability testing is a key step towards market deployment. EXCITING will identify and document the key international InterOp events at which European and Chinese manufacturers can test and certify their IoT and 5G products. It will also explain the rules for engaging in these events.

EXCITING will produce Best Practice guidelines for establishing and operating practical joint collaborations, in order to stimulate further such co-operations in the future on IoT and 5G Large Scale Pilots. As a result of the above investigations EXCITING will produce a roadmap showing how research and innovation ecosystems, policy, standardisation, interoperability testing and practical Large Scale Pilots should be addressed during the H2020 timeframe, and make recommendations for optimising collaboration between Europe and China for IoT and 5G.

Results

SECAN-Lab compiled and submitted two reports on the Harmonisation of standards for IoT and 5G technologies. Furthermore, we organized and participated in a number of events, including the EXCITING Plenary in Beijing in March 2017 and the IoT Week in Geneva in June 2017

Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and internet of Things deployments

http://www.privacyflag.eu/

Acronym:	Privacy Flag
Reference:	R-AGR-0587
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	4,000,000.00 €
Duration:	1 May 2015 – 30 Apr 2018
Members:	• Thomas ENGEL (Principal Investigator) • Marharyta ALEKSANDROVA (Researcher) • Karim Ahmed Awad El-Sayed EMARA (Researcher) • Daniel FORSTER (Researcher) • Stefan SCHIFFNER (Researcher)

- Stefanie OESTLUND (Project Coordinator)
- Latif LADID (Collaborator)
- Andriy PANCHENKO (Scientific Contact)

Area: Communicative Systems

Partners:
- Archimede Solutions
- CTI - Computer Technology Institute and Press "Diophantus"
- Dunavnet
- HWC
- Internationak Association of IT Lawyers
- Istituto Italiano per la Privacy
- Mandat International (International Cooperation Foundation)
- OTE
- University of Lulea
- Velti

Description

Privacy Flag combines crowd sourcing, ICT technology and legal expertise to protect citizen privacy when visiting websites, using smart-phone applications, or living in a smart city. It will enable citizens to monitor and control their privacy with a user friendly solution provided as a smart phone application, a web browser add-on and a public website. It will:

1. Develop a highly scalable privacy monitoring and protection solution with:
   - Crowd sourcing mechanisms to identify, monitor and assess privacy-related risks;
   - Privacy monitoring agents to identify suspicious activities and applications;
   - Universal Privacy Risk Area Assessment Tool and methodology tailored on European norms on personal data protection;
   - Personal Data Valuation mechanism;
   - Privacy enablers against traffic monitoring and finger printing;
   - User friendly interface informing on the privacy risks when using an application or website.
2. Develop a global knowledge database of identified privacy risks, together with online services to support companies and other stakeholders in becoming privacy-friendly, including: - In-depth privacy risk analytical tool and services; - Voluntary legally binding mechanism for companies located outside Europe to align with and abide to European standards in terms of personal data protection; - Services for companies interested in being privacy friendly; - Labelling and certification process.
3. Collaborate with standardization bodies and actively disseminate towards the public and specialized communities, such as ICT lawyers, policy mak-

ers and academics. 11 European partners, including SMEs and a large telco operator, bring their complementary technical, legal, societal and business expertise; strong links with standardization bodies and international fora; and outcomes from over 20 related research projects. It will build a privacy defenders community and will establish a legal entity with a sound business plan to ensure longterm sustainability and growth.

Results

Privacy Flag aims at developing a set of tools to enable citizens to check whether their rights as data subjects are being respected. Furthermore, we develop tools and services to help companies comply with personal data protection requirements. Some of the tools aim at consumers, so privacy and security measures for these tools are of vital importance. We supported the developers to adopt state of the art network communication protection mechanisms, such as encryption and anonymization. Moreover, UL researched the state of the art of privacy enablers, i.e., tools that improve the protection of personal data for future networked IT services. Finally, in our contribution, we worked on performance improvements for anonymous communication to reduce the user burden of privacy. This is a challenging issue, since on hand privacy likes a crowd so the more users are using the same service the more suspects are there to hide individual actions, but on the otters hand this also leads to overload situations and scaling issues. PrivacyFlag will conclude in 2018.

FIRE+ online interoperability and performance test tools to support emerging technologies from

http://www.f-interop.eu/

Acronym:	F-INTEROP
Reference:	R-AGR-0642
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	2,998,000.00 €
Duration:	1 Nov 2015 – 30 Sep 2018
Members:	• Thomas ENGEL (Principal Investigator) • Luca LAMORTE (Researcher) • Ion TURCANU (Researcher) • Stefanie OESTLUND (Project Coordinator) • Latif LADID (Collaborator)

Area: Communicative Systems

Partners:
- Device Gateway SA
- EANTC AG
- IMINDS
- INRIA
- Institut Européen des Normes de Télécommunication
- Mandat International (International Cooperation Foundation)
- The connected digital economy catapult limited
- Universite Pierre et Marie Curie
- University of Luxembourg

Description

F-Interop will develop and provide remotely accessible tools to support and accelerate standardization processes and products developments, by offsetting several cost and time barriers. It will research and develop a new FIRE experimental platform to support the development of new technologies and standards, from their genesis to the market for: online interoperability tests and validation tools, remote compliance and conformance tests, scalability tests, Quality of Service (QoS) tests, SDN/NFV interoperability tools, Online privacy test tools, energy efficiency tools.

F-Interop gathers standardization partners together with 3 FIRE federations (Fed4FIRE, IoT Lab, OneLab) to build a common experimental platform as a service. Following an end-user driven methodology, it will directly address the needs of 3 emerging standards: oneM2M led by ETSI, 6TiSCH (IETF) chaired by our Inria partner, Web of Things WG (start Feb 2015) led by W3C, our advisory board member. The open call will extend the platform to other standardization activities, as well as to additional tools extensions and SME products validations. F-Interop will: - Provide online interoperability tools enabling research and development teams to test their products development and implementations at any time, without having to wait until the next face-to-face interop meeting. - Provide an online platform for standards compliance and labelling to be used by the IPv6 Forum Ready Logo Program and other similar labelling bodies, including ETSI, IETF and W3C. - Enable SME to accelerate interoperability and the development of their products and services. - Extend FIRE testbeds and bring them closer to the market. To achieve this ambitious objective, F.-Interop gathers a formidable combination of leading industry experts form standardization bodies, research centres, FIRE testbeds and SMEs from Europe and Japan. The F-Interop Ecosystem will enable sustainable impact, commercial uptake and synergies at EU level.

Results

In 2017, Secan-Lab continued its active contribution to the F-Interop project. In particular, we released the first version of Privacy Tool, one of the testing tools available in F-Interop platform. The primary goal of Privacy Tool is to

define automatic methods to detect privacy and confidential data leaks while different kind of tests are executed on the F-Interop platform. Differently from other testing tools which are devoted to test performance, interoperability and compatibility of most relevant IoT protocols, this tool aims to identify the compliance with the current European Regulation in terms of data management, increasing the trustiness of the platform while communicating with the public internet. For this reason, we designed a general framework to match patterns in the data payload of IoT protocols in order to detect what is considered personal and/or private. Privacy Tool adopts an incremental approach by using plugins. These are components in charge of defining the privacy "patterns" and the best strategy to detect them. Following this approach, our tool can easily integrate new application protocols, and, simultaneously, tune or add other patterns over the time.

FLY faster through an innovative and robust risk-based SECurity tunnel

http://www.fly-sec.eu/

Acronym:	Flysec
Reference:	R-AGR-0586
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	5,000,000.00 €
Duration:	1 May 2015 – 30 Apr 2018
Members:	• Thomas ENGEL (Principal Investigator) • Detlef FUEHRER (Researcher) • Aurel MACHALEK (Researcher) • David NAVEH (Researcher) • Stefanie OESTLUND (Project Coordinator)
Area:	Communicative Systems
Partners:	• C.G - SMARTECH LTD. • Elbit Systems Ltd. • Embry-Riddle Aeronautical University • emza visuel sense Ltd. • Epsilon International SA • European Aviation Security Center AV • EXODUS SA • ICTS (UK) Limited

- Luxembourg Airport
- National Centre for Scientific Research - Demokritos

Description

Complementing the ACI/IATA efforts, FLYSEC project aims to develop and demonstrate an innovative integrated and end-to-end airport security process for passengers, enabling a guided and streamlined procedure from the landside to airside and into the boarding gates, and offering for the first time an operationally validated innovative concept for end-to-end aviation security. On the technical side, FLYSEC achieves its ambitious goals by integrating new technologies on video surveillance, intelligent remote image processing and biometrics combined with big data analysis, open-source intelligence and crowdsourcing. Repurposing existing technologies is also in the FLYSEC objectives, such as mobile application technologies for improved passenger experience and positive boarding applications (i.e. services to facilitate boarding and landside/ airside wayfinding) as well as RFID for carry-on luggage tracking and quick unattended luggage handling. Besides more efficient background checks and passenger profiling, FLYSEC aims to implement a seamless risk-based security process within FLYSEC combining the aforementioned technologies with behavioural analysis and innovative cognitive algorithms. A key aspect in the design of FLYSEC risk-based security is applying ethical-by-design patterns, maximizing the efficiency of security controls through passenger differentiation ranging from "unknown" to "trusted", while remaining ethical and fair in the process. Policy, regulatory and standardisation aspects will also be examined in the context of FLYSEC innovative security concept.

Results

In 2017, the SECAN-Lab team together with the project partners set up and integrated all technical components and software modules for a Proof-of-Concept at Schönhagen Airport, Germany. Four scenarios describing typical occurrences in an airport terminal were tested to the full satisfaction of the project partnership. The Assessors of the tests came to very positive conclusions as well. This also includes the Flysec mobile app, which was found very useful by the first passengers who had the opportunity to try and also by the staff of security services on site. The next and the last Flysec demonstration is scheduled for beginning of 2018 at LuxAirport, Luxembourg. Real condition of the Airport will proof all technology developed during the project lifetime.

Mining and Reasoning with Legal Texts

http://www.mirelproject.eu/

Acronym:	MIREL
PI:	Leon VAN DER TORRE
Funding:	European Commission - Horizon 2020
Budget:	1,152,000.00 €
Duration:	1 Jan 2016 – 31 Dec 2019
Members:	• Leon VAN DER TORRE (Principal Investigator) • Livio ROBALDO (Project Coordinator)
Area:	Intelligent and Adaptive Systems
Partners:	• APIS JSC Europe • DLVSystem SRL • INRIA • National ICT Australia Ltd • National University of Córdoba • National University of La Plata • Nomotika SRL • Stanford University • Universidad Nacional del Sur in Bahía Blanca • Università di Torino • University of Bologna • University of Cape Town • University of Huddersfield • Zhejiang University

Description

The MIREL project will create an international and inter-sectorial network to define a formal framework and to develop tools for MIning and REasoning with Legal texts, with the aim of translating these legal texts into formal representations that can be used for querying norms, compliance checking, and decision support. The development of the MIREL framework and tools will be guided by the needs of three industrial partners, and validated by industrial case studies. MIREL promotes mobility and staff exchange between SMEs to academies in order to create an inter-continental interdisciplinary consortium in Law and Artificial Intelligence areas including Natural Language Processing, Computational Ontologies, Argumentation, and Logic & Reasoning.

The Marie Sklodowska-Curie Research and Innovation Staff Exchange (RISE) project "MIREL - MIning and REasoning with Legal texts" (http://www.mirelproject.eu) has been retained for funding under the call H2020-MSCA-RISE-2015, with the overall score of 97.20%. University of Luxembourg is the coordinator of MIREL. Dr Livio Robaldo led the writing of the project and he is currently managing its activities.

Processing legal language for normative Multi-Agent Systems

Acronym:	ProLeMAS
Reference:	I2R-DIR-PEU-15PLMS
PI:	Livio ROBALDO
Funding:	European Commission - Horizon 2020
Budget:	160,800.00 €
Duration:	1 Jun 2015 – 31 May 2017
Members:	• Livio ROBALDO (Principal Investigator) • Leon VAN DER TORRE (Researcher)
Area:	Intelligent and Adaptive Systems

Description

The ProLeMAS project reconnects the textual representation of norms in legal documents with the logical representation of their meaning, in order to improve acceptability by legal practitioners of automatic reasoning on norms. It makes a bridge between deontic logic and natural language semantics, focusing on the modalities and the defeasible conditionals conveyed by norms. More generally, ProLeMAS develops a framework with a natural language processing pipeline able to computationally obtain explicit representations from legal text that is effective and acceptable to lawyers. ProLeMAS opens a new research trend in normative Multi-Agent systems, along three dimensions. First, ProLeMAS enhances the expressive power of deontic logic to formalize the meaning of the phrases constituting sentences, including a wide range of fine-grained intra-sentence linguistic phenomena. Natural language semantics is not part of the NorMAS roadmap, although it has been identified as a critical issue by the current scientific community in deontic logic and normative systems, as witnessed by the special focus on “deontic modalities in natural language” at the DEON 2014 conference. Secondly, ProLeMAS defines a first-order decision theory able to make inferences on norms from legislation as well as agents’ goals and attitudes. Third, ProLeMAS will develop a prototype able to extract obligations from laws and codify them in the chosen object logic. No system developed so far by members of the NorMAS community is capable of processing legal documents available on the Web. The prototype that will be implemented in ProLeMAS will use and extend two specific tools: the TULE parser and the Tacitus system.

Results

The project, now finished, greatly advanced current state-of-the-art in legal informatics, specifically the development of formalisms to represent the se-

mantic of norms found in existing legislation, available in natural language only. This objective was fully achieved by the design of a new logic, called reified Input/Ouput logic, whose definition has been published in the Journal of Logic and Computation [Robaldo and Sun, 2017]. The logic integrates the main insights of Input/Output logic, a well-known deontic framework defined in the past years by professor Leon van der Torre (my supervisor in ProLeMAS) and the reification-based approach of prof. Jerry R. Hobbs designed for Natural Language Semantics, exactly as it was planned in the ProLeMAS project original proposal.

Another relevant publication is [Sun and Robaldo, 2017], which has been published in the Journal of Applied Logic. This work investigates the complexity of Input/Output systems from a general perspectives, in order to study the conditions under which they can be used in practical applications for the legal domain. The importance of the work is of course represented by the aim of building computational systems using large knowledge bases of reified Input/Output logic formalisms.

[Robaldo and Sun, 2017] L. Robaldo and X., Sun: Reified Input/Output logic: Combining Input/Output logic and Reification to represent norms coming from existing legislation, The Journal of Logic and Computation, to appear.
[Sun and Robaldo, 2017] X., Sun and L. Robaldo: On the Complexity of Input/Output Logic, The Journal of Applied Logic, to appear.
[Sun et al, 2017b] X., Sun, X. Zhao, L. Robaldo: Norm-based deontic logic for access control, some computational results, Future Generation Computer Systems, to appear.
[Ajani et al, 2017] G. Ajani, G. Boella, L. Di Caro, L. Robaldo, L. Humphreys, S. Praduroux, P. Rossi, A. Violato: The European legal taxonomy syllabus: A multi-lingual, multi-level ontology framework to untangle the web of European legal terminology , Applied Ontology, Vol. 11, Issue 4.
[Nanda et al, 2017] R. Nanda, L. Di Caro, G. Boella, H. Konstantinov, T. Tyankov, D. Traykov, H. Hristo, F. Costamagna, L. Humphreys, L. Robaldo, M. Romano: A Unifying Similarity Measure for Automated Identification of National Implementations of European Union Directives, in proc. of the 16th International Conference on Artificial Intelligence and Law (ICAIL), London, 2017.
[Adebayo et al, 2017] K. J. Adebayo, L. di Caro, G. Boella and L. Robaldo: Legalbot: a Deep Learning-Based Conversational Agent in the Legal Domain, in proc. of the 22nd International Conference on Natural Language & Information Systems, Liege, Belgium, 2017.

SYSTEMIC ANALYZER IN NETWORK THREATS

https://project-saint.eu/

Acronym: SAINT

Reference: R-AGR-3238

PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	1,998,700.00 €
Duration:	1 May 2017 – 30 Apr 2019
Members:	• Thomas ENGEL (Principal Investigator) • Marharyta ALEKSANDROVA (Researcher) • Stefan SCHIFFNER (Researcher) • Latif LADID (Collaborator) • Andriy PANCHENKO (Scientific Contact)
Area:	Communicative Systems
Partners:	• Archimede Solutions • INCITES CONSULTING SARL • INSTITOUTO TECHNOLOGIAS YPOLOGISTONKAI EKDOSEON DIOFANTOS • KENTRO MELETON ASFALEIAS • Mandat International (International Cooperation Foundation) • MONTIMAGE EURL • National Centre for Scientific Research - Demokritos • Stichting CyberDefcon Netherlands Foundation

Description

SAINT proposes to analyse and identify incentives to improve levels of collaboration between cooperative and regulatory approaches to information sharing. Analysis of the ecosystems of cybercriminal activity, associated markets and revenues will drive the development of a framework of business models appropriate for the fighting of cybercrime. The role of regulatory approaches as a cost benefit in cybercrime reduction will be explored within a concept of greater collaboration in order to gain optimal attrition of cybercriminal activities. Experimental economics will aid SAINT in designing new methodologies for the development of an ongoing and searchable public database of cybersecurity indicators and open source intelligence. Comparative analysis of cybercrime victims and stakeholders within a framework of qualitative social science methodologies will deliver valuable evidences and advance knowledge on privacy issues and Deep Web practices. Equally, comparative analysis of the failures of current cybersecurity solutions, products and models will underpin a model for greater effectiveness of applications and improved cost-benefits within the information security industry. SAINT proposes to advance measurement approaches and methodologies of the metrics of cybercrime through the construct of a framework of a new empirical science that challenges traditional approaches and fuses evidence-based practices with more established disciplines for a lasting legacy. SAINT's innovative models, algorithms and automated framework for objective metrics will benefit decision-makers, regulators, law enforcement in the EU, at national and organisational levels providing improved cost-benefit analysis and supported by tangible and intangible costs

for optimal risk and investment incentives. The resulting ongoing business spin off and the potential for novel research and further studies will be attractive to academia and researchers beyond the lifetime of the project.

Results

For SAINT, UL investigates and establishes accurate indicators and metrics for privacy. This includes theoretical models to be able to compare different privacy enhancing technologies. Moreover, we researched practical indicators for privacy by design. Here, privacy indicators are used to select the right technologies to build new network services and by this improving the cyber-security situation in the future. SAINT is at the beginning of the project lifetime, our future research will result in tools that help to automatically collect and evaluate our new privacy indicators. We also started working on a tool for online estimation of users' privacy level in encrypted networks. UL contributed to the design and dissemination of the SAINT surveys that attempt to understand the current state of the cyber-security and cyber-crime landscape. In particular, the project was presented on Luxembourg Internet Days 2017.

Training Augmented Reality Generalized Environment Toolkit

http://www.target-h2020.eu/

Acronym:	TARGET
Reference:	R-AGR-0588
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	6,000,000.00 €
Duration:	1 May 2015 – 30 Apr 2018
Members:	• Thomas ENGEL (Principal Investigator) • Aurel MACHALEK (Researcher) • Stefanie OESTLUND (Project Coordinator)
Area:	Communicative Systems
Partners:	• Roderick McCall (LIST) • Arttic • ATRISc • Cleveland Fire Authority • Ecole Nationale Superieure de Police • Estonian Academy of Security Sciences

- Fachhochschule der Polizei des Landes Brandenburg
- Fraunhofer Institute for Transportation and Infrastructure Systems
- German Police University
- Guardia Civil
- Inconnect
- Institut de Seguretat Pública de Catalunya
- International Security and Emergency management Institute
- ISCC International Security Competence Centre
- Oslo Centre of Science in Society (OCSS)
- VectorCommand LtD

Description

TARGET will deliver a pan-European serious gaming platform featuring new tools, techniques and content for training and assessing skills and competencies of SCA (Security Critical Agents - counterterrorism units, border guards, first responders (police, firefighters, ambulance services civil security agencies, critical infrastructure operators).

Mixed-reality experiences will immerse trainees at task, tactical and strategic command levels with scenarios such as tactical firearms events, asset protection, mass demonstrations, cyber-attacks and CBRN incidents. Trainees will use real/training weaponry, radio equipment, command & control software, decision support tools, real command centres, vehicles. Social and ethical content will be pervasive. Unavailable real-source information will be substituted by AVR (Augmented/Virtual Reality - multimedia, synthetic role players). Near-real, all-encompassing and non-linear experiences will enable high degrees of dynamics and variability.

The distributed Open TARGET Platform will provide extensible standards driven methods to integrate simulation techniques and AVR technology with existing SCA training equipment and be customisable to local languages, national legal contexts, organisational structures, established standard operational procedures and legacy IT systems. At key training points realtime benchmarking of individuals and teams will be instrumented. TARGET will support inter-agency SCA exercising across the EU and act as a serious gaming repository and brokerage facility for authorised agencies to share training material and maximize reuse and efficiency in delivering complex exercises. TARGET, combining training, content and technology expertise, will be co-led by users and technologists, mainly SMEs. 2 successively developed and trialled versions of the TARGET Solution will support user-technologist dialogue. The TARGET Ecosystem will enable sustainable impact, commercial uptake and synergies at EU level.

Results

The project aims to enable effective Security Critical Agents (SCA) training by developing pan-European training content (6 scenarios was developed in the

course of the project), a TARGET marketplace in order to buy/sell what is available on the TARGET platform as well as associated TARGET products and services. The TARGET platform consist of architecture, development environment, technology components and a store with training content. The first version of the TARGET platform is available. These three elements combine to form the European TARGET Ecosystem for serious gaming, which stretches beyond the scope of the consortium and the duration of the project.

A critical part of the TARGET project is, not only the creation of relevant training technology and scenarios, but also the testing of these solutions for their relevance and suitability for innovating over existing training technology. The approach selected for this evaluation of the technology went along the following process in 2017:

- Analyse and understand existing solutions with end users
- Perform a requirements analysis to see what end users actually needed
- Create technical solutions (oriented around chosen scenarios) around these requirements
- Test these solutions using real exercises at customer sites to see if the requirements are met.

B.2 European Defence Agency Projects

Aid to SItuation Management based on MUtlmodal, MultiUAVs, Multi-level acquisition Techniques

Acronym:	ASIMUT
Reference:	R-AGR-0548-10-Z
PI:	Pascal BOUVRY
Funding:	European Defence Agency
Budget:	640,000.00 €
Duration:	5 Mar 2015 – 4 Mar 2017
Members:	• Pascal BOUVRY (Principal Investigator) • Matthias BRUST (Researcher) • Grégoire DANOY (Researcher) • Martin ROSALIE (Researcher)
Area:	Intelligent and Adaptive Systems
Partners:	• FLY-N-SENSE • FRAUNHOFER IOSB • THALES SYSTEMES AEROPORTES SAS • Université de Bordeaux I

Description

The ASIMUT Project aims at developing innovating algorithms based on learning techniques dedicated to fusion of data provided by airborne sensors embedded in a swarm of UAVs so as to improve the quality and significance of the pieces of information provided to an operator through Detection and Identification processes.

Results

For 2017, the last year of the project, we publish an article [115] that summarizes the activities and results of the ASIMUT project (Aid to SItuation Management based on MUltimodal, MUltiUAVs, MUltilevel acquisition Techniques) carried out by the consortium. It details the objectives of the ASIMUT project: design, implement and validate algorithms that will allow the efficient usage of autonomous swarms of Unmanned Aerial Vehicles (UAVs) for surveillance missions.

Further to the conference paper published in 2016 [10993/28921], we wrote a journal paper that was accepted recently (08/01/2018) for a publication in the Journal of Swarm and Evolutionary Computation (https://www.journals.elsevier.com/swarm-and-evolutionary-computation/); it will be published in 2018. In this article we propose novel mobility models for multi-level swarms of collaborating UAVs used for the coverage of a given area. These mobility models generate unpredictable trajectories using a chaotic solution of a dynamical system. We detail how the chaotic properties are used to structure the exploration of an unknown area and enhance the exploration part of an Ant Colony Optimization method. Empirical evidence of the improvement of the coverage efficiency obtained by our mobility models is provided via simulation. It clearly outperforms state-of-the-art approaches.

In addition, we also develop a website (https://asimut.gforge.uni.lu/) for the promotion of the project. It includes a video of the project, a summary of the development, the list of partners and a list of the publication related to the project.

B.3 European Space Agency Projects

Demonstrator of light-weight application and transport protocols for future M2M applications

Acronym:	M2MSAT
Reference:	R-AGR-3206
PI:	Thomas ENGEL
Funding:	European Space Agency

Budget:	500,000.00 €
Duration:	3 Oct 2016 – 31 May 2018
Members:	• Thomas ENGEL (Principal Investigator) • Luca LAMORTE (Researcher) • Ridha SOUA (Researcher) • Stefanie OESTLUND (Project Coordinator)
Area:	Communicative Systems
Partner:	SES Techcom Services

Description

An increasing number of devices and objects are connected to the Internet. Together with advances in sensor technology and their mass availability, the use of wireless networks drives the increasing penetration of Machine-to-Machine (M2M) communications in many domains, such as security and surveillance, transportation, and energy.

The Internet of Things (IoT) continues to make headlines, with enormous numbers of devices poised to go online in the coming years. Device heterogeneity, low power and memory, and the need to operate unattended for extended intervals on limited battery lifetimes are typical characteristics of M2M/IoT communications. Hence, there is an increasing drive among developers, equipment manufacturers, and users towards open and interoperable light-weight yet efficient M2M/IoT protocols (such as DDS, AMQP, MQTT, JMS, REST, CoAP and XMPP). So far, those protocols have been applied only in terrestrial networks, which are not always available. Thus, there is the need to assess their suitability also in satellite networks, and propose appropriate improvements to increase the share of satellite communications in the M2M/IoT market.

In this context, the project aims to critically review, to design optimization, and to assess in a satellite network testbed, the recent light-weight application and transport protocols proposed for M2M/IoT communications. The results will be actively reported back to relevant standardisation fora.

Results

In 2017, we focused on the problem of performances assessment of the selected IoT/M2M protocols in the reference satellite scenarios, in order to design suitable optimisation.

CoAP and MQTT protocols were studied to understand their basic functionalities, and the main parameters that could affect their performance. To compare the two selected application protocols, we have identified a set of Key Performance Indicators (KPIs) around which we have conducted the simulation study using OpenSAND simulator. In particular, the performances assessment of CoAP and MQTT from a numerical perspective in the first selected scenario has been conducted in terms of end-to-end delay, efficiency and packet delivery

ratio, under different network condition (satellite link disruption, traffic load, packet size, channel contention, etc.). Moreover, we have analysed theoretically the MEO scenario given that OpenSAND does not support the simulation of MEO constellations. Finally, some envisioned optimizations such as the header compressions protocols (ROHC) and security schemes are studied and discussed in the given selected reference scenarios.

The simulations results of the hybrid terrestrial-satellite scenario have been elaborated as a scientific paper that was submitted to WCNC 2018.

B.4 European Union Projects

High-Performance Modelling and Simulation for Big Data Applications

http://chipset-cost.eu

Acronym:	cHiPSet
PI:	Dzmitry KLIAZOVICH
Funding:	European Union - European Cooperation in Science & Technology Action
Duration:	8 Apr 2015 – 7 Apr 2019
Members:	()
Areas:	• Intelligent and Adaptive Systems • Security, Reliability and Trust in Information Technology
Partners:	• Aalesund University College • Cracow University of Technology • Gdansk University of Technology • INRIA • Istituto Superiore Mario Boella • Karlsruher Institut für Technologie • Linköping University • National College of Ireland • Politecnico di Milano • Politecnico di Torino • The University of Manchester • Universidad de Murcia • Università degli Studi di Catania • Université Lille • University of Cambidge • University of Innsbruck • University of La Laguna

- University of Lisbon
- University of Lübeck
- University of Palermo
- University of Pisa
- University of Stirling
- University of Vigo
- University Politehnica of Bucharest
- Warsaw University of Technology

Description

The Big Data era poses a critically difficult challenge and striking development opportunities in High-Performance Computing (HPC): how to efficiently turn massively large data into valuable information and meaningful knowledge. Computationally effective HPC is required in a rapidly-increasing number of data-intensive domains, such as Life and Physical Sciences, and Socioeconomic Systems.

Modelling and Simulation (MS) offer suitable abstractions to manage the complexity of analysing Big Data in various scientific and engineering domains. Unfortunately, Big Data problems are not always easily amenable to efficient MS over HPC. Also, MS communities may lack the detailed expertise required to exploit the full potential of HPC solutions, and HPC architects may not be fully aware of specific MS requirements.

Therefore, there is an urgent need for European co-ordination to facilitate interactions among data-intensive MS and HPC experts, ensuring that the field, which is strategic and of long-standing interest in Europe, develops efficiently – from academic research to industrial practice. This Action will provide the integration to foster a novel, coordinated Big Data endeavour supported by HPC. It will strongly support information exchange, synergy and coordination of activities among leading European research groups and top global partner institutions, and will promote European software industry competitiveness.

Network for Sustainable Ultrascale Computing

http://www.nesus.eu

Acronym:	NESUS
PI:	Pascal BOUVRY
Funding:	European Union - European Cooperation in Science & Technology Action
Duration:	28 Mar 2014 – 27 Mar 2018

Members:
- Pascal BOUVRY (Principal Investigator)
- Sébastien VARRETTE (Researcher)

Partners:
- Alexandru Ioan Cuza University of Iasi
- INRIA
- Jozef Stefan Institute
- Norwegian University of Science and Technology
- Politecnico di Torino
- Technical Unversity of Denmark
- Technische Universitaet Wien
- Universidad de Extremadura
- Universidad de Murcia
- Universidad de Valladolid
- Universität Wien
- Université de Mons, Belgique
- University of Amsterdam
- University of Bergen
- University of Calabria
- University of Cyprus
- University of Innsbruck
- University of La Laguna
- University of Malta
- University of Sarajevo
- University of Tartu
- University Ss Cyril & Methodiuous, Skopje

Description

The NESUS Action will focus on a cross-community approach of exploring system software and applications for enabling a sustainable development of future high-scale computing platforms. In details, the Action will work in the following scientific tasks:

- First, the current state-of-the-art on sustainability in large-scale systems will be studied. The Action will strive for continuous learning by looking for synergies among HPC, distributed systems, and big data communities in cross cutting aspects like programmability, scalability, resilience, energy efficiency, and data management.
- Second, the Action will explore new programming paradigms, runtimes, and middlewares to increase the productivity, scalability, and reliability of parallel and distributed programming.
- Third, as failures will be more frequent in ultrascale systems, the Action will explore approaches of continuous running in the presence of failures. The Action plans to find synergies between resilient schedulers that handle errors reactively or proactively, monitoring and assessment of failures, and malleable applications that can adapt their resource usage at runtime.
- Fourth, future scalable systems will require sustainable data management for addressing the predicted exponential growth of digital information. The Action plans to explore synergistic approaches from traditionally separated communities to reform the handling of the whole data life cycle, in particular:

restructure the Input/Output (I/O) stack, advance predictive and adaptive data management, and improve data locality.
- Fifth, as energy is a major limitation for the design of ultrascale infrastructures, the Action will address energy efficiency of ultrascale systems by investigating, promoting, and potentially standardizing novel metrics for energy monitoring and profiling, modelling, and simulation of energy consumption and CO2 emission, eco-design of ultrascale components and applications, energy-aware resource management, and hardware/software codesign.
- Finally, the Action will identify applications, high-level algorithms, and services amenable to ultrascale systems and investigate the redesign and reprogramming efforts needed for applications to efficiently exploit ultrascale platforms, while providing sustainability.

B.5 External Organisation Funding Projects

Networked SCADA Security

Reference:	R-AGR-0435
PI:	Thomas ENGEL
Funding:	External Organisation Funding
Budget:	841,679.00 €
Duration:	1 May 2012 – 30 Jun 2020
Members:	• Thomas ENGEL (Principal Investigator) • Florian ADAMSKY (Researcher)
Area:	Communicative Systems
Partner:	CREOS

Description

Researchers from the SECAN-Lab group headed by Prof. Dr. Thomas Engel continue their efforts to make industry control systems more secure and resilient against wide range of networks attacks. Together with the Luxembourg utility company Creos, they search for weaknesses within contemporary SCADA deployments using emulation — a method to analyze real-world systems with a high level of details. To this end, the SCADA team researches methods to stay safe and robust in the presence of network attacks.

Results

In 2017, together with the energy company CREOS, we planed and organized the move of the Supervisory Control and Data Acquisition (SCADA) laboratory from

Kirchberg to Belval. In Beval, we build a server room with an air-conditioning system, new racks, and uninterruptible power supply (UPS). This laboratory includes real hardware and software from CREOS, such as IP/MPLS routers and switches and several servers with specialist software.

Additionally, we started to investigate the security of industrial SCADA gateways such as serial-to-ethernet converters of different manufactures. We found several severe security vulnerabilities (CVE-2017-16719, CVE-2017-16715, CVE-2017-14028) for the Moxa NPort 5110/5130 device. In CVE-2017-16719, we found out that the TCP Initial Sequence Numbers (ISN) from Moxa NPort 5110/5130 are predictable. That means, if an attacker can predict the ISN, the attacker can craft network packets that will be accepted in an established TCP connection. Thus, an attacker can inject arbitrary network packets. The ISN should be completely; according to our findings the uptime was used as ISN which can be easily obtained via SNMP.

In CVE-2017-16715, we found out that these devices where using uninitialized memory as padding for network packets. According to RFC 894 the minimum Ethernet frame size is 46 bytes. If packet is smaller than the minimum size, the IP packet "should be padded (with octet of zero) to meet the Ethernet minimum frame size". Instead of octets of zeros, Moxa used uninitialized memory. This vulnerability is called Etherleak in the past and could expose previously sent network packets, which could contain the session ID of an HTTP connection. With a valid session ID, an attacker can get access the web interface to control the device.

In CVE-2017-14028, we found a simple TCP SYN flooding vulnerability. An attacker is able to exhaust memory resources by sending a large amount of TCP SYN packets. We followed the responsible disclosure procedure and communicated all vulnerabilities with ICS-CERT.

Securing Smart Entry Systems

Reference:	R-AGR-3246
PI:	Thomas ENGEL
Funding:	External Organisation Funding
Budget:	30,000.00 €
Duration:	1 Apr 2017 – 30 Mar 2018
Members:	• Thomas ENGEL (Principal Investigator) • Florian ADAMSKY (Researcher)
Area:	Communicative Systems
Partner:	Honda r&d Europe GmbH

Description

A smart key is an electronic device which authorizes the owner of a car to unlock and start the car based on proximity, without the need to physical contact of the key with the car or interaction with the key by the owner. The idea originates from the early ’80s, and it is now used by different manufacturers under different names, e.g., Honda calls it Smart Entry System. A number of scientific publications has shown that these Passive Keyless Entry and Start (PKES) systems are highly vulnerable to relay attacks, where an attacker amplifies or bridges the signal from the key over a distance to the car and is therefore able to unlock and start the car. For this attack, a criminal does not need special knowledge because there are low-coast off-the-shelf products on the market to facilitate the process.

In this project we aim to design a secure authentication protocol that can be used with smart devices such as smartphones or smartwatches to unlock and start the car without active interaction with the device. In order to achieve this, we will analyze different approaches such as Distance Bounding Protocol (DBP) and physical Device Fingerprinting (DFP) for smart devices which prevent relay attacks. Distance Bounding Protocols are cryptographic protocols that use the transmission time as an indicator to find out how far away a device is. Device Fingerprinting uses physical device characteristics in order to tell legitimate and relay devices apart. To support a wide range of smart devices, we will utilize Commercial off-the-shelf (COTS) wireless technology such as wireless LAN or Bluetooth and secure them to prevent relay attacks.

Results

We evaluated different techniques to measure the distance with wireless LAN (802.11b) securely and precisely. The most promising technique is to measure the signal propagation delay. Wireless signals are electromagnetic waves and therefore propagate with the speed of light. Thus, we need nanosecond resolution to measure the distance. We analyzed different clock sources such as Time Stamp Counter (TSC), High Precision Event Timer (HPET), Time Stamp Function (TSF), and PCAP timestamp. Additionally, we modified the kernel driver to take a timestamp with above mentioned clock sources when a frame is sent and received. We conducted several experiments outside without obstacles and found out that with TSF we can measure the distance with $\pm$ 1-2 meter accuracy.

Study and Optimisation of Inter and Intra-Vehicular Communications through Bluetooth Low Energy

http://www.vehicularlab.uni.lu/projects/enser/

Acronym:	BluVeC
Reference:	R-AGR-0458
PI:	Thomas ENGEL
Funding:	External Organisation Funding
Duration:	1 Apr 2013 – 13 Oct 2017
Members:	• Thomas ENGEL (Principal Investigator) • Walter BRONZI (Doctoral Candidate) • Raphaël FRANK (Scientific Contact)
Area:	Communicative Systems
Partner:	Telindus

Description

Bluetooth Low Energy (BLE) is quickly and steadily gaining importance for a wide range of applications.

In this research we investigate the potential of BLE for Inter and Intra-Vehicular Communications (IVC). This work is motivated by the fact that the deployment of specifically designed IVC technologies such as Dedicated Short Range Communications (DSRC) based on IEEE 802.11p, is taking longer than initially expected.

It is our belief that the ubiquity of BLE enabled mobile devices would allow a fast deployment of new Intelligent Transportation Systems (ITS) in a near future. This is especially true as more and more car manufacturers provide interfaces to tightly integrate mobile devices within new vehicles (e.g. Apple CarPlay, Android Auto) and that by 2018, 90 percent of mobile devices are expected to support the low energy standard.

BLE advantageous low energy requirements allow services to run in the background on battery powered mobile devices without limiting the usage of other applications.

Although this technology has originally been designed for short-range single hop communications, we plan on optimizing its use in a vehicular context with possible deployment alongside other technologies (DSRC/5G).

Results

During 2017, we worked on the BluVeC project extending the statistical analysis of the dataset, that was collected in 2016 by using BlueScanner, to further improve the feature selection for our environment classifier. Improved features allowed us to achieve more accurate results when identifying different road categories based on Bluetooth discovery data alone (up to 88% accuracy with two classes). Furthermore, we studied various possibilities to classify speed by creating a brand new feature selection based on the same collected data.

Various labels were identified in order to represent the most common speed categories within the road infrastructure in Luxembourg. We ultimately concluded that more data (a new data collection campaign) was required for this step. In a parallel study, we also explored the coexistence aspect of Bluetooth with other 2.4GHz wireless technologies (such as WiFi) and how different level of interference impact the Bluetooth (Classic and Low energy) communication channels.

B.6 Fonds National de la Recherche Projects

Integration of distributed controllable renewable generators in the Luxembourgish electricity system including innovative micro-hydrokinetic turbines

PI:	Juergen SACHAU
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche
Duration:	1 Mar 2013 – 31 Mar 2017
Members:	• Juergen SACHAU (Principal Investigator) • David NORTA (Doctoral Candidate)
Area:	Communicative Systems
Partner:	RWTH Aachen University

Description

Development of a hydrokinetic turbine prototype. Based on the oscillating hydrofoil approach a turbine will be built in Luxembourg and tested in a canal in Aachen at the RWTH Aachen University. Additionally, an energy economic analysis for the turbine prototype for Luxembourg will be done for Luxembourg for different renewable energy scenarios.

Coevolutionary HybRid Bi-level Optimization

Acronym:	CARBON
Reference:	I2R-DIR-PFN-11AFRT
PI:	Pascal BOUVRY
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD

Duration:	3 Jan 2015 – 3 Jan 2019
Members:	• Pascal BOUVRY (Principal Investigator) • Grégoire DANOY (Collaborator) • Emmanuel KIEFFER (Doctoral Candidate)
Area:	Intelligent and Adaptive Systems

Description

Multi-level problems are problems involving several different decision makers. In particular, bi-level problems engage two types of decision makers "playing" iteratively. The first decision maker is referred to as the leader while the second is the follower. Bi-level programs found their root in Game theory (Stakelberg equilibrium) and have a wide range of applications. They have been proved NP-hard even for convex leader and follower problems. Convexity gave us resolution tools in the single-level case but now we have to face this problem without this set of tools. When convexity cannot be assumed, metaheuristics are employed. Coevolutionary algorithms are well adapted to the structure of bi-level problems. They are a special kind of evolutionary metaheuristics designed to use collaborative or competitive metatheurisrtics working in parallel to find the optimal solution. We propose a novel approach which consists of hybridizing coevolutionary algorithms with exact approaches to take advantage of the research results made in exact decomposition techniques. According to these new hybrid and coevolutionary algorithms, we want to tackle the Cloud Pricing Problem. The latter is nowadays a real need for Cloud providers (and brokers) where optimal prices could be deduced by applying bi-level models.

The research will thus focus on:

- The development of a set of hybrid and coevolutionary bi-level algorithms
- The Cloud Pricing problem will be modeled as a bi-level problem (Cloud provider – customer) and solved by using the hybrid and coevolutive set mentioned before.

Results

*On Bi-level approach for Scheduling problems [***10993/28915***]:* Hierarchical optimization is concerned with several nested levels of optimization problems binding decision makers. Bi-level optimization is a particular case involving two nested problems representing two decision makers who control their own set of decision variables. The first decision maker referred to as the leader takes the first decision which restricts the second decision maker referred to as the follower. In response to it, the follower will try to react optimally to the leader's decision. This modelling pattern may lead to collaboration or competition between them. Closely related to Game Theory (Stackelberg games), bi-level strategies are more realistic since they do not overestimate the objective fitness when decision makers may have an impact on each other. Bi-levels modelling has been proposed for different kinds of problems (e.g. supply-chain management, network optimization, structural optimization). One of the most

studied bi-level problems is the Toll setting problem which consists in finding optimal toll locations knowing that network users try to minimize their travel cost. By considering the possible reactions of the network users, the authority operating tolls is able to maximize its revenue and avoid a situation discouraging network users to take highways. Despite the fact that the literature on scheduling is very rich, few scheduling problems have been modelled using bi-level representations. We propose here a survey on scheduling using bi-level models and show the necessity to develop new optimization tools to solve them.

*Co-evolutionary approach based on constraint decomposition [***10993/28914***]:* Practical optimization problems are often large constrained problems in which the generation of feasible solutions still represent an important challenge. Population-based algorithms (e.g. genetic algorithm) are natured-inspired methods which experience a real success when solving free optimization problems. Nevertheless when some decision variables are strongly linked through constraints, it may be very difficult to generate feasible solutions with standard evolutionary operators (e.g crossover, mutation). The initialization of the first population might also be a brainteaser and often rely on some random procedures. It is obvious that it is not possible to guaranty feasibility in these conditions. Penalty factors are thus added to the tness function to disadvantage non-feasible solutions. Nevertheless, they are hard to define and strongly depend on the considered instance. A large penalty factor will definitely drive solutions to the feasible decision set while a small factor will not be enough to discriminate non-feasible solutions. Penalty factors do not solve the problem of generating feasible solutions, they only penalize non-feasible ones. If the evolutionary operators are not able to generation new valid solutions, the penalty factor will not help. In some cases, one can also observe that a feasible solution with poor fitness can be rejected in favor of a non-feasible one which are particularly closed to the feasible decision set. In this paper, we are going to describe a new approach to fix this issue. This method is based on two phases. The first one consists in ensuring a minimum rate of feasible solutions in the initial population while the second one adds a mechanism which is triggered when feasibility falls below this rate during the evolution.

*A novel co-evolutionary approach for constrained genetic algorithms [***10993/28196***]:* Standard evolutionary algorithms are very efficient on unconstrained optimisation problems since evolutionary operators do not generate values outside the decision set. However constrained problems add a new level of difficulty. Various constraints handling techniques have been proposed, such as static or dynamic penalties, but few of them have attempted to handle constraints separately. Indeed, in many combinatorial problems, the conjunction of some groups of constraints makes them very hard. In this paper, a novel type of co-evolutionary algorithm based on constraints decomposition (CHCGA) is proposed. Its principle consists in dividing an initial constrained problem into a sucient number of sub-problems with weak constrained domains. Generally at this stage, it is trivial to obtain feasible solutions. Then, each of these sub-problems is evolved in order to increase their compatibility with another sub-population. When two sub-populations are compatible, i.e. they contain enough mutually feasible solutions, these two sub-populations merge and the process continues until reaching a single population representing the initial, globally constrained domain. Then, this population is used as initial population

for one selected metaheuristic, a genetic algorithm in this work. Experimental results on the Cloud Brokering optimization problem have demonstrated a strong solution quality gain compared to a standard genetic algorithm.

*Hybrid Mobility Model with Pheromones for UAV detection task [***10993/30387***]:* Over the last years, the activities related to unmanned aerial vehicles have seen an exponential growth in several application domains. In that context, a great interest has been devoted to search and tracking scenarios, which require the development of novel UAV mobility management solutions. Recent work on mobility models has shown that bio-inspired algorithms such as ant colonies, have a real potential to tackle complex scenarios. Nevertheless, most of these algorithms are either modified path planning algorithms or dynamical algorithms with no a priori knowledge. This paper proposes H3MP, a hybrid model based on Markov chains and pheromones to take advantage of both static and dynamic methods. Markov chains are evolved to generate a global behavior guiding UAVs to promising areas while pheromones allow local and dynamical mobility management thanks to information sharing between UAVs via stigmergy. Experimental results demonstrate the ability of H3MP to rapidly detect and keep watch on targets compared to random and pheromone based models.

*A Novel Co-evolutionary Approach for Constrained Genetic Algorithms [***10993/28196***]*: In this paper, a novel type of co-evolutionary algorithm based on constraints decomposition (CHCGA) is proposed. Its principle consists in dividing an initial constrained problem into a sufficient number of sub-problems with weak constrained domains where feasible solutions can be easily determined. One subpopulation for each sub-problems are then evolved independently and merged when they become compatible with each other, i.e. they contain enough mutually feasible solutions. Experimental results on the Cloud Brokering optimization problem have demonstrated a strong solution quality gain compared to a standard genetic algorithm.

A new Co-evolutionary Algorithm Based on Constraint Decomposition [166]: Handling constraints is not a trivial task in evolutionary computing. Even if different techniques have been proposed in the literature, very few have considered co-evolution which tends to decompose problems into easier subproblems. Existing co-evolutionary approaches have been mainly used to separate the decision vector. In this article we propose a different co-evolutionary approach, referred to as co-evolutionary constraint decomposition algorithm (CCDA), that relies on a decomposition of the constraints. Indeed, it is generally the conjunction of some specific constraints which hardens the problems. The proposed CCDA generates one subpopulation for each constraint and optimizes its own local fitness. A sub-population will first try to satisfy its assigned constraint, then the remaining constraints from other subpopulations using a cooperative mechanism, and finally the original objective function. Thanks to this approach, subpopulations will have different behaviors and solutions will approach the feasible domain from different sides. An exchange of information is performed using crossover between individuals from different subpopulations while mutation is applied locally. Promising mutated features are then transmitted through mating. The proposed CCDA has been validated on 8 well-known benchmarks from the literature. Experimental results show the relevance of constraint decomposition in the context of co-evolution compared

to state-of-the-art algorithms.

A new modeling approach for the biobjective exact optimization of satellite payload configuration [56]: Communication satellites have the crucial role to forward signals to customers. They filter and amplify uplink signals coming from Earth stations to improve the signal quality before reaching customers. These operations are performed by the payload component of the satellite which embeds reconfigurable components (e.g. switches). These components route signals to appropriate signal processing components (e.g. amplifiers, filters) and lead amplified signals to the output antenna. In order to route the channels that compose signals, satellite engineers can remotely modify switch states. These are typically updated when one or more new channels must be connected or when failures occur. However satellites embed always more switches to answer customer demands, which makes their reconfiguration time-consuming and error-prone without appropriate decision aid tools. Power transmission is a crucial objective to ensure a maximum quality of service at reasonable cost. This is why satellite operators aim at minimizing incoming power signals while guaranteeing a maximum factor of amplification at the output antenna. This problem is referred to as the Satellite Payload Power problem. Previous works have outlined the difficulty to solve exactly large instances of this problem. This work proposes to improve the existing mathematical formulation of the switch network. We show that it can be modelled as a static network and switch states can be deduced after optimization, thus limiting the combinatorial explosion. Computational experiments on different sizes of realistic instances using the adaptive ϵ-constraint method demonstrate the computational time gain with this new model and the possibility to solve larger instances.

Bayesian Optimization Approach of General Bi-level Problems [167]: Real-life problems including transportation, planning and management often involve several decision makers whose actions depend on the interaction between each other. When involving two decision makers, such problems are classified as bi-level optimization problems. In terms of mathematical programming, a bi-level program can be described as two nested problems where the second decision problem is part of the first problem's constraints. Bi-level problems are NP-hard even if the two levels are linear. Since each solution implies the resolution of the second level to optimality, efficient algorithms at the first level are mandatory. In this work we propose BOBP, a Bayesian Optimization algorithm to solve Bi-level Problems, in order to limit the number of evaluations at the first level by extracting knowledge from the solutions which have been solved at the second level. Bayesian optimization for hyper parameter tuning has been intensively used in supervised learning (e.g., neural networks). Indeed, hyper parameter tuning problems can be considered as bi-level optimization problems where two levels of optimization are involved as well. The advantage of the bayesian approach to tackle multi-level problems over the BLEAQ algorithm, which is a reference in evolutionary bi-level optimization, is empirically demonstrated on a set of bi-level benchmarks.

Evaluation of Authenticated Ciphers

Acronym:	EAC
Reference:	I2R-DIR-AFR-090000
PI:	Alexei BIRYUKOV
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD
Duration:	1 May 2015 – 31 Mar 2019
Members:	• Alexei BIRYUKOV (Principal Investigator) • Aleksei UDOVENKO (Collaborator)
Area:	Information Security

Description

Authenticated Encryption is an important and actively researched field of cryptography. This work will be closely related to the CAESAR competition of authenticated ciphers. The goal of the CAESAR competition is to select a portfolio of AE schemes suitable for various use cases and having strong cryptanalytic work done. There is no de facto standard for authenticated encryption and CAESAR winners may become such standards. The main goal of this research is to analyze CAESAR competition candidates and therefore to improve quality of the competition's results. Another objective is to develop new cryptanalysis methods and combine and generalize existing ones.

NAPEGRN

Acronym:	NAPEGRN
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD
Duration:	15 Jan 2014 – 14 Jan 2017
Member:	Sjouke MAUW (Principal Investigator)

Stream Mining for Predictive Authentication Under Adversarial Influence

PI:	Radu STATE
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD
Budget:	138,000.00 €

Duration:	11 Nov 2014 – 14 Nov 2017
Members:	• Radu STATE (Principal Investigator) • Christian HAMMERSCHMIDT (Doctoral Candidate)
Area:	Communicative Systems
Partner:	neXus

Symbolic verification of distance-bounding and multiparty authentication protocols

Acronym:	DBMP
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD
Budget:	119,943.00 €
Duration:	1 Jun 2015 – 31 May 2018
Members:	• Sjouke MAUW (Principal Investigator) • Rolando TRUJILLO RASUA (Collaborator) • Jorge Luis TORO POZO (Doctoral Candidate)
Area:	Information Security

Description

Formal methods are the most reliable approach to exhaustively verify the security of cryptographic protocols. As new applications arise, new security goals and protocols may be required and ultimately, new formal approaches aimed at verifying those protocols ought to be proposed. With the boom of wireless technologies, distance bounding protocols have gained in popularity as a countermeasure against different types of distance-based attacks, such as mafia fraud, distance fraud, terrorist fraud, and distance hijacking. That is why recent efforts have been made on the development of formal approaches for the security analysis of distance bounding protocols. All these approaches have in common that distance is modeled by introducing either timestamps or a global clock into the model. We claim that most (or maybe all) distance-based attacks proposed up-to-date can be modeled in a symbolic partially-ordered approach, that is to say, in a model that does not explicitly introduce time or location in absolute terms. In this project we will extend the security model and operational semantics of the protocol verification tool Scyther in order to capture different types of distance-based attacks. Differently to previous models, we plan to define the notion of proximity as an ordering predicate on the trace of messages during a protocol session. We will thus study the relation between classical security properties, e.g., aliveness and agreement, and distance-based attacks. The extended model will be used for the formal analysis of both distance bounding

and multiparty authentication protocols. Finally, we will design and implement model-checking algorithms so as to provide the Scyther tool with the ability to verify distance-based attacks.

Timing-aware Model-Based Design with application to automotive embedded systems

Acronym:	EARLY
PI:	Nicolas NAVET
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD
Budget:	119,943.00 €
Duration:	1 Oct 2015 – 30 Sep 2018
Members:	• Nicolas NAVET (Principal Investigator) • Sakthivel Manikandan SUNDHARAM (Doctoral Candidate)
Areas:	• Computational Sciences • Security, Reliability and Trust in Information Technology

Description

MBD is the use of models as the main artefacts to drive the development of systems. It has been profoundly reshaping and improving the design of software-intensive systems, and embedded systems specifically. However, the support for formal verification in the time-domain is mainly non-existing, especially in the early phases of the development cycle. This may be a threat to the safety because at run-time departures from the intended behaviour can be caused by insufficient computational resources. This Phd project explores a novel approach based on model-interpretation to provide support for resource usage estimation and integrate time-domain verification in the early phases of MBD.

Transparent Yet Private Access to Medical Data

Acronym:	TYPAMED
Reference:	FNR/AFR project 7842804
PI:	Peter Y. A. RYAN
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD
Duration:	1 Dec 2014 – 30 Nov 2017
Members:	• Peter Y. A. RYAN (Principal Investigator)

- Dayana PIERINA BRUSTOLIN SPAGNUELO (Doctoral Candidate)
- Gabriele LENZINI (Co-Investigator)

Description

Several pilot tests show that patients who are allowed to access their medical data commit more seriously to therapies and health programs. This finding is particularly relevant in medical research programs aiming at cross-sectional and longitudinal studies on patient cohorts (Luxembourg has recently established one of such programs to monitor the stratification of Parkinson's disease.) For the success of such programs, the commitment of patients and of patient organizations are of pivotal importance. However, letting patients accessing medical records raises many security concerns and creates tension among conflicting requirements. This research project (for a Ph.D.) has the objective to understand precisely such conflicts, and to study and design access control mechanisms that are socio-technically secure, that is secure not only at the technical level, where data management and communication protocols run, but also at a non-technical level, where richer human protocols and behavioural factors are in place. So, for instance, if on one hand patients' access should be controlled so that unauthorised disclosure and modifications are not allowed within the data they are entitled to access, on the other hand, patients should have control over their own data, who accesses it and for what purpose - a right that EU regulations are already trying to enforce.

The challenge comes from the fact that patients are not ICT (Information and Communication Technologies) experts. Access control mechanisms should be effective, but not hard to use or this will compromise a patient's active participation. But the same mechanisms should be transparent to let patients know what happens to their data, how secure they are, and be informed that their data are handled appropriately, reassuring them that their involvement in sensitive research programs will not cost them higher prices in terms of intrusions into their lives.

This Ph.D. project, a collaboration between SnT and LCSB, the Univ. Federal de Santa Catarina (BR), and Univ. of Porto (PT) intends to look at the socio-technical security problems concerning a secure access and use of medical data from patients. It will study access control and data confidentiality mechanisms and implementations, with the specific perspective that those solutions should be usable by inexpert patients and should inspire an honest sense of trust. In so doing, this research goes beyond understanding the security requirements of the technical protocols that realize a secure and confidential remote access to data, requirements widely studied elsewhere. Instead, it advocates studying the human-scale ceremonies in which those protocols are integrated. It will use both traditional expertise and knowledge in the design of secure systems and protocols, and more advanced methodologies suitable for a socio-technical analysis of security and trust.

B.7 Fonds National de la Recherche and Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services Projects

ILNAS - UL/SnT Research Programme on Digital Trust in SmartICT

https://smartict.gforge.uni.lu

Acronym:	Smart ICT
Reference:	R-AGR-3239-10-Z
PI:	Pascal BOUVRY
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD, Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services
Budget:	1,742,000.00 €
Duration:	1 Jan 2017 – 31 Dec 2020
Members:	• Pascal BOUVRY (Principal Investigator) • Grégoire DANOY (Researcher) • Matthias BRUST (Post-Doc) • Chao LIU (PhD student) • Nader SAMIR LABIB (PhD student)
Areas:	• Information Security • Intelligent and Adaptive Systems • Security, Reliability and Trust in Information Technology

Description

Following the successful launch of the University Certificate "Smart ICT for business innovation" in September 2015 and the creation of a new Master's degree in partnership with the Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS); the interdisciplinary center for security reliability and trust (SnT) and ILNAS entered a partnership to jointly develop Luxembourg as a European centre of excellence and innovation for secure, reliable, and trustworthy Smart ICT systems and services.

Research Pillars

With emphasis on digital trust for smart ICT and the related standardization efforts, the scientific research in the context of this joint program focuses on the three main pillars of, Big Data & Analytics, Internet-of-Things (IoT), Cloud Computing and has the following objectives:

- "Smart ICT for business innovation" certificate. The joint research programme is of primary importance at national level, as it will serve to consolidate and sustain the "Smart ICT for business innovation" certificate, while implementing the project of a new Master in Lifelong Learning in the field "Smart ICT for Business Innovation".
- Smart ICT and Standardization. Creating an innovative environment on digital trust for smart ICT and the related standardization efforts with its core pillars Big Data & Analytics, Internet-of-Things (IoT), Cloud Computing.
- Big Data & Analytics. One goal is standardization of annotated clinical data in the context of international biomedical research, with CDISC as an example. Secondly, efficiency and confidentiality of Big Data integration at an international level has to be achieved. Data exchange procedures and formats are needed to improve the efficiency of Big Data sharing and data integration.
- Internet-of-Things (IoT). Standardization in the field of drones is still recent with no final standard yet released. The objective is to investigate the use of UAV drones in the context of homogeneous and heterogeneous drone fleets. Ensuring the proper functioning of the fleet raises new problems of optimization at the level of the communications based on the future dedicated protocols.
- Cloud Computing. The objective is to provide tools for analyzing and comparing prices offered by different Cloud providers. A thorough study of the different pricing methods of suppliers' services is therefore required. Cloud service pricing models will be developed to enable brokers to automatically be determining the best service selection strategy(s) according to customer criteria.

B.8 Fonds National de la Recherche Projects

Subjective and Objective Uncertainty in Description Logics

Acronym:	SOUL
PI:	Giovanni CASINI
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche Postdoc
Duration:	1 Jul 2015 – 30 Jun 2017
Member:	Giovanni CASINI (Principal Investigator)

Area: Intelligent and Adaptive Systems

Description

Description Logics (DLs) are a major application-oriented research topic in Knowledge Representation and AI. They are used for modeling ontologies in many different domains (e-commerce, e-science, medicine, ...). Whereas in the past, research has focused on strict taxonomies, there are a number of areas where uncertainty has to be taken into account. The present proposal plans to investigate uncertainty in DLs on a very general level.

Because detailed and reliable quantitative information is not always available, it is necessary to consider not only probabilistic knowledge, but also more qualitative uncertain information. It may be represented by defeasible rules interpreted by suitable plausibility measures (possibilistic/Spohn's ranking functions), which have been investigated in nonmonotonic reasoning, but hardly applied to DLs. Particular attention will be paid to the DL-specific separation between general conditional information (TBox), and the agent's information about specific individuals (ABox). This approach becomes more challenging when dealing with uncertainty, since the objective level, presenting general shared defeasible conditional information, may conflict with the subjective level, modeling the conditional beliefs of an agent. The intermediate expressivity of DLs is an appropriate context to investigate the interaction between both levels.

The goal is to develop, analyze, and evaluate methods and implementable algorithms for attributing in a justifiable and rational way degrees of plausibility/belief to A-Box assertions about specific individuals, which amounts to complete the A-Box inductively based on defeasible/uncertain information from the T-Box.

Results

The project terminated on 31/06/2017. The project's aim was the investigation of uncertain qualitative reasoning in Description Logics: because detailed and reliable quantitative information is not always available, it is necessary to consider not only probabilistic knowledge, but also more qualitative uncertain information. Particular attention has been paid to the DL-specific separation between general conditional information (TBox), and the agent's information about specific individuals (ABox). This approach becomes more challenging when dealing with uncertainty, since the objective level, presenting general shared defeasible conditional information, may conflict with the subjective level, modeling the conditional beliefs of an agent. The intermediate expressivity of DLs is an appropriate context to investigate the interaction between both levels.

The goals of the project have gone under only minor modifications, and relevant results have been attained in all of them. The most relevant publications in 2017 connected to this project are:

- Casini G., Meyer T. (2017) 'Belief Change in a Preferential Non-monotonic Framework' in *Proceedings of the 26th International joint Conference on Artificial Intelligence (IJCAI-17)*, AAAI Press.
- Cramer M., Casini G. (2017) 'Postulates for Revocation Schemes', in *Principles of Security and Trust. Proceedings of the 6th International Conference POST 2017*, LNCS 10204, Springer, pp. 232-252.

Functional Encrypted Secure Systems

Acronym:	FESS
PI:	Vincenzo IOVINO
Funding:	Fonds National de la Recherche - CORE - Core Junior
Duration:	1 Dec 2016 – 30 Nov 2019
Members:	• Vincenzo IOVINO (Principal Investigator) • Najmeh SOROUSH (PhD student)

Description

Traditional public-key encryption is an invaluable tool for the Web and is used by billions of users everyday for secure communication. Notwithstanding, traditional public-key encryption is an all-or-nothing concept: if you have the secret-key you can decrypt the ciphertext, otherwise you can not recover any information of the encrypted plaintext.

This is becoming a limitation nowadays.

In fact, the Internet 2.0 is moving towards the emerging paradigm of cloud computing, in which the users delegate their data to a cloud server and need to compute functions over the encrypted data.

For these applications the notion of traditional encryption is unsatisfactory.

When the data are encrypted the server needs a secret key to decrypt them but giving the secret key to the server enables it to learn all information not just the result of the computation over the encrypted data, as the users wish.

Functional cryptography allows to selectively control the amount of information that the users can decrypt, thus enabling novel and powerful applications. Software obfuscation is a tightly related primitive that allows to "obfuscate" a computer program so as to make it sufficiently unintelligible while preserving its functionality. This primitive showed recently its tremendous power and many open problems in cryptography were solved using it.

In this project, we will try to advance the area of functional cryptography and software obfuscation by tackling known problems, proposing and solving new ones, and finding new applications for these powerful primitives.

A Theory of Matching Sessions

Acronym:	AtoMS
PI:	Peter Y. A. RYAN
Funding:	Fonds National de la Recherche - CORE
Duration:	1 May 2015 – 30 Apr 2018
Members:	• Peter Y. A. RYAN (Principal Investigator) • José Miguel LOPEZ BECERRA (PhD student) • Dimiter OSTREV (Research Associate) • Marjan SKROBOT (Research Associate)
Area:	Information Security

Description

Authenticated Key Exchange protocols (AKEs) are cryptographic protocols that allow two or more parties to jointly compute a shared session key over an insecure public channel. This key can subsequently be used as input to other algorithms in order to provide various secure services for and between said parties.

Ever since the advent of provable security, an enormous amount of research has been done to define ever-stronger complexity-theoretic security models to capture desirable AKE properties. However, consensus has yet to be established over which models are the most suitable, both in theory and practice.

Several modelling artefacts are at the heart of this problem. First of all, provable security has not yet yielded a unified definition for what it means for parties running a protocol to have established matching sessions. Many different ad hoc avenues have been proposed to deal with this (matching conversations, pre-established or post-established sessions identities, matching functions, etc.) but they often introduce artificial subtleties that yield incompatibility results between models that seem otherwise acceptable. Secondly, a fundamental definition of internal state information is also lacking; this introduces even more difficulties in comparing models that authorize the attacker to obtain various forms of this internal state (unerased internal state revealing, session state revealing, ephemeral key revealing, etc.). Furthermore, internal state revealing seems to be widely more-or-less hard to deal with depending on the model's underlying flavor, i.e., whether it is indistinguishability-based or simulation-based.

We strongly believe that the above-mentioned discrepancies rest on something that is fundamentally unified, and with this proposal we wish to undertake the tasks of 1) discovering and studying this mathematical lowest common denominator and 2) using the outcome of this study to find some order in the vast landscape that is AKE security modelling, and uncover the core governing observed incompatibility results. Our goal is to conduct this study 1) independently of the authentication mechanism used (PKI-based, password-based, attribute-based,

etc...) and 2) independently the underlying intractability assumption (group-based, lattice-based, quantum-based etc.).

Incorporating quantum key distribution to the study is particularly promising because the interface between the quantum phase and the classical phase within such protocols is highly under-investigated. Furthermore, the threat models in which quantum proofs of security are established are not clearly defined. How to solve these problems will certainly bring further insight to AKE security modelling as a whole.

Attack-Defence Trees: Theory Meets Practice

Acronym:	ADT2P
Reference:	C13/IS/5809105
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - CORE
Budget:	494,000.00 €
Duration:	1 Sep 2014 – 31 Aug 2017
Members:	• Sjouke MAUW (Principal Investigator) • Ravi JHAWAR (Collaborator)
Area:	Information Security
Partners:	• Sintef • THALES Research & Technology

Description

Threat and risk analysis are crucial steps in developing secure and usable ICT solutions. An optimal security assessment methodology should combine sound, mathematical foundations with practical and user friendly criteria, which explains their increasing popularity over the last decade.

Attack–defense trees (ADTrees) augment attack trees by including defensive measures into the model. They provide the means to qualitatively and quantitatively assess security. The extended formalism allows for an improved analysis, without however requiring additional computational power.

The objective of the ADT2P project is to elevate the attack–defense tree methodology to an industrially applicable security analysis framework and to integrate it with standard risk assessment tools. In order to achieve this goal, fundamental research as well as practical validation will be performed. ADTrees will be extended with additional features that are necessary to model real-life scenarios. This will include introducing the notions of actors and objects as well as defining dedicated security measures, such as risk and impact. New algorithms that can cope with large-scale models as well as methods to construct ADTrees

from generic attack and defense patterns will be designed. For this, the automatic composition of models will be investigated. Finally, a new version of ADTool, a software tool supporting the ADTree formalism, will be released.

The ADT2P project will build upon the expertise of ADTrees, which was gained within the FNR CORE project ATREES (http://satoss.uni.lu/projects/atrees/). Collaboration with the industrial partners SINTEF and THALES will ensure that the proposed methodology will be highly usable and practical. By integrating the project results into existing security and risk assessment solutions, ADT2P will assist small and mid-size auditing and consulting companies in providing better and more accurate security assessment.

Automated Program Repair using Fix patterns Learned from Human-written Patches

Acronym:	FIXPATTERN
PI:	Dongsun KIM
Funding:	Fonds National de la Recherche - CORE
Budget:	499,000.00 €
Duration:	1 Dec 2015 – 30 Nov 2018
Member:	Dongsun KIM (Principal Investigator)
Area:	Software and Systems

Description

Patch generation is one of the important tasks in software maintenance. However, it is the least explored area while a large number of research work have been conducted for other debugging activities such as fault localization and prioritization . In practice, debugging cannot be completed without patch generation even if a fault is accurately localized or efficiently prioritized.

In addition, patch generation is recognized as an essential task in software development since most contemporary software systems inevitably contain bugs that need to be fixed. As the size and complexity of software systems get larger and higher, significantly more number of bugs are found and reported. Naturally, the corresponding cost for resolving the bugs is rapidly increasing.

To minimize time and cost spent fixing bugs, an automated program repair technique must be devised. Even if this approach may fix a certain portion of bugs, it can largely mitigate burden for debugging so that developer can focus on more creative activities. In addition, the quality of software can be improved as the number of bugs is reduced. This strongly motivates the project, FIXPATTERN, an automated technique for patch generation.

The FIXPATTERN project aims at presenting new approaches to automated pro-

gram repair. First, the project devises a novel pattern-based repair technique learned from human-written patches. This technique can outperform existing techniques based on random mutation with respect to patch quality and readability. Second, this project proposes an semantic-based approach to fix pattern mining for supporting the pattern-based repair technique. Third, a bug classification method is presented by this project. The method is essential since the efficiency of the repair technique can be improved if it can figure out the type of a given bug upfront. Fourth, this project provides the result of a large empirical study on open source projects. One of the main reasons that only few practitioners adopted existing automated repair techniques is that only few evaluation results in practice are available. Thus, it is necessary to provide empirical results studied on a large set of real bugs in practice.

Automatic Bug Fix Recommendation: improving Software Repair and Reducing Time-to-Fix Delays in Software Development Projects

Acronym:	RECOMMEND
PI:	Tegawendé François d Assise BISSYANDE
Funding:	Fonds National de la Recherche - CORE
Budget:	536,000.00 €
Duration:	1 Feb 2016 – 30 Jan 2019
Member:	Tegawendé François d Assise BISSYANDE (Principal Investigator)
Area:	Software and Systems

Description

There is today a momentum of automatic program repair, a research field where various approaches are devised to auto- matically fix programs once a fault is detected. Such approaches attempt to patch a program in a way that makes it pass all the tests. So far, there are no reports of adoption of these approaches in the industry. Indeed, currently, automatic program repair is a young and immature research field, and it has a number of caveats including the fact that: (1) only a limited set of fault types are considered, (2) the proposed fixes can be perceived as alien code and may be out of tune with the rest of the code and (3) there is no guarantee that this fix should be maintained or that it definitely fixes the bug.

The industry standard remains to thoroughly review bug reports and manually write corresponding fixes. Developers thus require new approaches and tools to help them readily understand bug report and infer the appropriate fix so as to (1) reduce the time-to-fix delay and (2) produce homogeneous code that is

easy to maintain.

The RECOMMEND project aims at designing and building a bug fix recommendation system for software development projects. The system will be independent from any programming language. We will leverage information retrieval tech- niques and machine learning techniques to identify, from the history of a project or of similar projects, examples of fixes which can be proposed to address a newly submitted bug report.

Boosting Security and Efficiency in Recommender Systems

Acronym:	BRAIDS
PI:	Qiang TANG
Funding:	Fonds National de la Recherche - CORE
Duration:	15 Apr 2014 – 14 Apr 2017
Member:	Jun WANG (Doctoral Candidate)
Areas:	• Information Security • Intelligent and Adaptive Systems
Partners:	• Jiuyong Li (University of South Australia) • Irdeto

Description

Nowadays, recommender systems play an important role in highly rated commercial websites such as Amazon.com, Facebook, and IMDb, Netflix, Yahoo, and YouTube. Netflix even awarded a million dollars prize to the team that first succeeded in improving substantially the performance of its recommender system. Besides these well-known examples, recommender systems can be found almost everywhere in our daily life. In order to compute recommendations for users, a recommendation service provider needs to collect a lot of personal data from its customers, such as ratings, transaction history, and location. This makes recommender systems a double-edged sword. On one side users get better recommendations when they reveal more personal data, but on the flip side they sacrifice more privacy if they do so.

In this project, we aim at solving the utility-privacy dilemma, namely we want to protect users' privacy to the maximal extent while still enabling them to receive accurate recommendations. We will investigate the realistic privacy notions for recommender systems, and invent privacy-enhancing technologies that allow recommendations to be generated in a secure manner (e.g. generated on encrypted data). We expect that the resulting technologies can also be used in other related services, e.g. privacy-preserving event correlation between different ISPs (Internet Service Providers).

CONtext and conTent Aware CommunicaTions for QoS support in VANETs

Acronym:	CONTACT
Reference:	R-AGR-0643
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - CORE
Budget:	1,346,000.00 €
Duration:	1 Apr 2016 – 31 Mar 2020
Members:	• Thomas ENGEL (Principal Investigator) • Ridha SOUA (Researcher) • Antonio DI MAIO (Doctoral Candidate)
Area:	Communicative Systems
Partners:	• CarPostalSwiss • HES-SO Valais • University of Bern

Description

Vehicular Ad hoc Networks (VANETs) have been receiving a lot of interest from academia, automotive industry, and government, as they hold the potential to enable a wide range of applications and services, improving both safety and comfort on the road.

One of the main drivers of vehicular communications is the support for safety applications (e.g. accident, traffic jam notifications), which together with the more recent autonomous and coordinated driving applications require low end-to-end delay and no packet loss. These applications will share the vehicular network resources with services with very different QoS requirements, such as infotainment services (e.g. live video streams, tourist information).

Due to the volatility of the vehicular environment, VANETs are characterized by a dynamic topology, short-lived intermittent wireless connectivity, and a cooperative and decentralized communication paradigm. All these features make the provision of high levels of QoS in VANETs a challenging task. Even more challenging is the support of a very diverse set of QoS requirements, due to the high heterogeneity of existing and prospective vehicular applications. The main existing approaches to QoS provisioning in VANETs either tackle this issue by focusing on a single layer of the network architecture, or focus on enabling a single specific QoS class of service. The CONTACT project aims at enabling Quality of Service (QoS) support in VANETs by taking a multi-pronged, cross-layer approach, by developing a set of communication techniques, which efficiently adapt, at the same time to the highly volatile and unstable vehicular environment, to content attributes and properties, and to application performance requirements. For this purpose, CONTACT will investigate the use of three

different emerging approaches: Content-Centric Networking (CCN), Software Defined Networking (SDN), and Floating Content (FC). CCN implies introducing (content) name-based addressing instead of host-based addressing. This can be beneficial for communications in highly mobile network scenarios such as vehicular networks, where host addresses are not very meaningful. SDN, with its centralized view of network resources, may help in handling efficiently dynamic (re)allocation of resources/channels, and distribution of content (e.g., by reducing amount of Geobroadcast messages). Finally, FC techniques could be used to improve content availability for delay tolerant communications. The main idea behind CONTACT is to combine and exploit the advantages offered by CCN, SDN and FC, to offer a variety of QoS levels. The improvements in communication reliability, content availability, and end-to-end delay are pursued by adopting strategies based on the type of content (alerts, driving coordination, informational) as well as on its context attributes (such as location of origin, geographical range of interest, time of validity).

Results

The work carried out in 2017 focused on three aspects:

The first aspect investigates content sharing without direct support from the infrastructure using Floating Content (FC). We have addressed the issue of how to control FC performance in a realistic vehicular setting. To this end, we proposed a set of strategies for tuning the size of the AZ, based on the estimation of some key mobility parameters and of target FC performance. Furthermore, we proposed a method to improve FC performances by optimizing the AZ size with the support of a Software Defined Network (SDN) controller, which collects mobility information, such as speed and position, of the vehicles in its coverage range. This study has resulted in two accepted scientific papers (IEEE INFOCOM International Workshop on Mobility Management in the Networks of the Future World and CCNC 2017).

The second aspect investigates the balance between network throughput and user fairness to provide an acceptable Quality of Service (QoS) for infotainment applications. This is challenging in VANETs, which are characterized by a high dynamism of the network topology, volatility of inter-vehicular links, and heterogeneity of the exchanged content. Hence, we proposed a cooperative content dissemination scheme that provides a trade-off between the network throughput and the fairness among users. The novelty of the proposed scheme is twofold: we introduce a new strategy to compute user priority and a new multichannel scheduling algorithm to increase the throughput across all the Service Channels, ensuring load balance. The results of this study was submitted to ICC 2017.

The third aspect tackles the IEEE802.11p standard, which does not provide any mechanism for assigning SCHs to different providers. Thus, we proposed a load-balancing and interference-aware SCH allocation scheme, ESCiVA that is orchestrated by SDN controllers, implemented in the infrastructure. While the previous studies assume the existence of a SouthBound Interface (SBI) between the central controller and the nodes, no standardized SBI for mobile and wire-

less networks is available yet. For this reason, in our approach we adopt the messages already available in IEEE802.11p/WAVE VANETs to collect information about network topology, and exchange SCH requests and SCH schedule between the service providers, and the RSU controllers. By doing so, our solution is feasible and can be implemented in already deployed IEEE802.11p/WAVE networks. The results of this study were published in a scientific paper at Med-Hoc-Net conference.

Data Protection Regulation Compliance

https://www.fnr.lu/projects/data-protection-regulation-compliance/

Acronym:	DAPRECO
PI:	Gabriele LENZINI
Funding:	Fonds National de la Recherche - CORE
Duration:	1 Feb 2017 – 30 Jun 2019
Members:	• Gabriele LENZINI (Principal Investigator) • Livio ROBALDO (Researcher)
Areas:	• Intelligent and Adaptive Systems • Law, stressing European Law • Security, Reliability and Trust in Information Technology

Description

The recently approved General Data Protection Regulation (GDPR) is expected to have a significant impact on the European Digital Single Market because it changes how enterprises have to protect individual's personal data records. To keep their businesses up and running, and to avoid the high fines that the GDPR accounts for not being comply with its provisions, enterprises must be prepared to face the effects of the application of the regulation. Concomitantly, regulators and authorities should understand how to assess compliance with the GDPR.One way to face these challenges, the way this project helps pursue, is to look at current security standards and to check what "correlations" (i.e. relations of the form "a provision x implements a provision y") they have with the GDPR. Such correlations depend on the legal interpretations that exist and may exist of the terms and the provisions in the GDPR and in the security standards. Once these correlations are made clear, an enterprise that implements a standard will benefit from a presumption of compliance with the GDPR with respect to those parts covered by the standard. This is possible because standards provide consolidated practices and are certified by auditors and, therefore, by implementing them, enterprises have an argument of compliance coming from having followed the best practices. The same argument can be used

by regulators and authorities when assessing an enterprise's compliance with the GDPR.However, this solution has a problem that hinders its effectiveness. The GDPR and the standards are available in natural language only. Finding correlations by hand is a hard work even without considering the various legal interpretations, which however we must consider. Without an appropriate methodology and without the support of a knowledge base, the task will become easily beyond capacity for a single enterprise or authority to achieve.This project, DAPRECO, offers a solution to this well-recognized challenge in legal informatics. DAPRECO will represent in an innovative logic, the provisions in the GDPR and the current security standards. The logic, and which we call here ProLeMAS (PROcessing LEgal language in normative Multi-Agent Systems) been recently defined by one of the proponents. The provisions will be correlated via operators of the same logic. ProLeMAS integrates insights from modern formalisms in Deontic Logic and Natural Language Semantics and it has been specifically designed to handle legal norms written in natural language. A key aspect for the innovative character of this project is that ProLeMAS is capable of handling a pluralism of interpretations of its items. It is therefore able to host the plethora of legal interpretations that usually occur in the legal domain, where laws are subject to the different understandings defined by subjects such as judges, regulators, and lawyers. This is possible because the operators of the ProLeMAS logic are defeasible. DAPRECO will output a knowledge base which contains the ProLeMAS correlations expressing the 'formal compliance' (versus 'substantive compliance') of the terms and provisions in the standards and the GDPR. The output of this project is therefore a formal knowledge base, the DAPRECO Knowledge Base, built according to the rigorous methodology that we are going to define fully during the execution of the project. Notably, the legal interpretations of the existing correlations between the security standards and the GDPR can be updated. Different interpretations can be accumulated in our knowledge base, together with the history of their supersedences or their unsolved conflicts, so making the DAPRECO Knowledge Base be the potentially ground-breaking support for professionals and for authorities in the assessment of the compliance of data processing practices with the GDPR's provisions.

ID-based Secure Communications system for unified access in IOT

https://idsecom.itl.waw.pl/

Acronym:	IDSECOM
Reference:	R-AGR-0474
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - CORE

Budget:	692,000.00 €
Duration:	1 Apr 2014 – 31 Mar 2018
Members:	• Thomas ENGEL (Principal Investigator) • Luca LAMORTE (Researcher) • Stefanie OESTLUND (Project Coordinator) • Salvatore SIGNORELLO (Doctoral Candidate) • Radu STATE (Scientific Contact)
Area:	Communicative Systems
Partner:	Warsaw University of Technology

Description

The project IDSECOM aims to build a secure platform for self-management of the Things and services in the Internet of Things environment. The proposed platform brings the functionalities of the so-called ID layer to the network structure and integrates selfmanagement, mobility and security/privacy functionalities in order to create a network infrastructure that offers an easier (and intuitive) access to the IoT (Internet of Things) services. As referred in the project CASAGRAS, "Internet of Things (IoT) is a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities" [Cas09]. Briefly speaking, IoT will be a huge connectivity platform for self-managed devices. A key-challenging question in IoT research is how to identify and access the objects. This issue is solved in the so-called ID layer, which is the common layer for communicating Things. The current solutions for ID layer [Sou09, Swi10, Kos10, IoT@W] are performed by additional protocols, overlay services or infrastructures that need a lot of configuration, have a limited support or may suffer incompatibility between solutions in different networks. In the same way, the current solutions for discovering and accessing the services in IoT are limited to overlay systems. The efforts of this project are directed to build an extended secure ID layer, which solves object and service access in the network itself. Moreover, IDSECOM system extends the current ID layer solutions by (1) addressing not only objects but also services, (2) distributing and facilitating general process as registration and publication of objects/services, (3) adding enhanced security and privacy mechanisms, (4) introducing ID layer self-management functionalities in network level, (5) improving flexibility in multicast/anycast communications at different levels and (6) optimizing information forwarding.

The following proposal is based on the architecture that we presented mainly in [Mon13], and extends its functionalities by providing a self-managed and secure network that is capable of registering, publishing, discovering and managing IDentifiers (ID) attached to objects and services in the IoT. In fact, in [Mon13] we developed the low level operations, i.e., IoT CCNspecific packet forwarding but operations related with IoT services (registration, publication and so on) that are specific of ID layer were discussed superficially. We grouped together challenges and requirements rather than solutions for ID layer operations. This proposal will centre in ID layer-specific operations.

Over ID layer proposed in IDSECOM it will be possible to present primitive services of sensors/actuators or composed services for sharing the resources of different sensor networks. Each service may acquire a public context and location-aware ID (with appropriate hierarchy), by which the service can be easily discovered by remote applications. For building the platform we consider the Software Defined Networking approach and, specifically, OpenFlow, which is widely extended in modern network devices. OpenFlow allows for separation of control and data plane in the devices. This way, dedicated traffic can be processed with appropriate routing rules, which are different than the IP based routing and, on the other hand, the network devices are able to fulfil high level IoT-specific operations. The project partners will investigate new solutions in OpenFlow to ensure IoTspecific operations and ID-based routing into the IoT domain. These solutions may cover new controller functionalities, new OpenFlow rules for treating the ID header and extensions of the OpenFlow protocol, if needed.

At last, for assuring security in the communications inside of the ID layer, we will analyse how switches and controllers can directly collaborate in anomalies discovery (ID layer specific security issue) taken benefit from the efficient organization and routing. On the other hand, we will deal with security in specific modules of ID layer architecture.

Results

Within the project framework, the UL team has been investigating opportunities and security risks of the adoption of two emerging network paradigms, namely, the Software-Defined Networking (SDN) and the Information-Centric Networking (ICN). In particular, the 3rd-year's research activities done by the UL mainly focused on the identification and evaluation of security threats introduced by leveraging SDN and/or ICN solutions in IoT environments via software simulations and experiments on physical testbed.

Among the main outcomes of IDSECOM in 2017, the project consortium has achieved several scientific publications at A- and B-rank international conferences (e.g., IEEE-NCA, IEEE-ICC) and journals (e.g., IEEE Communications Magazine, IEEE Wireless Communications). As foreseen in the original description of work, the IDSECOM members have also actively contributed to the organization of the 3rd DISSECT workshop on "Workshop on Security for Emerging Distributed Network Technologies" held at the 15 th IFIP/IEEE-IM conference in Lisbon. With regard to further dissemination activities, experience on cutting-edge technology grown throughout the project's lifetime has also allowed some project members to give tutorials and lab sessions about emerging SDN technologies at different scientific events (e.g., tutorials on the P4 language were given at IEEE-IM'17 and AIMS'17). Finally, some more open source software contributions have been produced and released to the research community to make the results achieved in the framework of IDSECOM reproducible and to advance the state of the art on the related research topics.

Indoor Navigation with Ambient Radio Signals

Acronym:	INDOORS
Reference:	R-AGR-0176
PI:	Andrei POPLETEEV
Funding:	Fonds National de la Recherche - CORE
Budget:	381,000.00 €
Duration:	1 Jan 2015 – 31 Dec 2017
Members:	• Andrei POPLETEEV (Principal Investigator) • Stefanie OESTLUND (Project Coordinator) • Thomas ENGEL (Collaborator)
Area:	Communicative Systems
Partner:	Microsoft Research

Description

The aim of the project is to explore indoor positioning based on ambient radio signals, such as FM and TV broadcasts, cellular network signals. While GPS has practically solved the problem of outdoor navigation, indoor localization remains an open challenge. Existing systems require dedicated localization infrastructure and work only within instrumented buildings. Broadcasted radio signals, in contrast, are tailored for indoor reception and are widely available even in less populated areas. Pioneering works have already demonstrated feasibility of indoor localization with FM, TV and GSM signals. However, they only proved the concept and more research is required to evaluate practical benefits and limitations of indoor localization based on ambient radio signals.

The following research questions will be addressed: 1) What is the localization performance of ambient radio based systems over a long time span, in terms of accuracy, time stability and robustness to environment dynamics? 2) Which signals properties apart from signal strength can be used for localization? 3) What signal types/bands, signals features and localization methods, or their combinations, provide best performance, stability and robustness?

The project will focus on real-world experimental approach. Firstly, a multi-band radio signal acquisition and localization platform will be created, leveraging the flexibility of software-defined radio (SDR) approach. The SDR platform will be employed to systematically collect raw multi-band signal samples in multiple locations across several indoor testbeds, over the course of two years. In parallel with data collection, the project will develop relevant signal processing methods and localization algorithms; the latter will include both basic and advanced methods derived from state-of-the-art indoor localization systems. Analysis of the collected data with developed algorithms will provide insights to the research questions.

As a result, the project will provide understanding of practical bounds of ambi-

ent radio based indoor localization. Collected data will be released to scientific community, thus providing a common reference for evaluation of novel localization algorithms. All of the above will facilitate further research of this relatively young approach to indoor localization, potentially leading to cost-efficient widely available indoor localization, which will in turn boost the development of indoor location-based services.

The project aligns with the research directions of the host institution by addressing an enabling indoor positioning technology for ongoing projects which require location sensing. In particular, the results of this project will extend the scope of such projects as LOCALE (location-based storytelling), eGlasses (augmented reality) and SnT's Vehicular Lab projects (driver behavior monitoring) to GPS-deprived environments (such as office buildings, warehouses, underground parking lots, shopping malls).

Results

During 2017, the INDOORS project has made further progress towards globally available indoor localization. The project has developed new methods for indoor positioning based on ambient radio broadcasts, and provided deeper understanding of the long-term performance of the ambient localization approach in different weather conditions and environment dynamics. Moreover, the project has released AmbiLoc - a large-scale long-term dataset of georeferenced FM, TV and GSM signals. As the first open dataset in the field, AmbiLoc (http://ambiloc.org) is designed to facilitate further research in the area of ambient indoor localization.

Localised Legacies

Acronym:	LOCALE
Reference:	R-AGR-0475
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - CORE
Budget:	815,000.00 €
Duration:	1 May 2014 – 30 Apr 2017
Members:	• Thomas ENGEL (Principal Investigator) • Sébastien FAYE (Researcher) • Stefanie OESTLUND (Project Coordinator)
Area:	Communicative Systems
Partners:	• Roderick McCall (LIST) • Amiperas a.s.b.l. • Centre National de l'Audiovisuel • Centre Virtuel de la Connaissance sur l'Europe

- konviktsgaart

Description

The Locale project aims at a collaborative mobile and web-based platform for authoring and sharing multi-media historical heritage content about the period 1945 - 1960: from the end of WWII to the dawn of Europe, in the context of their respective 70th (2015) - 60th (2017: EEC) anniversaries. Targeted users are on the one hand (quasi-)witness people who keep direct or indirect memories of the period, and on the other hand all people who have historical interest or knowledge in the period. Emphasis will be put on location-based storytelling and sharing experiences that are designed to allow elderly people to share their stories in an intuitive and easy way with younger members of the population. The Locale project will thus foster the sharing of personal historical accounts that may not be included in the standard historical literature. The platform will include advanced functionalities to explore multidimensional data using various human analyses and data mining strategies, based on metadata, tags, attributes entered by the user, as well as browsing history (e.g. relation between a place and queries about a given historical fact). Interaction between users of the platform will allow to follow discussions based on data contributed as well as to verify, complete, and put in perspective pieces of historical information.

Results

The LOCALE project is about sharing cultural heritage through mobile devices. As a follow-up of earlier work, a privacy model has been developed for the online services provided by the platform. Additionally, several end-user workshops have been held using cultural probes. A range of mock-ups have been designed and evaluated as early prototypes for the client-side application.

MAintaining Driving Skills in Semi-Autonomous Vehicles

Acronym:	MaDSAV
Reference:	R-AGR-0158
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - CORE
Budget:	903,000.00 €
Duration:	1 Apr 2015 – 31 Mar 2018
Members:	• Thomas ENGEL (Principal Investigator) • Sébastien FAYE (Researcher) • Ion TURCANU (Researcher) • Stefanie OESTLUND (Project Coordinator)

Area: Communicative Systems

Partners:
- Roderick McCall (LIST)
- University of Salzburg, Austria

Description

Semi-Autonomous Vehicles present a major challenge for drivers, namely the risk that their driving skills will decline. This problem is further compounded by the fact that while the number of semi-autonomous vehicles will increase there will for the foreseeable future still remain a large number of vehicles with no or little autonomous control. This combination of the decline in driving skills plus the complicated mix of vehicles on the road will raise a number of safety challenges. For example, drivers of semi-autonomous vehicles may be forced to take control under certain circumstances but may not possess the skills which would enable them to react quickly enough or to take the right decision. Also they will not be able to rely on other vehicles taking the right course of action. As a result there needs to be methods employed which can encourage people to maintain their driving skills which are turned to the needs of particular drivers. This project will specifically explore how to profile driver performance and the development of tools which will focus on safe driving within semi-autonomous vehicles.

Results

In 2017, we contributed to the improvement of the driving simulation platform prototype, which now can be easily installed on a final user computer. The users are able to choose between five tracks layouts and drive in a semi-autonomous mode. The simulation platform registers driving-related information on a remote server for further processing and evaluation. We have also participated at the definition of two study concepts: laboratory studies and home studies. Laboratory studies mainly focus on situation awareness and persuasive systems, having the following objectives: (i) to assess situational awareness including hazard perception in manual and auto driving task, and (ii) to persuade drivers to drive safely for as long as possible. Home studies aim to explore potential deskilling effects in drivers who operate semi-autonomous vehicles regularly over an extended period of time. The overall aim of the study is to find out, whether individuals who manually operate their vehicle retain their manual driving skills better than individuals, who drive mainly in autonomous modes or with several ADAS active.

MultimodAl MoBility Assistance

Acronym: MAMBA

Reference: R-AGR-0476

PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - CORE
Budget:	886,000.00 €
Duration:	1 Apr 2014 – 31 Mar 2018
Members:	• Thomas ENGEL (Principal Investigator) • German CASTIGNANI (Researcher) • Sébastien FAYE (Researcher) • Raphaël FRANK (Researcher) • Stefanie OESTLUND (Project Coordinator) • Thierry DERRMANN (Doctoral Candidate)
Area:	Communicative Systems
Partner:	UCLA (non contracting)

Description

In Luxembourg, mobility has over the years become a socio-economical issue due to the large number of foreign commuters that cross the border everyday causing significant travel delays on the transportation network. Recently, a lot has been done to reduce traffic congestions and improve public transportation services, especially in urban environments where the road network cannot be easily extended. Traffic jams can now be detected with the help of mobile phones that act as traffic sensors. The location of buses and trains are monitored in real time to inform the passengers about possible delays. What is still missing is a holistic mobility concept that spans the entire ecosystem of transportation possibilities and tries to optimize its usage based on the demand.

The MAMBA project envisions to propose and validate a multimodal mobility platform that relies on new Internet technologies to interconnect different mobile services with the aim to provide relevant travel advice based on the users' context. Taking into account real time traffic conditions, the status of the public transportation services (e.g. buses, trains, parking slots) and the users' preferences, the individual travel assistant will proactively suggest the best transportation mode to reach a desired destination.

The key to the success of such a mobility concept is to have real time and relevant data of all the actors that are part or make use of the transportation network. Luxembourg, due to its size and geographical location, is the ideal candidate to showcase such a service on a countrywide scale. Local transport operators have already mentioned their interest to collaborate with the project, as they will benefit from its outputs such as better planning their schedules and resources.

Optimizing urban transportation services may be achieved in different ways. For example, by limiting or avoiding unnecessary journeys, one can significantly disencumber the road network. Providing drivers with incentives not to take the car during rush hour, if possible, is currently investigated by a partnering FNR CORE iGear project1. The results of those studies will be used as

an input in this project. Similarly, the tangible outputs of the still running FNR CORE MOVE project2 will provide important building blocks to achieve the holistic mobility framework.

By taking into account all those sources of information, we will be able to optimize the already existing public transportation network and influence the itinerary of the users and by suggesting new multimodal routes based on their preferences. This concept will also help develop new means of transportation i.e. public electrical vehicles that can be used as last mile transportation to reduce the vehicular traffic going in and out the city. Ultimately, by exactly knowing all travel plans in advance, such a concept will lead to demand-driven transportation services avoiding unnecessary trips and thus reduce the overall energy footprint.

The system architecture will be divided into three distinct layers as depicted in Figure 1. The first being the data collection layer, which is composed of all the relevant information sources that are needed to provide the multimodal mobility services. In a first phase, the sources have to be identified and a common middleware has to be specified and implemented in order to efficiently retrieve real time data. The second layer is the communication network, which is used to make the data available trough ubiquitous network technologies i.e. 3G/4G mobile networks and metropolitan or community WiFi networks. The third and last layer implements the travel optimizer and stores the data received by the participating agents.

Results

In 2017, we investigated whether we can estimate road traffic state from cellular data. To this end, we utilized different cellular datasets provided by our external partner POST, Luxembourg. By using this real data as well as conducting experiments in simulation environment, we showed that aggregated cellular network handovers serve as a strong predictors for urban traffic. Based on this, we further refined certain models used in the MAMBA multimodal trip-planning platform. The results were summarized in a journal article for IEEE Transactions on Intelligent Transportation Systems that is currently under review. In addition, we collected Wi-Fi data traces from a smart phone that were used to draw conclusions about the mobility of users in Luxembourg. The results from this study published in the International Journal of Distributed Sensor Networks.

Several tools have been developed and demonstrated, including a mobility assistant application and a multimodal trip planner. The mobility assistant mobile phone application and the web-based multimodal trip planner were presented as a demo paper at IEEE VNC 2017. We also extended one of our tools LuST-LTE, presented at IEEE ITSC 2017, to reflect the actual Luxembourg LTE network needed for our research. A Matlab package for calibrating the travel demand using PTV Visum as traffic simulation model has been developed. It was used to create a PTV Visum scenario of both private and public transport of Luxembourg (presented at IEEE ITSC 2017) that aims provide real time travel time estimation.

Last but not least, we organised a workshop on Smart Mobility. The main objective of this event was to bring together European actors from both industry and academia with shared interests in transportation and related topics. In total, 80 participants took part in the workshop (representatives of the ministries, companies related to automotive industry, SMEs and academics), covering the broad spectrum of topics around Smart Mobility.

Privacy Enhancing Techniques for Future Internet

Acronym:	PETIT
Reference:	R-AGR-0665
PI:	Andriy PANCHENKO
Funding:	Fonds National de la Recherche - CORE
Budget:	654,000.00 €
Duration:	1 Sep 2016 – 31 Aug 2020
Members:	• Andriy PANCHENKO (Principal Investigator) • Stefan SCHIFFNER (Researcher) • Augusto Wladimir DE LA CADENA RAMOS (Doctoral Candidate)
Area:	Communicative Systems
Partner:	University College London

Description

Internet Technology invades almost all spheres of our everyday life. Due to emerging use cases such as online social networks, banking, buildings automation, smart metering, eHealth, and eGovernment, networks are increasingly used to transmit privacy-sensitive data. The volumes of transferred, processed, and stored data are continuously expanding. There is an ever-growing temptation to collect the information once revealed: storage becomes steadily cheaper, data mining increasingly better. As a consequence, privacy on the Internet is attracting more and more attention and has become a serious concern.

The goal of the proposal “Privacy-Enhancing Techniques for Future Internet” (PETIT) is to advance the state-of- the-art in the field of Privacy-Enhancing Techniques (PETs) in order to meet the challenges of the Future Internet and to create solid fundamentals for systems that empower users with tools for strengthening their privacy protection on the Internet. This will be done by analysing existing and developing new methods for privacy-friendly communication and by contributing to a broader understanding of the topic and its primitives within the community of researchers as well as the society. To this end, we will thoroughly analyze the susceptibility of existing PETs with respect to traffic analysis to make them robust against this kind of vulnerability. Afterwards,

we will design and analyze methods for network discovery in untrustworthy environments in order to overcome scalability and trustworthiness issues in currently deployed systems. Moreover, we will address the topic of privacy-preserving routing by means of new communication paradigms for emerging protocols and performance-improved path selection metrics for better optimization of available resources and provision of an adequate quality of service.

Privacy-friendly communication is essential for exercising the right to freedom of expression, particularly in those countries that are filtering and censoring access to information. On the other hand, there should be a possibility for law enforcement to persecute criminals that misuse these techniques. Finally, we will address the contradictory issues of censorship resistance and law enforcement in order to harmonize them in future designs. This will help to increase the acceptance and integration of PETs into our daily life to give users the possibility to retain control over their personal data and to mitigate privacy threats and concerns.

Results

The junior core project PETIT has a focus on designing and evaluating privacy-enhancing techniques for future Internet. The focus of the first year of the project was on traffic analysis and countermeasures to hamper this kind of analysis. One of the followed directions was to analyze the susceptibility of anonymous communication networks such as Tor with respect to website fingerprinting, a special case of traffic analysis. The focus was on location hidden services (also known as onion services). Our findings were published at ACM WPES (a targeted workshop of ACM CCS) 2017. For countermeasures, we analyzed different methods for multipath routing in order to distribute traffic and thus thwart traffic analysis without putting additional (dummy) traffic load on the network. As a side effect, this method could even improve performance due to a better load balancing. The goal was to compare existing methods with respect to their performance and security and to select the most appropriate defense. Our findings revealed weaknesses of existing methods and, thus, we proposed an own scheme for multipath routing in the Tor network. Its implications are subject to our current research work. We also started investigating real-world cases of website fingerprinting, where the user does not visit random websites but rather different subpages within a website (which is a typical user behaviour during web browsing sessions).

B.9 Fonds National de la Recherche and Narodowe Centrum Badań i Rozwoju Projects

Verification of Voter-Verifiable Voting Protocols

Acronym: VoteVerif

PI:	Peter Y. A. RYAN
Funding:	Fonds National de la Recherche - CORE, Narodowe Centrum Badań i Rozwoju
Duration:	1 Sep 2016 – 31 Aug 2019
Members:	• Peter Y. A. RYAN (Principal Investigator) • Leon VAN DER TORRE (Researcher) • Salima LAMHAR (PhD student) • Gergely BANA (Research Associate)
Partners:	• Wojciech Jamroga • Institute of Computer Science, Polish Academy of Sciences

Description

We propose to use techniques from formal specification and verification of multi-agent systems, and apply them to verify information security requirements for voting protocols. In particular, we will look at various formalizations of confidentiality, coercion-resistance, and voter-verifiability in e-voting protocols. The research will lead to the development of a toolbox for practical verification of strategic properties in interaction protocols. Based on case studies using the toolbox, we will draft some advice on how societal processes of governance and collective choice can be improved.

B.10 Fonds National de la Recherche Projects

Formal Models for Uncertain Argumentation from Text

Acronym:	FMUAT
PI:	Leon VAN DER TORRE
Funding:	Fonds National de la Recherche - INTER
Budget:	99,850.00 €
Duration:	1 Mar 2015 – 28 Feb 2018
Member:	Leon VAN DER TORRE (Principal Investigator)
Area:	Intelligent and Adaptive Systems
Partner:	Beishui Liao (Zhejiang University)

Description

The topic of this project is formal models for uncertain argumentation from natural language text. Based on Dung's argumentation theory, integrating uncertainty into argumentation is gaining momentum. However, to the best of our knowledge, little attention has been paid to the modelling of uncertain argumentation in which the uncertainty of arguments is obtained mainly from text (e.g. biological papers). The aim of this project is to develop theory and algorithms to formalize and evaluate the uncertain argumentation from natural language text, such that uncertain arguments represented by natural language can be formalized and their status be properly and efficiently evaluated. The project is carried out by the cooperation between the Individual and Collective Reasoning (ICR) group at the University of Luxembourg and the group of Beishui Liao of the Center for Study of Language and Cognition (CSLC) at Zhejiang University.

INTER/CNRS/14/10367986 Algorithmic Decision Theory

http://leopold-loewenhein.uni.lu/bisdorff/research.html

Acronym:	Algodec 2
Reference:	F1R-CSC-PFN-14ALG2
PI:	Raymond Joseph BISDORFF
Funding:	Fonds National de la Recherche - INTER
Budget:	10,000.00 €
Duration:	1 Jan 2015 – 31 Dec 2019
Members:	• Raymond Joseph BISDORFF (Principal Investigator) • Pascal BOUVRY (Researcher) • Ulrich SORGER (Researcher) • Leon VAN DER TORRE (Researcher) • Emil WEYDERT (Researcher)
Area:	Intelligent and Adaptive Systems
Partners:	• Yves De Smet (Université Libre de Bruxelles) • Eyke Hüllermeier (Universität Paderborn) • Pierre Marquis (Université d'Artois, France) • Brice Mayag (Université Paris-Dauphine) • Patrice Perny (Universite Pierre et Marie Curie) • Marc Pirlot (Université de Mons, Belgique) • Bernard Ries (Université Paris-Dauphine) • Fred S. Roberts (DIMACS (USA)) • CNRS

Description

The CNRS-GDRI Algodec 2 is expected to be involved in the following activities:

1. Contribute to the organization International Conference on AlgorithmicDecision Theory (ADT), to be held in 2015 in Lexington, Kentucky (US) and in 2017 (Luxembourg). The ADT conference series was created with the support of the ALGODEC GDRI.

2. Contribute to the workshop series From Multicriteria Decision Aid to Preference Learning (DA2PL), to be organized on even years (2016 and 2018). The themes of preference analytics and learning are central in DA2PL.

3. Organize one or two summer doctoral schools during the span of the four years addressing the whole of the PhD students enrolled with the partners and beyond.

4. Contribute to the organization of workshops on the themes of the GDRI co-located in highly rated international conferences such as AAAI, IJCAI, ICML, ECML. A number of workshops on topics related to preferences and preference learning has been organized in the past by the participants of the proposed GDRI on Preference Analytics (such as the NIPS workshop on Choice models and Preference Learning in 2011, and the series of workshops on Preference Learning organized by Eyke Hullermeier). We will consider the possibility of establishing a new workshop venue, but perhaps given the number of already established venues, we will focus on continuing these series, with possibly a larger thematic scope. We also plan to keep contributing to the successful series of Multi-disciplinary Workshop on Advances in Preference Handling (MPREF), held annually since 2004, that allows possibility of interaction with researchers interested in preferences from other fields (databases processing, algorithmic, theoretical computer science).

5. Organize joint seminars among the participating (research centres) laboratories/institutes as well as further dissemination activities.

6. Promote mobility of early stage and experienced researchers as well as for the permanent academic staff. In particular, we will support research visits of members of the GDRI in the lab of another partner, with the goal of undertaking collaborative research leading to joint publications.

7. Establish a website for the GDRI where activities will be described. A person, among the researchers implicated in the project, will be responsible for the website so that it will be updated regularly. A blog-like interfaces will allow to keep tracks of project meetings, but also to present abstracts of seminars given at the universities involved, announce recent publications on the subject, advertise call for papers. We will consider the possibility of a forum or a dedicated page on social networks, so that young PhD students can discuss with practitioners and other senior (or junior) researchers with whom develop new research ideas or practical support activities, not necessarily within the principal axis of the PhD.

8. Promote the co-tutoring of each PhD student by at least two senior researchers from two different partner laboratories.

Internet Shopping Optimisation Project

http://www.cs.put.poznan.pl/ishop/

Acronym:	IShOP
Reference:	R-AGR-0453-10-V
PI:	Pascal BOUVRY
Funding:	Fonds National de la Recherche - INTER
Budget:	1,029,639.00 €
Duration:	1 Mar 2014 – 28 Feb 2017
Members:	• Pascal BOUVRY (Principal Investigator) • Grégoire DANOY (Researcher) • Sébastien VARRETTE (Researcher) • Raymond Joseph BISDORFF (Collaborator)
Area:	Intelligent and Adaptive Systems
Partners:	• Jacek Blazewicz (Poznan University of Technology) • Maciej Drozdowski (Poznan University of Technology) • Mikhail Kovalyov • Jakub Marszalkowski (Poznan University of Technology) • Jedrzej Musial (Poznan University of Technology) • Kamil Sedlak (Poznan University of Technology) • Malgorzata Sterna (Poznan University of Technology)

Description

This project proposes innovative and realistic models for different typical online shopping operations, supported by strong mathematical and operational research fundamentals, and well balanced with lightweight computational algorithms. These models are designed in order to allow the optimization of such transactions. Finding accurate solutions to the defined problems implies both lowering customer expenses and favouring market competitiveness.

One of the main aims of this project is to model and formulate new advanced and realistic flavours of the Internet Shopping Optimization Problem (ISOP), considering discounts and additional conditions like price sensitive shipping costs, incomplete offers from shops, or the minimization of the total realiza-

tion time, price, and delivery time functions, among others. The models will be mathematically and theoretically well founded. Moreover, the challenge of defining and addressing a multi-criteria version of the problem will be addressed too. Other important contributions will be the mapping of ISOP to other new challenges. One of them is the design of a novel business model for cloud brokering that will benefit both cloud providers and consumers. Providers will be able to easily offer their large number of services, and to get a fast answer from the market to offers (e.g., when infrastructure is under-utilized). Additionally, customers will easily benefit from offers and find the most appropriate deals for his/her needs (according to service level agreements, pricing, performance, etc.). Modelling some of these aspects and coupling it with an optimization tool for the brokering of cloud services among various providers would be a key contribution to the field.

A wide set of optimization algorithms will be designed and developed for the addressed problems. They include from fast lightweight specialized heuristics to highly accurate parallel and multi-objective population-based metaheuristics. They all will be embedded in a software framework for their practical applications, and validation.

IShOP is an INTER POLLUX project, cofunded by Luxembourg National Research Funds (FNR) and the Polish National Research Centre for Research and Development (NCBiR).

This project is a collaboration between the Laboratory of Algorithm Design and Programming Systems of the Institute of Computing Science, Poznan University of Technology, Poland, and the Interdisciplinary Center of Security, Reliability and Trust (SnT) of the University of Luxembourg, Luxembourg.

Secure Voting Technologies

Acronym:	SeVoTe
PI:	Peter Y. A. RYAN
Funding:	Fonds National de la Recherche - INTER
Duration:	1 Oct 2016 – 30 Sep 2020
Members:	• Peter Y. A. RYAN (Principal Investigator) • Marie-Laure ZOLLINGER (PhD student)

Description

The goal of this research project is to provide significant advances on the issues that appear in modern voting and e-voting systems, with a particular focus on the following aspects: Rigorous expression of the security properties intended from and/or exhibited by a voting system, in order to both improve our understanding of what can be achieved in general, and of the properties, and potential weaknesses, of actual systems. Further, the design of voting sys-

tems and components thereof (cryptographic schemes, ...), that offer, firstly, a more effective balance between coercion-resistance and, secondly, usability and improved robustness, resilience to incidents, and more effective dispute resolution procedures.

Security Properties, Process Equivalences, and Automated Verification

Acronym:	SEQUOIA
PI:	Peter Y. A. RYAN
Funding:	Fonds National de la Recherche - INTER
Duration:	1 Mar 2015 – 28 Feb 2019
Member:	Peter Y. A. RYAN (Principal Investigator)
Area:	Information Security
Partners:	• ENS Cachan • Université de Lorraine

Description

Modern society is becoming ever-more digitalized. In particular, electronic services provided over the internet are now standard tools for individuals to network, manage their bank accounts, and even vote in important elections. It is therefore critical to deploy strongly secure systems to accomplish these tasks, which present the dual challenge of being both of socio-economic importance, and highly complex.

While cryptographic protocols are implemented to attempt securing these procedures, design errors remain abundant, as recent examples of practical attacks on such systems demonstrate. It is thus important to further refine the necessary tools to verify the correctness of these protocols. A highly successful technique to accomplish this is to use symbolic analysis. Two particularly important features of this technique stand out: 1) it is well-suited to analyze complex systems and 2) it is amenable to automation.

The aim of this project is to extend the capabilities of symbolic analysis so as to capture the subtle security properties of modern-day cryptographic protocols. Many of these properties can be expressed in terms of indistinguishabilty of processes, a notion that symbolic analysis currently lacks the necessary theoretical foundations to fully understand, and automated tools to verify. The technical objective is to begin filling this gap.

Examples of concrete security properties that indistinguishability naturally captures include anonymity, unlinkability, maximal protection of weak secrets such as passwords, and more. The main practical objective of the project is to provide an automated tool (using AKISS – Active Knowledge In Security proto-

colS - as a starting point) allowing the verification of indistinguishability, and therefore of the above-mentioned properties. We plan to illustrate our findings by performing an analysis on an e-voting protocol that actually relies on several of these properties.

Specification logics and Inference tools for verification and Enforcement of Policies

http://icr.uni.lu/SIEP/

Acronym:	SIEP
Reference:	I2R-DIR-PFN-11SIEP
PI:	Leon VAN DER TORRE
Funding:	Fonds National de la Recherche - INTER
Budget:	450,000.00 €
Duration:	1 Jun 2012 – 31 May 2017
Members:	• Leon VAN DER TORRE (Principal Investigator) • Marcos CRAMER (Collaborator) • Diego Agustin AMBROSSIO (Doctoral Candidate)
Areas:	• Information Security • Intelligent and Adaptive Systems • Software and Systems
Partners:	• Guillaume Aucher (Université de Rennes) • Marc Denecker (Katholieke Universiteit Leuven) • Dov Gabbay (King's College) • Pieter van Hertum (Katholieke Universiteit Leuven)

Description

The aim of SIEP is to develop an expressive logic for specifying distributed authorization policies and to implement various forms of inference suitable for verification tasks (e.g., compliance) as well as for enforcing such policies. There are three objectives.

Objective 1 is to develop an expressive modular logical framework suitable for specifying complex composite distributed access control policies, which allow for delegation and revocation of access rights, dynamic aspects such as evolving policies, trust, and the representation of the beliefs of agents.

Objective 2 is to develop tools for verification, checking compliance, experimentation, simulation and analysis of access control and privacy policies.

Objective 3 is the creation of a prototype system to enforce distributed access control policies.

Combatting Context-Sensitive Mobile Malware

Acronym:	COMMA
Reference:	C15/IS/10404933
PI:	Olga GADYATSKAYA
Funding:	Fonds National de la Recherche
Budget:	690,000.00 €
Duration:	1 Apr 2016 – 30 Mar 2019
Members:	• Olga GADYATSKAYA (Principal Investigator) • Sjouke MAUW (Collaborator)
Area:	Information Security

Description

Mobile computing devices, or simply smartphones, are ubiquitous today. Many consumers rely on their smartphone for such personal computing tasks as communication with friends and family through numerous messengers, email activity, mobile banking, GPS navigation, etc. Moreover, through the so-called Bring-Your-Own-Device (BYOD) schemes, smartphones are increasingly used for executing business tasks. With this proliferation of mobile devices security and privacy of smartphones and the data they process become crucial requirements. Unfortunately, we know that mobile platforms today are insecure. For example, the growth rate of mobile malware samples for the Android platform run by Google is exponential. And the price of admitting a malicious application onto an end-user platform is often very high, especially if the device is used in the corporate environment and handles highly sensitive information. Malicious mobile applications are known to steal private data handled by the smartphones almost by default. Therefore, there is a high demand for anti-virus services tailored for mobile devices that could evaluate for a third-party application whether it is malicious or not. For example, Google and Apple utilise their own on-market security services for application vetting. There exist also a number of third-party online security services offering to check security of mobile applications, such as VirusTotal and Andrubis.

Security services o ered by antivirus companies often rely on known malware signatures. Therefore these services do not detect zero-day malware samples that rely on new attacks or recently discovered vulnerabilities. This approach is not sufficiently reliable in the context of application market. Indeed, if Apple or Google will distribute zero-day malware, they will face a customer drain. Thus on-market security services typically use a combination of static and dynamic security checks that could reveal malicious behaviour. For example, if such

service detects a known root exploit code or a suspicious API calls pattern, it can mark the sample in question as malicious. However, the recent generations of mobile malware that utilise obfuscation and dynamic code updates to thwart the security services pose a big challenge. Such dangerous samples can be often categorised as environment-sensitive or context-sensitive malware: they change their behaviour depending on the context. If they are able to detect that they are executed by a security service, they do not exhibit their malicious payload. If the payload is obfuscated (e.g., encrypted), it can be very challenging to identify malicious code in these samples.

Currently there exist security techniques that aim to combat this malware type. They typically rely on machine learning-based classifiers, or they utilise discrepancies in several executions of the same sample, and check if one of these executions actually shows malicious actions. The challenge for a machine learning-based approach is the weakness of the feature selection. Code obfuscation alone cannot be reliably used as a malware feature: many benign apps obfuscate their code to thwart plagiarism. If an attacker knows which other features contribute to the malicious profile utilised by a security service, he can change the app to avoid being compliant with this profile. If a security service can find a suitable context to execute the sample such that it exhibits some malicious behaviour, this sample can be successfully categorised as malicious. The main challenge for these approaches is to find the suitable context, what can be very difficult in general, given that malware often is able to detect that the security service's emulator is applied, and thus to refrain from malicious actions. Generation of a right context often requires manual inspection of the code. This is a tedious task that is often not suitable in the context of online third-party security services, such as Andrubis.

Our contribution: In our project we plan to improve the state-of-art mechanisms for reliable detection of malicious applications by looking simultaneously at executed and not-executed code paths. The intuition is simple: context-sensitive malware tries to conceal the malicious behaviour, so the most security-critical code will be hidden in the code paths that were not executed by the security service. For such code paths we will 1) identify automatically how to bring the app execution to these paths; and 2) analyse these code paths automatically to detect concealed security issues. The detection will rely on machine learning techniques and data flow analysis.

Results

- The project has started on the 1st April 2016. A postdoc has joined the COMMA team on the 1st November 2016. The project is in the process of hiring a technician.
- A postdoc and a programmer have joined the COMMA team in 2017. The project has acquired the server infrastructure.

Distance Bounding: a graph theoretical and formal approach

Acronym:	DIST
Reference:	C15/IS/10428112
PI:	Rolando TRUJILLO RASUA
Funding:	Fonds National de la Recherche
Budget:	349,000.00 €
Duration:	1 Apr 2016 – 30 Mar 2018
Members:	• Rolando TRUJILLO RASUA (Principal Investigator) • Yunior RAMIREZ CRUZ (Researcher) • Sjouke MAUW (Collaborator) • Jorge Luis TORO POZO (Collaborator)
Areas:	• Communicative Systems • Information Security

Description

Physical proximity is a common requirement in access control policies in the physical world. One normally expects someone to be present when opening a door or turning on a car. In practice, the very design of many access control mechanisms enforces physical proximity naturally, e.g., mechanic locks or biometric identification. In wireless systems, however, providing the same kind of guarantee is far from being trivial. The most reliable approach to proximity checking in wireless systems is distance bounding, that is, a cryptographic protocol where the propagation time of messages traveling at the speed of light determine an upper bound on the distance between two devices. Distance bounding protocols can be used as efficient building blocks for a variety of services and applications, such as routing, physical access control, neighbor discovery, tracking and localization.

The purpose of this project is to improve and formally verify the security guarantees of distance bounding protocols. In particular, we will focus on graph-based distance bounding protocols; a prominent family of distance bounding protocols based on random walks in graphs. Graph-based distance bounding protocols are efficient building blocks suitable to be implemented in low-cost devices such as RFID tags. One based on trees and another one based on a peculiar graph structure named Poulidor, are the two graph-based distance bounding protocols proposed up to now. They remain unbroken, and no other distance bounding protocol has proven to outperform them. Nevertheless, very little is known about this type of protocols. In this project, we will study the relation between graph properties and the security properties of graph-based distance bounding protocols. Our starting point is an observation that, to the best of our knowledge, has not been made before: the Poulidor graph belongs to the well known family of Cayley graphs. Therefore, understanding and study-

ing the relation between graph-based hash functions (where Cayley graphs are used) and graph-based distance bounding protocols, may lead to better designs of this type of security protocols. We will also develop a symbolic approach for the formal verification of distance bounding protocols, which will be used to verify the security and correctness of our own solutions. The few existing symbolic approaches explicitly introduce either timestamps or a global notion of time to the security model. The novelty of our approach is that we expect to formalize the notion of proximity as an ordering problem instead. This keeps the model simple and more appealing to practitioners.

Results

- Optimality results on the security of lookup-based protocols. S. Mauw, J. Pozo and R. Trujillo-Rasua. In At the 12th Workshop on RFID and IoT Security (RFIDSec 2016), Hong kong, November 29, December 2, 2016, 2016.
- A class of precomputation-based distance-bounding protocols. S. Mauw, J. Toro-Pozo and R. Trujillo-Rasua. In 1st IEEE European Symposium on Security and Privacy (Euro S & P), Saarbrücken, Germany, March 21-24, 2016, 2016.
- Distance-Bounding Protocols: Verication without Time and Location. S. Mauw, Z. Smith, J. Toro-Pozo and R. Trujillo-Rasua. In IEEE Symposium on Security and Privacy (Oackland), S&P'18, May 21 { 23, 2018, San Francisco, California, USA, 2018.
- Security of Distance-Bounding: A Survey. G. Avoine, M. Bingol, I. Boureanu, S. Capkun, G. Hancke, S. Kardas, C. Kim, C. Lauradoux, B. Martin, J. Munilla, A. Peinado, K. Rasmussen, D. Singelee, A. Tchamkerten, R. Trujillo-Rasua and S. Vaudenay. ACM Computing Survey, 2017. (to appear)

HotspotID-crowdsourced WiFi security

https://www.hotspotid.com/

Acronym:	HotspotID
Reference:	C-AGR-0623
PI:	Thomas ENGEL, Raimondas SASNAUSKAS
Funding:	Fonds National de la Recherche
Budget:	271,000.00 €
Duration:	15 Jan 2016 – 31 Jul 2017
Members:	• Thomas ENGEL (Principal Investigator) • Daniel FORSTER (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Andriy PANCHENKO (Scientific Contact)

Area: Communicative Systems

Partner: Red Dog Communications s.a.

Description

Today's security solutions do not provide WiFi users with the tools needed to asses the security risks associated with connecting to a WiFi network, in real time. It is impossible to verify that you are connected to the legitimate access point (AP) and not an imposter (Evil Twin). Nor do you have any information about the access point. Likewise the owners of WiFi access points have no means to clearly identify themselves for their users, so they will not be mistaken for an imposter.

Hotspot ID offers WiFi users a FREE mobile app which fingerprints all WiFi connections made and registers this (crowdsourced) data on the central server for analysis & evaluation. The server tracks all the data it receives to generate a reputation score for each registered access point (AP). The server returns to the app all relevant data for the WiFi network and warns the user if connected to an unsafe AP (i.e. Evil Twin). We propose to WiFi owners to certify their Access Points - a subscription based service to register verified network data in the system. This permits better attack detection as the live fingerprints are checked against verified networks, instead of crowdsourced records. This results in better security for the users of Certified AP.

Results

The HotSpotID is a PoC project of FNR and thus does not aim at producing any research results. It is the first WiFi security app to use real-time crowdsourced network fingerprints to protect users from connecting to fake WiFi access points. The primary goal during the PoC project was to test our preliminary ideas under real market conditions and to transfer our research findings to the real-world settings.

In collaboration with the University's data protection officer and the CNPD a legal ground for the collection of fingerprints was found. The documentation for the notification to the CNPD was created, signed, and sent out to the CNPD. The team managed to fine tune and improve the functionality of the app to detect evil twins. We found out that our initial strategy for commercialisation did not work out. Hence, we proposed another strategy that is though less scalable, but is able to ease the bootstrapping for going into masses. Also, we proposed an alternative solution that requires additional hardware on the operator side but provides more secure protection (guaranteed vs. probabilistic) against the evil twin attack. We also prepared a demonstration to be shown within the EU H2020 FlySec project in the scope of airport security. The purpose of the demo is to raise awareness to the problem of the evil twin attacks and to show how easily every user can become a victim of this attack.

Security and Privacy for System Protection

Acronym:	PRIDE: SPsquared
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche
Duration:	1 Jan 2016 – 31 Dec 2021
Members:	• Sjouke MAUW (Principal Investigator) • Alexei BIRYUKOV (Collaborator) • Jean-Sébastien CORON (Collaborator) • Thomas ENGEL (Collaborator) • Jacques KLEIN (Collaborator) • Gabriele LENZINI (Collaborator) • Jun PANG (Collaborator) • Peter Y. A. RYAN (Collaborator) • Radu STATE (Collaborator)

Description

The proposed Doctoral Training Unit (DTU) focuses on information security and privacy, including its storage, processing and transmission. Our Security and Privacy for System Protection (SP2) research program is set up by the leading researchers of CSC research unit and the Interdisciplinary Centre SnT at the University of Luxembourg. The SP2 program is designed to provide a high-quality research environment for PhD students and to strengthen the links between fundamental and applied research. In particular, research is organized in an interdisciplinary way along five themes where the most critical and pressing research challenges will be addressed:

1. Number Theory, Cryptography and Cryptographic Protocols;
2. Implementation of Cryptography;
3. Internet Privacy;
4. System Security;
5. Socio-Technical Security.

In addition to the research program, our DTU offers a comprehensive training and career development program, with a strong quality control framework, that will not only ensure a high quality scientific output but also prepare our students for an excellent future career in academia, industry and governmental environment. We believe that our DTU's contributions will have a significant scientific, economical and societal impact and will realize strategic priorities of the involved institutions.

B.11 University of Luxembourg Projects

A Personalization Framework for Sentiment Categorization with Recurrent Neural Network

http://acc.uni.lu

Acronym:	PERSEUS
PI:	Christoph SCHOMMER
Funding:	University of Luxembourg
Duration:	15 Jan 2017 – 15 Jan 2020
Members:	• Christoph SCHOMMER (Principal Investigator) • Siwen GUO (Doctoral Candidate)
Area:	Intelligent and Adaptive Systems
Partner:	DFKI

Description

The term Artificial Companion has originally been introduced by Y. Wilks as "...an intelligent and helpful cognitive agent, which appears to know its owner and their habits, chats to them and diverts them, assists them with simple tasks...". To serve the users' interests by considering a personal knowledge is, furthermore, demanded. The following position paper takes this request as motivation for the embedding of the PERSEUS system, which is a personalized sentiment framework based on a Deep Learning approach. We discuss how such an embedding with a group of users should be realized and why the utilization of PERSEUS is beneficial.

Artificial Chatbots and Companions

http://acc.uni.lu

Acronym:	ACC
PI:	Christoph SCHOMMER
Funding:	University of Luxembourg
Duration:	1 Jan 2017 – 31 Dec 2030

Members:
- Christoph SCHOMMER (Principal Investigator)
- Siwen GUO (Doctoral Candidate)

Area: Intelligent and Adaptive Systems

Description

Artificial Creative Chatbots

We are facing a world where autonomous systems will change our daily life. In addition to self-driving vehicles and drones, an increasingly networked home, or the use of intelligent artificial agents as assistants, our belief is that innovative language-based creative chatbots offer a great potential, for example, for a language learning or for natural language-based conversations in general. We, hereby, follow Yorick Wilkes's idea to create artificial companions to be designed to help people and to "study conversational software-based artificial agents that will get to know their owners over a substantial period. These could be developed to advise, comfort and carry out a wide range of functions to support diverse personal and social needs, such as to be an 'artificial companion' for the elderly, helping their owners to learn, or assisting to sustain their owners' fitness and health." *(Source: M. Peltu, Y. Wilks: Close Engagements with Artificial Companions: Key Social, Psychological, Ethical and Design Issues. Oxford Internet Institute (2008).*

CAESAREA

Acronym: CAESAREA

PI: Alexei BIRYUKOV

Funding: University of Luxembourg

Duration: 15 Apr 2015 – 14 Apr 2017

Members:
- Alexei BIRYUKOV (Principal Investigator)
- Vesselin VELICHKOV (Researcher)

Area: Information Security

Description

Evaluation and Analysis of Authenticated Encryption Schemes

Cognitive Aspects of Formal Argumentation Theory

Acronym:	CAFAT
Reference:	R-AGR-0749-11
PI:	Leon VAN DER TORRE
Funding:	University of Luxembourg
Budget:	350,000.00 €
Duration:	1 Oct 2016 – 31 Jul 2018
Member:	Leon VAN DER TORRE (Principal Investigator)
Areas:	• Computational Sciences • Educational Sciences

Description

Formal Argumentation Theory is a popular framework for capturing deliberative aspects of reasoning in Artificial Intelligence. While it has been thoroughly studied theoretically and implemented in many systems, its relation to actual human reasoning has not been studied much. This project will conduct an empirical cognitive study that tests assumptions and predictions of Formal Argumentation Theory. In order to minimize the interference with domain-specific knowledge, the arguments used in the study will be on conflicts arising in informal mathematical and metalinguistic reasoning.

The project cost will be 350k€, out of which 306k€ are staff costs.

Results

Marcos Cramer has co-authored three papers in argumentation theory:

- A published workshop paper that applies the meta-argumentation methodology to study extensions of Explanatory Argumentation Frameworks [1]
- A published workshop paper that proposes an adaptation of ASPIC+, called ASPIC-END, motivated by argumentation about semantic paradoxes [2]
- A submitted journal paper extension of [2] that motivates the applicability of ASPIC-END to debates in the formal sciences [3]
- Additionally, a journal paper that he submitted in 2016 got published [4].

Furthermore, he has participated in the planning and evaluation of two empirical cognitive studies about argumentation theory. Publications describing the findings of these studies are still in the making.

[1] Jeremie Dauphin and Marcos Cramer. Extended Explanatory Argumentation Frameworks. TAFA 2017
[2] Jeremie Dauphin and Marcos Cramer. ASPIC-END: Structured Argumentation with Explanations and Natural Deduction. TAFA 2017
[3] Marcos Cramer and Jeremie Dauphin. A Structured Argumentation Framework for Modeling Debates in the Formal Sciences. Submitted to Journal for

General Philosophy of Science.
[4] Marcos Cramer. Implicit dynamic function introduction and Ackermann-like Function Theory. IfCoLog Journal of Logics and their Applications. Volume 4, Issue 4, May 2017.

Collaborative Compound Document Authoring and Annotation

Acronym:	CoCoDA^2
PI:	Steffen ROTHKUGEL
Funding:	University of Luxembourg
Budget:	169,825.00 €
Duration:	1 Feb 2014 – 31 Jan 2017
Members:	• Steffen ROTHKUGEL (Principal Investigator) • Jean BOTEV (Collaborator) • Johannes KLEIN (Doctoral Candidate)
Areas:	• Communicative Systems • Intelligent and Adaptive Systems • Software and Systems

Description

The CoCoDA^2 project focuses on collaboration in compound document systems based on a flexible and more fine-grained document handling than the one provided by existing file abstractions. Taking an interdisciplinary perspective, the efficient collaborative authoring as well as the intra- and inter-item annotation of compound documents particularly for geographically remote users will be investigated. This involves areas of research ranging from network science over concurrency control with operational transformation to the social sciences. The CoCoDA^2 project thus aims at contributing to the general understanding of how the structure of compound documents and collaborative aspects – such as the simultaneous multi-user authoring process itself or the concomitant sharing of semantic data – interact and integrate.

Foundations of Argumentation

Acronym:	FA
PI:	Emil WEYDERT
Funding:	University of Luxembourg
Duration:	1 Jan 2017 – 31 Dec 2018

Member: Emil WEYDERT (Principal Investigator)

Description

We continued our long-term program aimed at providing a semantics for arguments to evaluate, justify, and complement existing inferential semantics for abstract and structured argumentation. In particular, we introduced a more general notion of structured arguments, better suited to explore techniques from neighbouring areas and invented a novel blocking semantics for arguments which is based on ranking measure fusion concepts. It questions current assumptions about the reinstatement principle although it does not share the more pronounced weaknesses of our previous overriding semantics.

High Performance Computing @ UL

http://hpc.uni.lu/

Acronym: UL HPC

PI: Pascal BOUVRY, Sébastien VARRETTE

Funding: University of Luxembourg

Duration: 1 Jul 2007 – 31 Dec 2020

Members:
- Pascal BOUVRY (Principal Investigator)
- Sébastien VARRETTE (Principal Investigator)
- Valentin PLUGARU (Researcher)
- Clément PARISOT (Collaborator)

Description

The intensive growth of processing power, data storage and transmission capabilities has revolutionized many aspects of science. These resources are essential to achieve high- quality results in many application areas.

In this context, the University of Luxembourg (UL) operates since 2007 an High Performance Computing HPC facility and the related storage. The aspect of bridging computing and storage is a requirement of UL service – the reasons are both legal (certain data may not move) and performance related.

Nowadays, people from the three faculties and/or the three Interdisciplinary centers within the UL, are users of this facility. Obviously, many CSC members are relying on the platform to perform their research, as highlighted on the corresponding list of publications. More specifically, key research priorities such as Computational Sciences, Systems Bio-medicine (by LCSB) and Security,

Reliability & Trust (by SnT) require access to such HPC facilities in order to function in an adequate environment.

The HPC facility is managed by an expert team under the responsibility of Prof. Pascal Bouvry and Dr. Sebastien Varrette. Composed by several clusters of compute nodes, the UL HPC platform has kept growing over time thanks to the continuous efforts of the UL HPC Team (S. Varrette, V. Plugaru, S. Peter, H. Cartiaux and C. Parisot). At the end of 2017, the facility consists of 5 clusters, featuring a total of 602 nodes (i.e. 8428 computing cores: 206 TFlops + 76 TFlops on GPU accelerators) and 7 PB of shared raw storage which are all configured, monitored and operated by 5 HPC specialists. This places the HPC center of the University of Luxembourg as one of the major actors in HPC and Big Data for the Greater Region Saar-Lor-Lux. In addition, a total of 130 servers are operated to pilot the HPC platform and the other deployed services for research such as Gforge and GitLab used by hundreds of researchers.

In these exciting times, the role of university-based HPC is more critical than ever in providing the foundation for a healthy HPC "ecosystem" for Luxembourg, where computational scientists and HPC-service providers work together in a highly collaborative community. Through their locality to today's research base, and the students who will become our next generation of computational scientists, universities such as the UL are uniquely positioned to deliver excellent return on investment in HPC as a platform for future economic growth.

From its reputation and national expertise in the HPC and Big Data domains, the University of Luxembourg (also member of ETP4HPC - European Technology Platform (ETP) in the area of High-Performance Computing (HPC)) has been chosen by the ministry to represent the country within PRACE (Partnership for Advanced Computing in Europe). This implements a new crucial step in the gouvernemental priority aiming at accelerating the development of world-class HPC technologies in Luxembourg.

Homomorphic Encryption and Multilinear Maps for Cloud Computing

Acronym:	HEMAC
Reference:	R-AGR-3224-00
PI:	Jean-Sébastien CORON
Funding:	University of Luxembourg
Budget:	185,000.00 €
Duration:	1 Jul 2017 – 30 Jun 2019
Member:	Jean-Sébastien CORON (Principal Investigator)
Areas:	• Computational Sciences • Security, Reliability and Trust in Information Technology

Description

Homomorphic cryptography offers the tantalizing goal of being able to process sensitive information in encrypted form, without needing to compromise on the privacy and security of the citizens and organizations that provide the input data.

The goal of the proposal is to improve the efficiency of existing homomorphic encryption schemes and possibly design new ones, in order to bridge the gap between the theoretical constructions and the concrete applications.

Reconciling the Uneasy Relationship between the Economics of Personal Data and Privacy

Acronym:	REQUISITE
PI:	Peter Y. A. RYAN
Funding:	University of Luxembourg
Duration:	1 Jun 2015 – 31 May 2018
Member:	Peter Y. A. RYAN (Principal Investigator)
Areas:	• Information Security • Intelligent and Adaptive Systems

Description

Personal data is nowadays a common commodity in the web space, yet our understanding of cost–benefit trade-offs that individuals undertake when getting involved in digital transactions and disclosing personal data is far from complete. On the one hand, users benefit from personalisation of products and contributing to the societal good, but, on the other hand, might be locked into services and suffer from severe privacy risks, e.g. that data may be compromised once disclosed to a service provider. We focus on healthcare-related personal data and mainly consider two scenarios. One is *public medical research*, where personal data will be used by third-party organizations (e.g. by various medical labs) to conduct research, such as studying the trend of a disease. The other is *medical recommender systems*, where patients interact with each other and third-party professionals (e.g. doctors, and people from pharmaceutical and insurance companies) for a variety of purposes. These two scenarios only represent a small segment of the whole ecosystem, but they vividly illustrate the dilemma of utility and privacy of sensitive personal data.

In this project, we carry out interdisciplinary research to bridge the theory-practice gap in tackling the privacy issues associated with personal data. We (economists and information security researchers) will investigate the economic incentives behind users' participation in the systems, and subsequently establish models for gains and costs in the two application scenarios. Then, we will

apply the concept of *mechanism design* to our scenarios, and propose mechanisms for safeguarding users' utility and privacy against rational attackers (e.g. legitimate participants in the systems). Finally, to complement the developed mechanisms, we will propose new cryptographic protocols to safeguard privacy against potential malicious and irrational attackers (e.g. outside attackers). The task of this project is essentially twofold: economic understanding and modelling, and realization of (rational) cryptographic protocols.

Scalable External Control of Probabilistic Boolean Networks

Acronym:	SEC-PBN
Reference:	R-AGR-0744-11
PI:	Jun PANG
Funding:	University of Luxembourg
Budget:	336,000.00 €
Duration:	1 Jul 2016 – 30 Jun 2019
Member:	Jun PANG (Principal Investigator)
Areas:	• Computational Sciences • Security, Reliability and Trust in Information Technology • Systems Biomedicine

Description

Computational modelling plays a prominent role in systems biology. Modelling of certain parts of cellular machinery such as gene regulatory networks (GRNs) often leads to models characterised by huge state spaces. Therefore, profound understanding of biological processes asks for the development of scalable methods that would provide means for analysis and reasoning about such huge systems. In this project, we concentrate on external control of GRNs, modelled as probabilistic Boolean networks. Instead of deriving optimal control strategies, our methods aim for approximate, suboptimal solutions, which are computationally efficient. Our proposed methods will be valuable in practice, e.g, in cellular reprogramming.

Results

- Soumya Paul joined the project on April 15th, 2017.
- The paper titled "ASSA-PBN: A toolbox for probabilistic Boolean networks" has been accepted by the IEEE/ACM Transactions on Computational Biology and Bioinformatics.
- The project team has worked on a few methods for (sub)optimal simultaneous

control of large Boolean networks.

Time Predictable Embedded Systems

Acronym:	TIME
Reference:	R-AGR-0741-00
PI:	Nicolas NAVET
Funding:	University of Luxembourg
Budget:	156,822.00 €
Duration:	1 Jul 2016 – 30 Jun 2019
Member:	Nicolas NAVET (Principal Investigator)
Area:	Security, Reliability and Trust in Information Technology

Description

In our everyday life, we interact with a huge number of computer systems embedded into larger devices. Examples are phones, cars, home and factory appliances, airplanes and many more. Many of these devices are subject to real-time constraints. Real-time means that the correctness of a system is not only a functional (the right result), but also an extra-functional property (the right result at the right time). Currently, the development of such systems is very challenging as high-level modelling tools only capture the functional behaviour, whereas the timing behaviour simply happens: as the exact timing behaviour depends on the precise target architecture, little to no knowledge about the exact timing is available at an early design-phase.

The aim of the project is to re-think the development process of real-time embedded systems and to devise a timing-aware model-driven design process. In stark contrast to the current best-practice approach, we aim at a timing verification already at the modelling level, i.e., right from the start. To lift the timing behaviour from the low-level architecture to the high-level model, we propose to use model interpretation instead of compilation. The model interpreter on the target architecture must provide the same timing behaviour as a model verifier on the host machine, where the high-level model is developed and verified. We refer to this property as timing equivalence. We believe that the strongly simplified and accelerated model development and model verification (including functional verification and timing verification), will outweigh by far the additional overhead due to model interpretation on the target architecture. In the project, we will put this assumption to the test and develop a prototype of the timing-aware model-driven design process.

Unclonable Networks for Identification using Cholesteric Emulsions

Acronym:	UNIQUE
PI:	Jan LAGERWALL, Gabriele LENZINI
Funding:	University of Luxembourg
Budget:	397,000.00 €
Duration:	1 Apr 2015 – 31 Mar 2018
Members:	• Gabriele LENZINI (Principal Investigator) • Samir OUCHANI (Collaborator) • Peter ROENNE (Collaborator) • Peter Y. A. RYAN (Collaborator)

Description

We live in an era where digital services are offered ubiquitously, with increasingly sensitive and valuable transactions being effectuated on-line. This creates an urgent need to uniquely and safely identify and authenticate persons and goods. At the same time we demand personal integrity and there is a strong - and well-founded - reluctance to allow authorities to register biometric data, challenging many approaches to ensure security and privacy. A promising approach to solving the problem is to introduce an artificial identity pattern (IDP) into the authentication chain. IDPs should be as unique as the fingerprint or iris of a person, unclonable, but allow production at low cost in enormous quantities without risking overlap between IDPs. They should be robust and easy to read out quickly and repeatedly for identification and authentication purposes. UNIQUE aims to develop such a pattern, using microfluidics to produce an emulsion of cholesteric liquid crystal shells in specific 2D arrangement. The spherically symmetric photonic crystal properties of cholesteric shells lead to an intricate pattern of brightly colored and circularly polarized reflections. The details depend sensitively on the arrangement and internal order of the shells, and spots can be turned on or off dynamically by modulating the area and/or wavelength of illumination. By combining the very different expertise of a soft matter physics/materials science group and an information and communication technology group specializing in security and trust issues, this strongly interdisciplinary project aims to solve a critical societal and commercial/industrial problem by using a novel and promising approach to liquid crystal technology, involving microfluidic emulsification, polymerization, advanced optics, machine-based pattern analysis, computer simulations and novel security protocol development.

Appendix C

Representational Activities

C.1 Conference Committee Memberships

10th EAI International Conference on Bio-inspired Information and Communications Technologies (BICT 2017)

Location: Hoboken, United States of America, 15 Mar 2017 – 16 Mar 2017.

Participating Members:

- Sjouke MAUW (Program Committee Member)

10th International Conference on Security of Information and Networks (SIN 2017)

http://www.sinconf.org/sin2017/index.php

Location: Jaipur, India, 13 Oct 2017 – 15 Oct 2017.

Description: The 10th International Conference on Security of Information and Networks (SIN-2017) organized by School of Computing and Information Technology (SCIT), provides an excellent international forum for sharing knowledge and results in theory, methodology and applications of Security in information and networks. Papers, special sessions, tutorials, and workshops addressing all aspects and issues of security in information and networks are being pursued. The conference invites significant contributions from researchers and industrial working on the development of cryptographic algorithms, security schemes, cryptanalysis, application security, system security, cloud security and network security. The aim of the conference is to provide a platform to the researchers and practitioners from both academia as well as industry to meet

and share cutting-edge advancements in the field of information and network security.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

10th International Symposium on Foundations & Practice of Security (FPS'17)

Location: Nancy, France, 23 Oct 2017 – 25 Oct 2017.

Participating Members:

- Jun PANG (Program Committee Member)

11th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO 2017)

Location: Tucson, AZ, United States of America, 18 Sep 2017 – 22 Sep 2017.

Participating Members:

- Jean BOTEV (Program Committee Member, Doctoral Symposium Chair)

11th International Conference on Network and System Security (NSS 2017)

https://research.comnet.aalto.fi/NSS2017/

Location: Helsinki, Finland, 21 Aug 2017 – 23 Aug 2017.

Description: While the attack systems have become more easy-to-use, sophisticated, and powerful, interest has greatly increased in the field of building more effective, intelligent, adaptive, active and high performance defense systems which are distributed and networked. The conference will cover research on all theoretical and practical aspects related to network and system security, such as authentication, access control, availability, integrity, privacy, confidentiality, dependability and sustainability of computer networks and systems. The aim of NSS is to provide a leading edge forum to foster interaction between researchers and developers with the network and system security communities, and to give attendees an opportunity to interact with experts in academia, industry, and governments.

NSS 2017 is the next event in a series of highly successful events of Network and System Security. Previous editions were held in: Taipei (2016), New York City, USA (2015), Xi'an, China (2014), Madrid, Spain (2013), Wu Yi Shan, China (2012),

Milan, Italy (2011), Melbourne, Australia; (2010), Gold Coast, Australia (2009), Shanghai, China (2008), and Dalian, China (2007).

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

11th International Symposium on Theoretical Aspects of Software Engineering (TASE'17)

Location: Sophia Antipolis, France, 13 Sep 2017 – 15 Sep 2017.

Participating Members:

- Jun PANG (Program Committee Member)

11th WISTP International Conference on Information Security Theory and Practice (WISTP 2017)

Location: Heraklion, Greece, 28 Sep 2017.

Participating Members:

- Sjouke MAUW (Program Committee Member)

13th IEEE International Workshop on Factory Communication Systems (WFCS'2017)

http://wfcs2017.org

Location: Trondheim, Norway, 31 May 2017 – 2 Jun 2017.

Participating Members:

- Tingting HU (Program Committee Member)

13th International Workshop on Security and Trust Management

Location: Oslo, Norway, 14 Sep 2017 – 15 Sep 2017.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

13th International Workshop on Security and Trust Management (STM 2017)

Location: Oslo, Norway, 14 Sep 2017 – 15 Sep 2017.

Participating Members:

- Sjouke MAUW (Program Committee Member)

14th European Semantic Web Conference (ESWC-17)

https://2017.eswc-conferences.org/

Location: Portoroz, Slovenia, 28 May 2017 – 1 Jun 2017.

Description: The ESWC is a major venue for discussing the latest scientific results and technology innovations around semantic technologies. Building on its past success, ESWC is seeking to broaden its focus to span other relevant related research areas in which Web semantics plays an important role.

The goal of the Semantic Web is to create a Web of knowledge and services in which the semantics of content is made explicit and content is linked to both other content and services allowing novel applications to combine content from heterogeneous sites in unforeseen ways and support enhanced matching between users needs and content. This network of knowledge-based functionality will weave together a large network of human knowledge, and make this knowledge machine-processable to support intelligent behaviour by machines. Creating such an interlinked Web of knowledge which spans unstructured text, structured data (e.g. RDF) as well as multimedia content and services requires the collaboration of many disciplines, including but not limited to: Artificial Intelligence, Natural Language Processing, Databases and Information Systems, Information Retrieval, Machine Learning, Multimedia, Distributed Systems, Social Networks, Web Engineering, and Web Science. These complementarities are reflected in the outline of the technical program of the ESWC 2017; in addition to the standard research and in-use tracks, we will feature two special tracks putting particular emphasis on interdisciplinary research topics and areas that show the potential of exciting synergies for the future, namely: 'Multilinguality' and 'Semantics and Transparency'. ESWC 2017 will present the latest results in research, technologies and applications in its field. Besides the technical program organized over twelve tracks, the conference will feature a workshop and tutorial program, a dedicated track on Semantic Web challenges, system descriptions and demos, a posters exhibition and a doctoral symposium.

Participating Members:

- Giovanni CASINI (Program Committee Member)

14th IEEE International Conference on Advanced and Trusted Computing (ATC'17)

Location: San Francisco, United States of America, 4 Aug 2017.

Participating Members:

- Olga GADYATSKAYA (Program Committee Member)
- Rolando TRUJILLO RASUA (Program Committee Member)

14th IEEE International Conference on Ubiquitous Intelligence and Computing (UIC'17)

Location: San Francisco, United States of America, 4 Aug 2017 – 8 Aug 2017.

Participating Members:

- Jun PANG (Program Committee Member)

16th International Conference on Cryptology And Network Security (CANS 2017)

Location: Hong Kong, Hong Kong, 29 Nov 2017 – 2 Dec 2017.

Participating Members:

- Vincenzo IOVINO (Program Committee Member)

17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid'17)

Location: Madrid, Spain, 14 May 2017 – 18 May 2017.

Participating Members:

- Jun PANG (Program Committee Member)

19th International Conference on Formal Engineering Methods (ICFEM'17)

Location: Xian, China, 13 Nov 2017 – 17 Nov 2017.

Participating Members:

- Jun PANG (Program Committee Member)

20th Annual International Conference on Information Security and Cryptology (ICISC 2017)

Location: Seoul, South Korea, 29 Nov 2017 – 1 Dec 2017.

Participating Members:

- Sjouke MAUW (Program Committee Member)

20th International Conference on Information and Communications Security (ICICS2017)

http://www.icisc.org/icisc/asp/index.html

Location: Seoul, South Korea, 29 Nov 2017 – 1 Dec 2017.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

22nd Australasian Conference on Information Security and Privacy 2017

Location: Auckland, New Zealand, 3 Jul 2017 – 5 Jul 2017.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

22nd European Symposium on Research in Computer Security (ESORICS 2017)

Location: Oslo, Norway, 11 Sep 2017 – 15 Sep 2017.

Participating Members:

- Sjouke MAUW (Program Committee Member)

22nd IEEE Pacic Rim International Symposium on Dependable Computing (PRDC 2017)

Location: Christchurch, New Zealand, 22 Jan 2017 – 25 Jan 2017.

Participating Members:

- Sjouke MAUW (Program Committee Member)

22nd International Conference on Engineering of Complex Computer Systems (ICECCS'17),

Location: Fukuoka, Japan, 5 Nov 2017 – 7 Nov 2017.

Participating Members:

- Jun PANG (Program Committee Member)

23rd International Symposium on Methodologies for Intelligent SystemsISMIS -

http://ismis2017.ii.pw.edu.pl/

Location: Warsaw, Poland, 26 Jun 2017 – 29 Jun 2017.

Participating Members:

- Christoph SCHOMMER (PC Member)

24rd Conference on Selected Areas in Cryptography (SAC 2017)

http://sacworkshop.org/SAC17/SAC2017.htm

Location: Ottawa, Canada, 16 Aug 2017 – 18 Aug 2017.

Description: The conference on Selected Areas in Cryptography (SAC) is an annual conference dedicated to specific themes in the area of cryptographic system design and analysis. Authors will present original research papers related to the themes for the SAC 2017 conference:

1. Design and analysis of symmetric key cryptosystems
2. Primitives for symmetric key cryptography, including block and stream ciphers, hash functions, and MAC algorithms
3. Efficient implementations of symmetric and public key algorithms
4. Post-quantum cryptography

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

24th ACM Conference on Computer and Communications Security (ACM CCS 2017)

https://ccs2017.sigsac.org

Location: Dallas, United States of America, 30 Oct 2017 – 3 Nov 2017.

Description: The ACM Conference on Computer and Communications Security (CCS) is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM). The conference brings together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results. It provides an environment to conduct intellectual discussions. From its inception, CCS has established itself as a high-standard research conference in its area.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

24th IEEE International Conference on Software Analysis, Evolution, and Reengineering

Location: Klagenfurt, Austria, 21 Feb 2017 – 24 Feb 2017.

Participating Members:

- Dongsun KIM (Program Committee Member)

25th IEEE International Conference on Software Analysis, Evolution and Reengineering

Location: Campobasso, Italy, 20 Mar 2017 – 23 Mar 2017.

Participating Members:

- Dongsun KIM (Program Committee Member)

30th IEEE International Symposium on Computer-based Medical Systems

Location: Thessaloniki, Greece, 22 Jun 2017 – 24 Jun 2017.

Participating Members:

- Christoph SCHOMMER (PC Member)

31st International Conference on Information Networking (ICOIN)

http://2017.icoin.org/sub/sub01.asp?sub_param=1

Location: Da Nang, Vietnam, 11 Jan 2017 – 13 Jan 2017.

Description: The 31st International Conference on Information Networking (ICOIN) is organized by KIISE and technically co-sponsored by IEEE Computer Society. For the past 31 years, computer communication and networking technologies have changed every aspect of our lives and societies. While computer networks have contributed largely to the current ICT advancement, it will play a key role in new ICT paradigms such as IoT and cloud computing and will be applied to various areas of the upcoming society including industry, business, politics, culture, medicine and so on.

ICOIN is the most comprehensive conference focused on the various aspects of advances in computer communication and networking technologies. The main purpose of ICOIN 2017 is to improve our research by achieving the highest capability and encourage open discussions on computer communication and networking technologies. Authors are invited to submit original unpublished manuscripts that demonstrate recent advances in computer communications, wireless/mobile networks, and converged networks in the theoretical and practical aspects. Accepted papers will be published in the proceedings with an assigned ISBN number and submitted to IEEE Xplore, SCOPUS, and EI Compendex.

Participating Members:

- Pascal BOUVRY (Technical Program Committee Member)

32nd International Conference on ICT Systems Security and Privacy Protection

Location: Rome, Italy, 29 May 2017 – 31 May 2017.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

39th CogSci 2017

http://www.cognitivesciencesociety.org/conference/cogsci2017/

Location: London, United Kingdom, 26 Jul 2017 – 29 Jul 2017.

Description: see http://www.cognitivesciencesociety.org/conference/cogsci2017/

Participating Members:

- Christoph SCHOMMER (PC Member)

3rd IEEE International Conference on Cybernetics

http://cse.stfx.ca/~CybConf2017/index.php

Location: Exeter, United Kingdom, 21 Jun 2017 – 23 Jun 2017.

Description: The biennial International Conference on Cybernetics (CYBCONF) provides a premier international forum for researchers and practitioners to report the latest innovations, summarize the state-of-the-art, and exchange ideas and advances in all aspects of Cybernetics. Apart of the main track it includes special sessions and plenary talks by invited eminent speakers.

CYBCONF-2017 is organized by University of Exeter, sponsored byIEEE Systems, Man, and Cybernetics Society (SMC), and supported by IEEE SMC Technical Committees on Cybermatics for Cyber-enabled Worlds; Awareness Computing; Intelligent Industrial Systems; and Distributed Intelligent Systems. CYBCONF-2017 will be hosted in Exeter, the capital city of Devon and provides the county with a central base for education, medicine, religion, commerce and culture. The city is also home to the magnificent Exeter Cathedral, which dates back to Norman times. Exeter is also ideally placed to base a trip to branch out visiting places such as the famous Dartmoor National Park and the unspoilt beaches of the North and South Devon coastlines.

Participating Members:

- Nicolas GUELFI (Program Committee Member)

3rd Symposium on Dependable Software Engineering (SETTA'17)

Location: Changsha, China, 25 Oct 2017.

Participating Members:

- Jun PANG (Program Committee Member)

3rd Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems (CyberICPS 2017)

Location: Oslo, Norway, 14 Sep 2017 – 15 Sep 2017.

Participating Members:

- Sjouke MAUW (Program Committee Member)

3th International Conference Beyond Databases, Architectures and Structures

Location: Ustron/Krakau, Poland, 30 May 2017 – 2 Jun 2017.

Participating Members:

- Christoph SCHOMMER (Panelist)

41st IEEE Computer Society International Conference on Computers, Software & Applications (COMPSAC'17)

Location: Turin, Italy, 4 Jul 2017 – 8 Jul 2017.

Participating Members:

- Jun PANG (Program Committee Member)

4th International Conference on Cryptography and Security Systems (C&SS 2017)

Location: Prague, Czech Republic, 3 Sep 2017 – 6 Sep 2017.

Participating Members:

- Sjouke MAUW (Program Committee Member)

4th International Workshop on Self-Improving System Integration (SISSY 2017)

Location: Columbus, OH, United States of America, 17 Jul 2017 – 21 Jul 2017.

Participating Members:

- Jean BOTEV (Program Committee Member)

5th International Conference on Algorithmic Decision Theory (ADT 2017)

https://sma.uni.lu/adt2017/

Location: Luxembourg, Luxembourg, 25 Oct 2017 – 27 Oct 2017.

Description: The ADT 2017 conference seeks to bring together researchers and practitioners coming from diverse areas such as *Artificial Intelligence, Database Systems, Operations Research, Discrete Mathematics, Theoretical*

Computer Science, Decision Theory, Game Theory, Multiagent Systems, Computational Social Choice, Argumentation Theory, and *Multiple Criteria Decision Aiding* in order to improve the theory and practice of modern decision support. Some of the scientific challenges facing the Algorithmic Decision Theory (ADT) community include big preference data, combinatorial structures, partial and/or uncertain information, distributed decision making, and large user bases. Such challenges occur in real-world decision making in domains like *electronic commerce, recommender systems, argumentation tools, network optimization* (communication, transport, energy), *risk assessment and management*, and *e-government*.

ADT 2017 provides a multi-disciplinary forum for sharing knowledge in this area with a special focus on algorithmic issues in Decision Theory. The first four International Conferences on Algorithmic Decision Theory: ADT 2009 Venice , ADT 2011 Rutgers (DIMACS), ADT 2013 Brussels, ADT 2015 Lexington (Kentucky US)) brought together researchers and practitioners from diverse areas of computer science, economics, and operations research from around the globe.

Participating Members:

- Raymond Joseph BISDORFF (Program Committee Member)
- Leon VAN DER TORRE (Program Committee Member)
- Raymond Joseph BISDORFF (Organizing Chair)

5th International Workshop on Self-Adaptive and Self-Organising Socio-Technical Systems (SASO^ST 2017)

Location: Tucson, AZ, United States of America, 22 Sep 2017.

Participating Members:

- Jean BOTEV (Program Committee Member)
- Steffen ROTHKUGEL (Program Committee Member)
- Jean BOTEV (Workshop Organiser / Co-Organiser)

5th International Workshop on Self-Optimisation in Organic and Autonomic Computing Systems (SAOS 2017)

Location: Vienna, Austria, 3 Apr 2017 – 4 Apr 2017.

Participating Members:

- Jean BOTEV (Program Committee Member)

5th Workshop on Hot Issues in Security Principles and Trust (HotSpot 2017)

Location: Uppsala, Sweden, 23 Apr 2017.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

7th International Workshop on Peer-to-Peer Architectures, Networks and Systems (PANS 2017)

Location: Genoa, Italy, 17 Jul 2017 – 21 Jul 2017.

Participating Members:

- Jean BOTEV (Program Committee Member)

8th IEEE INFOCOM International Workshop on Mobility Management in the Networks of the Future World (MobiWorld)

http://infocom2017.ieee-infocom.org/workshop/mobiworld-mobility-management-networks-future-world

Location: Atlanta, United States of America, 1 May 2017.

Description: Mobility management has been identified as a key technology in the areas of heterogeneous networks, mobile networks, vehicular networks, multimedia computing, and autonomous computing, as well as in the Future Internet. The development of mobility management in the areas is expected to enable mobility services for users, vehicles, robots, etc. However, many issues in mobility management including location update, handover, identity split, security, and performance analysis have posed various challenges to the academic and industry. The purpose of MobiWorld 2017 is to bring together the academic and industry working on different aspects, exchange ideas, and explore new research directions for addressing the challenges in mobility management. MobiWorld 2017 also aims to publish high quality papers which are closely related to various theories and practical applications in mobility management to highlight the state-of-art research.

Participating Members:

- Sébastien FAYE (Technical Program Committee Member)

8th IEEE INFOCOM International Workshop on Mobility Management in the Networks of the Future World (MobiWorld'17)

http://infocom2017.ieee-infocom.org/workshop/mobiworld-mobility-management-networks-future-world

Location: Atlanta, GA, United States of America, 1 May 2017.

Description: Mobility management has been identified as a key technology in the areas of heterogeneous networks, mobile networks, vehicular networks, multimedia computing, and autonomous computing, as well as in the Future Internet. The development of mobility management in the areas is expected to enable mobility services for users, vehicles, robots, etc. However, many issues in mobility management including location update, handover, identity split, security, and performance analysis have posed various challenges to the academic and industry. The purpose of MobiWorld 2017 is to bring together the academic and industry working on different aspects, exchange ideas, and explore new research directions for addressing the challenges in mobility management. MobiWorld 2017 also aims to publish high quality papers which are closely related to various theories and practical applications in mobility management to highlight the state-of-art research.

Participating Members:

- Sébastien FAYE (Technical Program Committee Member)

8th International SuperComputing Camp 2017

http://www.sc-camp.org/2017/

Location: Cadiz, Spain, 23 Oct 2017 – 28 Oct 2017.

Description: SC-Camp is a summer school and non-profit event about Super Computing and Distributed Systems. It proposes a series of courses around the thematic of High Performance Computing with an important focus on practical sessions (more than half of the time). It targets Master and PhD students in the field of Computer Sciences, Engineering and any other fields that could benefit from HPC (Physics & Material Sciences, Biology/Bioinformatics, Finance, etc.).

Taking advantage of the Internet and high speed networks available today, one can exploit high performance computing infrastructures from anywhere, even located in the middle of the nature. SC-Camp is an initiative of researchers inspired by this idea that offers undergraduate and master students state-of-the-art lectures and programming practical sessions upon High Performance and Distributed Computing topics. It is an itinerant school, bringing the HPC knowledge to a different place every year.

SC-Camp is a non-profit event, addressed to all students including those that lack of financial backup, so we try to keep the cost for the students as low as possible.

Content

The summer school focus on the following topics:

- Distributed Systems: Grid/Cluster/Cloud/Volunteer Computing
- Distributed parallel programming with MPI

- Shared Memory parallel programming with OpenMP
- Accelerators: GPUs with CUDA, XeonPhi
- Debugging and Performance Optimization
- Data Analysis with R
- Resource/Job Management & Scheduling
- Big Data

Please check the detailed program here.

Organization

SC-Camp 2017 features 5 days of scientific sessions, during which several programming practical sessions will be held.

We welcome applications of undergraduate (preferable in Senior year) or master students from all areas of Engineering and Computational Sciences with strong interest upon High Performance and Distributed Computing. Due to the advanced content of lectures some basic notions of Parallel and Distributed Computing along with programming skills are desirable. All courses and lectures will be held in English, thus a good knowledge of English -both oral and written- is mandatory. The scientific and steering committee will evaluate the application forms based on the applicant's scientific background and their motivation letter. This year, as the former year, we expect to accept 20 - 40 students.

Participants

Master and PhD students in the field of Computer Science, or any other domain working with HPC (Physics, Material Science, Biology/Bioinformatics, Finance, etc.), who are already familiar with programming. SC-Camp is the perfect event to learn all about Distributed and Parallel programming, from basics to the most advanced level, offering a thoughtful practical experience in High Performance Systems to assimilate the concepts.

Participating Members:

- Sébastien VARRETTE (Invited Speaker)

8th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2017)

http://cosade.telecom-paristech.fr

Location: Paris, France, 13 Apr 2017 – 14 Apr 2017.

Description: Side-channel analysis (SCA) and implementation attacks have become an important field of research at universities and in the industry. In order to enhance the resistance of cryptographic and security critical implementa-

tions within the design phase, constructive attacks and analyzing techniques may serve as a quality metric to optimize the design and development process. Since 2010, COSADE provides an international platform for researchers, academics, and industry participants to present their work and their current research topics. It is an excellent opportunity to exchange on new results with international experts and to initiate new collaborations and information exchange at a professional level. The workshop will feature both invited presentations and contributed talks.

The eighth International Workshop on Constructive Side-Channel Analysis and Secure Design will be organized and held by Télécom ParisTech, Paris, France.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

8th International Workshop on Emerging Trends in Software Metrics

Location: Buenos Aires, Argentina, 23 May 2017.

Participating Members:

- Dongsun KIM (Program Committee Member)

9th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2017)

https://2017.cloudcom.org

Location: Hong Kong, Hong Kong, 11 Dec 2017 – 14 Dec 2017.

Description: CloudCom is the premier conference on Cloud Computing worldwide, attracting researchers, developers, users, students and practitioners from the fields of big data, systems architecture, services research, virtualization, security and privacy, high performance computing, always with an emphasis on how to build cloud computing platforms with real impact. The conference is co-sponsored by the Institute of Electrical and Electronics Engineers (IEEE), is steered by the Cloud Computing Association, and draws on the excellence of its world-class Program Committee and its participants.

The 9th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2017) will be held in Hong Kong on 11-14 December 2017.

Participating Members:

- Valentin PLUGARU (Technical Program Committee Member)

9th International Conference on Agents and Artificial Intelligence (ICAART)

Location: Porto, Portugal, 24 Feb 2017 – 26 Feb 2017.

Participating Members:

- Christoph SCHOMMER (PC Member)

9th International Workshop on Massively Multiuser Virtual Environments (MMVE 2017)

Location: Taipei, Taiwan, 20 Jun 2017 – 23 Jun 2017.

Participating Members:

- Jean BOTEV (Program Committee Member)

AAMAS 2017

http://www.aamas2017.org/

Location: Sao Paulo, Brazil, 8 May 2017 – 12 May 2017.

Description: AAMAS is the largest and most influential conference in the area of agents and multiagent systems. The aim of the conference is to bring together researchers and practitioners in all areas of agent technology and to provide a single, high-profile, internationally renowned forum for research in the theory and practice of autonomous agents and multiagent systems.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

ACM GECCO 2017

http://gecco-2017.sigevo.org/index.html/HomePage

Location: Berlin, Germany, 15 Jul 2017 – 19 Jul 2017.

Description: The Genetic and Evolutionary Computation Conference (GECCO) presents the latest high-quality results in genetic and evolutionary computation since 1999.

Participating Members:

- Grégoire DANOY (Program Committee Member)

ACM TURC 2017 (SIGSAC China)

Location: Shanghai, China, 12 May 2017 – 14 May 2017.

Participating Members:

- Zhe LIU (PC Member)

Advances in Secure, Electronic Voting Second workshop in association with Financial Crypt (Voting'17)

Location: Sliema, Malta, 7 Apr 2017.

Participating Members:

- Peter Y. A. RYAN (Co-Chair)

AICOL2017@JURIX2017

http://www.aicol.eu/

Location: Luxembourg, Luxembourg, 13 Dec 2017.

Description: The AICOL workshops welcome research in AI, political and legal theory, jurisprudence, philosophy of technology and the law, social intelligence, NorMAS, to address the ways in which the current information revolution affects basic pillars of today's legal and political systems, in such fields as e-democracy, e-government, e-justice, transnational governance, Data Protection, and Security.

We are, indeed, dealing with changes and developments that occur at a rapid pace, as the law transforms itself, in order to respond to and progress alongside with the advances of technology. In addition to the traditional hard and soft law-tools of governance, such as national rules, international treaties, codes of conduct, guidelines, or the standardization of best practices, the new scenarios of the information revolution have increasingly suggested the aim to govern current ICTs-driven societies through the mechanisms of design, codes and architectures. AI approaches to the complexity of legal systems should take into account how the regulatory tools of technology impact on canonical interpretations of the law. This Workshop is mainly addressed to computer scientists, legal theorists, social scientists, and philosophers.

Participating Members:

- Livio ROBALDO (Program Committee Member)
- Leon VAN DER TORRE (Program Committee Member)

BIDMA 2017

Location: Calgary, Canada, 17 Apr 2017 – 18 Apr 2017.

Description:

International Symposium on Big Data Management and Analytics

Participating Members:

- Christoph SCHOMMER (PC Member)

BNAIC 2017

http://bnaic2017.ai.rug.nl

Location: Gronigen, Netherlands, 8 Nov 2017 – 9 Nov 2017.

Description: 29th Benelux Conference on Artificial Intelligence

Participating Members:

- Grégoire DANOY (Program Committee Member)

CA3PP-2017 17th International Conference on Algorithms and Architectures for Parallel Processing

https://research.comnet.aalto.fi/ICA3PP2017/

Location: Helsinki, Finland, 21 Aug 2017 – 23 Aug 2017.

Description: ICA3PP 2017 is the 17th in this series of conferences started in 1995 that are devoted to algorithms and architectures for parallel processing. ICA3PP is now recognized as the main regular event of the world that is covering the many dimensions of parallel algorithms and architectures, encompassing fundamental theoretical approaches, practical experimental projects, and commercial components and systems. As applications of computing systems have permeated in every aspects of daily life, the power of computing system has become increasingly critical. This conference provides a forum for academics and practitioners from countries around the world to exchange ideas for improving the efficiency, performance, reliability, security and interoperability of computing systems and applications.

Following the traditions of the previous successful ICA3PP conferences held in Hangzhou, Brisbane, Singapore, Melbourne, Hong Kong, Beijing, Cyprus, Taipei, Busan, Melbourne, Fukuoka, Vietri sul Mare, Dalian,Japan, Zhangjiajie,

and Granada, ICA3PP 2017 will be held in Helsinki, Finland. The objective of ICA3PP 2017 is to bring together researchers and practitioners from academia, industry and governments to advance the theories and technologies in parallel and distributed computing. ICA3PP 2017 will focus on two broad areas of parallel and distributed computing, i.e. architectures, algorithms and networks, and systems and applications. The conference of ICA3PP 2017 will be co-organized by Aalto University, Finlan and Xidian University, China.

Participating Members:

- Pascal BOUVRY (PC Member, PC Member)
- Grégoire DANOY (PC Member)
- Sébastien VARRETTE (PC Member)

CARLA 2017 : Latin American HPC Conference - CARLA 2017 - Springer CCIS Series

http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=61086&copyownerid=95805

Location: Buenos Aires, Argentina, 20 Sep 2017 – 22 Oct 2017.

Description: Building on the success of the previous editions of the CARLA Conference (and former HPCLATAM and CLCAR Conferences), the tenth edition will be organized by Universidad de Buenos Aires (Argentina) and Universidad de la República (Uruguay).

The main goal of CARLA is to provide a forum fostering the growth of the HPC community in Latin America, through the exchange and dissemination of new ideas, techniques, and research in HPC. CARLA will feature invited talks from academy and industry, short and fullpaper sessions presenting mature work and new ideas in research and industrial applications.

Suggested topics of interest include, but are not restricted to: Distributed Systems, Parallel Algorithms and Concurrency; GPU and MIC Computing; Mobile, Grid & Cloud Computing; Big data, Data Management & Visualization; Scientific Computing & Computing Applications; Architecture, Infrastructure and HPC Data Center; HPC Computing Education and Outreach; Industrial Solutions.

Participating Members:

- Pascal BOUVRY (Keynote speaker)

CCGRID 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid

https://www.arcos.inf.uc3m.es/ccgrid2017/

Location: Madrid, Spain, 14 May 2017 – 17 May 2017.

Description: CCGrid is a successful series of conferences that serves as the major international forum for presenting and sharing recent research results and technological developments in the fields of Cluster, Cloud and Grid computing. The CCGrid symposium, which is sponsored by the IEEE Computer Society Technical Committee on Scalable Computing (TCSC) and the ACM, reaches out to both researchers and practitioners, and to both academia and industry. The conference features keynotes, technical presentations, posters, workshops, tutorials, as well as the SCALE challenge featuring live demonstrations. CCGrid has traveled the world over, and this year will be held in May in Madrid, Spain, for the first time. Madrid is the capital City of Spain and it gathers a thrilling mix of antique and modern cultures that is reflected in their environment, monuments, and warm people.

Topics of interest

CCGrid 2017 will have a focus on important and immediate issues that are significantly influencing all aspects of cluster and cloud computing. Topics of interest include, but are not limited to:

- Applications and Big Data
- Architecture and Networking
- Data Centers and CyberInfrastructure
- Programming Models and Runtime Systems
- Performance Modeling and Evaluation
- Scheduling and Resource Management
- Mobile and Hybrid Clouds
- Storage and I/O
- Security, Privacy and Reliability

Participating Members:

- Pascal BOUVRY (Program Committee Member, Program Committee Member)
- Sébastien VARRETTE (Program Committee Member)
- Jun PANG (PC Member)

Central European Cybersecurity Conference 2017

Location: Ljubljan, Slovenia, 16 Nov 2017 – 17 Nov 2017.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

cex 2017 @ IA*AI 2017

https://cex.inf.unibz.it/

Location: Bari, Italy, 16 Nov 2017 – 17 Nov 2017.

Description: Quite frequently demands for better comprehensible and explainable Artificial Intelligence (AI) and Machine Learning (ML) systems are being put forward. The **cex** workshop sheds light on notions such as "comprehensibility" and "explanation" in the context of AI and ML, working towards a better understanding of what an explanation is when talking about intelligent systems, what it means to comprehend a system and its behaviour, and how human-machine interaction can take these dimensions into account.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

CICN 2017 9th International Conference on Computational Intelligence and Communication Networks

http://cicn2017.org/

Location: GIRNE, Cyprus, 16 Sep 2017 – 17 Sep 2017.

Description: The 9th International Conference on Computational Intelligence and Communication Networks (CICN 2017) is organized to address various issues to prosper the creation of intelligent solutions in future. The aim is to bring together worldwide leading researchers, developers, practitioners and educators interested in advancing the state of the art in computational intelligence and communication Networks for exchanging knowledge that encompasses a broad range of disciplines among various distinct communities. It is expected that researchers will bring new prospect for collaboration across disciplines and gain idea facilitating novel breakthrough. The theme for this conference is Innovating and Inspiring the researchers to adopt the outcome for implementation.

The conference will provide an exceptional platform to the researchers to meet and discuss the utmost solutions, scientific results and methods in solving intriguing problems with people that actively involved in these evergreen fields. The 3-day conference commencing from 16 Sep will feature prominent keynote speakers, tutorials and paper presentation in parallel sessions. All accepted papers will appear in conference proceedings published by the Conference Publishing Services.

CICN 2017 will no doubt be proven to be exciting and educative. The General Chair, along with the entire team cordially invite you to take part in this upcom-

ing event and together we flourish it into a most memorable experience. Organising committee will also plan for various tours to various historical Places around Sea Resorts of North Cyprus.

Participating Members:

- Pascal BOUVRY (Workshop Organiser / Co-Organiser, Organising Committee)

CloudCom 2017 9th International Conference on Cloud Computing Technology and Science

http://2017.cloudcom.org/

Location: Hong Kong, Hong Kong, 11 Dec 2017 – 14 Jan 2018.

Description: CloudCom is the premier conference on Cloud Computing worldwide, attracting researchers, developers, users, students and practitioners from the fields of big data, systems architecture, services research, virtualization, security and privacy, high performance computing, always with an emphasis on how to build cloud computing platforms with real impact. The conference is co-sponsored by the Institute of Electrical and Electronics Engineers (IEEE), is steered by the Cloud Computing Association, and draws on the excellence of its world-class Program Committee and its participants.

The 9th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2017) will be held in Hong Kong on 11-14 December 2017. Pre-registration is required.

Participating Members:

- Grégoire DANOY (Track / Working Group Chair)
- Sébastien VARRETTE (Track / Working Group Chair)
- Pascal BOUVRY (Technical Program Committee Member, Technical Program Committee Member)

COLIEE 2017@ICAIL2017

http://webdocs.cs.ualberta.ca/~miyoung2/COLIEE2017/

Location: London, United Kingdom, 12 Jun 2017 – 13 Jun 2017.

Description: In 2017, International Conference on Artificial Intelligence and Law (ICAIL) newly invites participation in a competition on legal information extraction/entailment. We held the previous three competitions on legal information extraction/entailment (COLIEE 2014-2016) on a legal data collection with the JURISIN workshop, and they helped establish a major experimental effort in the legal information extraction/retrieval field. We will hold the fourth

competition (COLIEE-2017) in 2017 with the ICAIL conference, and the motivation for the competition is to help create a research community of practice for the capture and use of legal information.

Participating Members:

- Livio ROBALDO (Program Committee Member)

CORIA 2017

http://www3.lsis.org/coria2017/

Location: Marseille, France, 29 Mar 2017 – 31 Mar 2017.

Participating Members:

- Christoph SCHOMMER (PC Member)

CPSCOM 2017

http://cse.stfx.ca/~CPSCom2017/

Location: Exeter, United Kingdom, 21 Jun 2017 – 23 Jun 2017.

Description: The 2017 IEEE International Conference on Cyber, Physical, and Social Computing (CPSCom-2017) will provide a high-profile, leading-edge forum for researchers, engineers, and practitioners to present state-of-art advances and innovations in theoretical foundations, systems, infrastructure, tools, testbeds, and applications for the CPSCom, as well as to identify emerging research topics and define the future.

Participating Members:

- Grégoire DANOY (Program Committee Member)

CryptoIC2017

Location: Chengdu, China, 22 Sep 2017 – 24 Sep 2017.

Participating Members:

- Zhe LIU (Keynote speaker)

CSNT 2017 7th International Conference on Communication Systems and Network Technologies

https://www.aconf.org/conf_104741.2017_7th_International_Conference_on_Communication_Systems_and_Network_Technologies.html

Location: Nagpur Maharashtra, India, 11 Nov 2017 – 13 Nov 2017.

Description: The International Conference on Communication Systems and Network Technologies (CSNT-2017) is organized by IIIT Nagpur in association with Machine Intelligence Research Labs, Gwalior with technical support of IEEE Bombay Section to address various issues to prosper the creation of intelligent solutions in future. The aim is to bring together worldwide leading researchers, developers, practitioners and educators interested in advancing the state of the art in computational intelligence and communication Networks for exchanging knowledge that encompasses a broad range of disciplines among various distinct communities. It is expected that researchers will bring new prospect for collaboration across disciplines and gain idea facilitating novel breakthrough. The theme for this conference is Innovating and Inspiring the researchers to adopt the outcome for implementation.

The conference will provide an exceptional platform to the researchers to meet and discuss the utmost solutions, scientific results and methods in solving intriguing problems with people that actively involved in these evergreen fields. The 3-day conference commencing from 11 Nov, will feature prominent keynote speakers, tutorials, Pannel Discussion, Workshops. All accepted and presented papers will submitted to Conference Publishing Services (CPS) for publication in IEEE CPS.

CSNT 2017 will no doubt be proven to be exciting and educative. The General Chairs, along with the entire team cordially invite you to take part in this upcoming event and together we flourish it into a most memorable experience.

Participating Members:

- Pascal BOUVRY (Technical Program Committee Member, Technical Program Committee Member)

DH 2017

Location: Montreal, Canada, 8 Aug 2017 – 11 Aug 2017.

Participating Members:

- Christoph SCHOMMER (PC Member)

DHd - Digital Humanities im Deutschsprachigen Raum 2017 - Digitale Nachhaltigkei

Location: Bern, Switzerland, 13 Feb 2017 – 18 Feb 2017.

Participating Members:

- Christoph SCHOMMER (PC Member)

Early Symmetric Crypto 2017 (ESC 2017)

https://www.cryptolux.org/mediawiki-esc2017/index.php/Main_Page

Location: Canach, Luxembourg, 16 Jan 2017 – 20 Jan 2017.

Description: Early Symmetric Cryptography (ESC) is a bi-annual event (2008, 2010, 2013, 2015) taking place in Luxembourg and paired with Dagstuhl seminars (2007, 2009, 2012, 2014, 2016) on symmetric cryptography.

Cryptography deals with secure communication in adversarial environments as well as protecting information in storage. It is the key ingredient of information security. Applications such as electronic commerce, e-banking, secure communications (ex. mobile phones, Skype, etc.) are made possible due to advances in applied cryptography. The seminar is concentrating on:

- symmetric primitives (block and stream ciphers, message authentication codes and hash functions), and
- complex cryptosystems and cryptographic protocols employing these primitives
- algorithmic challenges in public and symmetric cryptography.

The aim of the workshop is to bring together leading experts and talented junior researchers and to let them exchange ideas, open problems in an informal atmosphere.

Participating Members:

- Alexei BIRYUKOV (Programme Chair)

ECML-PKDD 2017

http://ecmlpkdd2017.ijs.si/

Location: Skopje, Macedonia, 18 Sep 2017 – 22 Sep 2017.

Participating Members:

- Christoph SCHOMMER (PC Member, PC Member)

ESORICS Doctoral Consortium 2017 – COINS Nordic Ph.D. Workshop

Location: Oslo, Norway, 15 Sep 2017.

Participating Members:

- Peter Y. A. RYAN (Technical Program Committee Member)

EUMAS 2017

https://eumas2017.ibisc.univ-evry.fr/index.php

Location: Evry, France, 14 Dec 2017 – 15 Dec 2017.

Description: In the last two decades, we have seen a significant increase of interest in agent- based computing. This field is now set to become one of the key intelligent systems technologies in the 21st century. The aim of the EUMAS series is to provide a forum for academics and practitioners in Europe at which current research and application issues are presented and discussed.

EUMAS 2017, the 15th instalment of the conference series, follows the tradition of previous editions (Oxford 2003, Barcelona 2004, Brussels 2005, Lisbon 2006, Hammamet 2007, Bath 2008, Agia Napa 2009, Paris 2010, Maastricht 2011, Dublin 2012, Toulouse 2013, Prague 2014, Athens 2015, Valencia 2016), and aims to encourage and support activity in the research and development of multi-agent systems, in academic and industrial efforts.

The conference is primarily intended as a European forum for anybody interested in the theory and practice of autonomous agents and multi-agent system to meet, present challenges, preliminary and mature research results in an open and informal environment. To attract students as well as experienced researchers, preliminary as well as mature work, EUMAS 2017 offers three submission types and formal proceedings. Also, post-publication in form of a special issues of a high-quality journal in the area are planned.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

Eurocrypt 2017

Location: Paris, France, 30 Apr 2017 – 4 May 2017.

Participating Members:

- Jean-Sébastien CORON (Co-Chair)

Euro-Par 2017 Workshops 23nd International Conference on Parallel and Distributed Computing Workshops

https://europar2017.usc.es/#euro-par-2017

Location: Galicia, Spain, 28 Aug 2017 – 1 Sep 2017.

Description: Euro-Par is the prime European conference covering all aspects of parallel and distributed processing, ranging from theory to practice, from small to the largest parallel and distributed systems and infrastructures, from fundamental computational problems to full-fledged applications, from architecture, compiler, language and interface design and implementation, to tools, support infrastructures, and application performance aspects. Euro-Par's unique organization into topics provides an excellent forum for focused technical discussion, as well as interaction with a large, broad and diverse audience.

Scope

We invite submissions of high-quality, novel and original research results in areas of parallel and distributed computing covered by the following topics:

1. Support Tools and Environments
2. Performance and Power Modeling, Prediction and Evaluation
3. Scheduling and Load Balancing
4. High Performance Architectures and Compilers
5. Parallel and Distributed Data Management and Analytics
6. Cluster and Cloud Computing
7. Distributed Systems and Algorithms
8. Parallel and Distributed Programming, Interfaces, and Languages
9. Multicore and Manycore Parallelism
10. Theory and Algorithms for Parallel Computation and Networking
11. Parallel Numerical Methods and Applications
12. Accelerator Computing

The conference will feature contributed and invited talks. Co-located workshops are also planned. See also the Paper Submission section.

Participating Members:

- Pascal BOUVRY (Technical Program Committee Member, Technical Program Committee Member)

European Symposium on Research in Computer Security (ESORICS 2017)

Location: Oslo, Norway, 11 Sep 2017 – 13 Sep 2017.

Participating Members:

- Peter Y. A. RYAN (Steering Committee Member)
- Gabriele LENZINI (Program Committee Member)
- Peter Y. A. RYAN (Program Committee Member)

FAB 2017

Location: Sydney, Australia, 1 Aug 2017 – 3 Aug 2017.

Participating Members:

- Christoph SCHOMMER (PC Member)

Fast Software Encryption 2017 (FSE 2017)

http://www.nuee.nagoya-u.ac.jp/labs/tiwata/fse2017/

Location: Tokyo, Japan, 5 Mar 2017 – 8 Mar 2017.

Description: Original research papers on symmetric cryptology are invited for submission to FSE 2017. The scope of FSE concentrates on fast and secure primitives for symmetric cryptography, including the design and analysis of block ciphers, stream ciphers, encryption schemes, hash functions, message authentication codes, (cryptographic) permutations, authenticated encryption schemes, cryptanalysis and evaluation tools, and security issues and solutions regarding their implementation. From this year, FSE 2017 also solicits submissions for Systematization of Knowledge (SoK) papers. These papers aim at revieweing and contextualizing the existing literature in a particular area in order to systematize the existing knowledge in that area. To be considered for publication, they must provide an added value beyond prior work, such as novel insights or reasonably questioning previous assumptions.

Participating Members:

- Dmitry KHOVRATOVICH (Program Committee Member)
- Vesselin VELICHKOV (Program Committee Member)

Fifth International Symposium on Security in Computing and Communications (SSCC 2017)

Location: Manipal, India, 13 Sep 2017 – 16 Sep 2017.

Participating Members:

- Sjouke MAUW (Program Committee Member)

Financial Cryptography and Data Security 2017 (FinCrypto 2017)

https://fc17.ifca.ai

Location: Malta, Malta, 3 Apr 2017 – 7 Apr 2017.

Description: Financial Cryptography and Data Security is a major international forum for research, advanced development, education, exploration, and debate regarding information assurance, with a specific focus on commercial contexts. The conference covers all aspects of securing transactions and systems. Original works focusing on both fundamental and applied real-world deployments on all aspects surrounding commerce security are solicited. Submissions need not be exclusively concerned with cryptography. Systems security and interdisciplinary works are particularly encouraged.

The goal of the conference is to bring security and cryptography researchers and practitioners together with economists, bankers, implementers and policy-makers. Intimate and colourful by tradition, the FC program features invited talks, academic presentations, technical demonstrations and panel discussions. In addition, several workshops will be held in conjunction with the FC conference.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

Fourth International Workshop on Defeasible and Ampliative Reasoning (DARe 2017)

https://sites.google.com/view/dare-17/

Location: Espoo, Finland, 3 Jul 2017.

Description: The International Workshop on Defeasible and Ampliative Reasoning (DARe), held in conjunction with LPNMR 2017 in Espoo, Finland, aims at bringing together researchers and practitioners from core areas of artificial intelligence, cognitive sciences, philosophy and related disciplines to discuss the defeasible and ampliative aspects of reasoning in a multi-disciplinary forum.

There are expressions of human cognition for which the development of logical formalisations is desirable but particularly problematic, since classical reasoning cannot be straightforwardly applied. Some typical examples are reasoning with uncertainty, exceptions, similarity, vagueness, incomplete or contradic-

tory information and many others. They often show two strongly intertwined aspects:

Ampliative aspect: the ability to make inferences that venture beyond the scope of the premises, in a somehow daring but justifiable way. The focus is on those forms of inference that, moving from true premises, allow the derivation of conclusions that are not necessarily true, but that we are somehow rationally justified in expecting to be true. Some examples are default, inductive and abductive reasoning.

Defeasible aspect: the ability to backtrack one's conclusions or to admit exceptions in reasoning. Some examples are retractive reasoning (e.g., belief contraction and negotiation) and preemptive reasoning (e.g., multiple inheritance networks and in regulatory systems).

The goal of DARe is to present latest research developments on the aforementioned aspects of reasoning, to discuss current directions in the field, and to collect first-hand feedback from the community. Among the foreseen outcomes is the emergence of a framework to relate canonical problems, tools and applications, filling an important gap in the convergence of logical, statistical and probabilistic approaches to defeasibility and ampliativeness in reasoning, as well as to get a better understanding of how to effectively implement these ideas.

Participating Members:

- Giovanni CASINI (Organising Committee)

Fourth InternationalWorkshop on Graphical Models for Security (GraMSec 2017)

Location: Santa Barbara, United States of America, 21 Aug 2017.

Participating Members:

- Sjouke MAUW (Chair)
- Olga GADYATSKAYA (Program Committee Member)

GCAI 2017

http://easychair.org/smart-program/GCAI2017/

Location: Miami, United States of America, 20 Oct 2017 – 22 Oct 2017.

Description: The 3rd Global Conference on Artificial Intelligence (GCAI 2017) will be held in Miami, USA, at the AC Marriott hotel on South Beach, 19-22 October 2017.

Participating Members:

- Christoph Ewald BENZMÜLLER (Programme Chair)

- Martin THEOBALD (Programme Chair)
- Xavier PARENT (Program Committee Member)

GECCO 2017 The Genetic and Evolutionary Computation Conference

http://gecco-2017.sigevo.org/index.html/HomePage

Location: Berlin, Germany, 15 Jul 2017 – 19 Jul 2017.

Description: The Genetic and Evolutionary Computation Conference (GECCO) presents the latest high-quality results in genetic and evolutionary computation since 1999. Topics include: genetic algorithms, genetic programming, ant colony optimization and swarm intelligence, complex systems (artificial life/robotics/evolvable hardware/generative and developmental systems/artificial immune systems), digital entertainment technologies and arts, evolutionary combinatorial optimization and metaheuristics, evolutionary machine learning, evolutionary multiobjective optimization, evolutionary numerical optimization, real world applications, search-based software engineering, theory and more.

Participating Members:

- Pascal BOUVRY (Technical Program Committee Member, Technical Program Committee Member)

Grande Region Security and Reliability Day 2017

Location: Luxembourg, Luxembourg, 9 Mar 2017.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

Grande Region Security and Reliability Day 2017 (GRSRD'17)

Location: Luxembourg, Luxembourg, 3 Sep 2017.

Participating Members:

- Jun PANG (Co-Chair)

Grande Region Security and Reliability Day (GRSRD 2017)

http://grsrd.uni.lu/2017/

Location: Luxembourg, Luxembourg, 9 Mar 2017.

Description: Security and reliability are interdisciplinary areas, drawing from several fields: mathematics (number theory, statistics, logic), computer science (algorithms, information theory, cryptology, formal methods, computational complexity, software engineering), electrical engineering (electronics, signal acquisition and processing, secure hardware design), management (security and quality policies, risk assessment) and social aspects (security awareness, ethical and legal issues, privacy). The objective of the Grande Region Security and Reliability Day (GRSRD) is to increase scientic interaction in security and reliability at the regional level. The workshop provides a platform for exchange of ideas, discussion and co-operation. It focuses on the Grande Region, but is open to submissions and participation of the whole scientic community working in security and reliability. This year, the GRSRD is jointly organized by University of Luxembourg, LORIA-INRIA Nancy, and Saarland University. More information can be found at http://grsrd.uni.lu/2017/.

Participating Members:

- Jun PANG (Co-Chair)

HPC School 2017 - Newcomer Training Day

https://hpc.uni.lu/hpc-school/2017/11/index.html

Location: Belval, Luxembourg, 9 Nov 2017.

Description: The UL HPC team, together with leading computational scientists of the UL and HPC technologists will offer instructions and **practical sessions** on a variety of topics, including:

- Access to and interaction with the UL HPC infrastructures
- HPC challenges, especially as regards data and storage management
- HPC workflow management (for sequential and parallel tasks)
- Prototyping with Python and Matlab in an HPC environment
- Parallel debugging, profiling and performance analysis

The aim is to cover basic and intermediate-level usage of the platform, Whether you have no HPC experience or are an advanced user looking to refresh and update your knowledge, don't miss this unique opportunity to learn more about the efficient usage of the system.

This sixth edition of the UL HPC School will take place on Thursday, November 9th, 2017, on the Belval campus, Location: MSA 3rd floor, rooms 3.070 and 3.100

Participating Members:

- Pascal BOUVRY (Chair)
- Sébastien VARRETTE (Chair, Keynote speaker)
- Clément PARISOT (Organising Committee)
- Valentin PLUGARU (Organising Committee)

HPC School 2017 - Summer School

https://hpc.uni.lu/hpc-school/2017/06/

Location: Belval, Luxembourg, 12 Jun 2017 – 13 Jun 2017.

Description: The UL HPC team, together with leading computational scientists of the UL and HPC technologists will offer instructions and **practical sessions** on a variety of topics, including:

- Access to and interaction with the UL HPC infrastructures
- HPC challenges, especially as regards data and storage management
- HPC workflow management (for sequential and parallel tasks)
- HPC Programming and Usage of the main software available on the platform (Matlab, R, MPI, physics, chemistry, bioinformatics, BigData tools) and services using the platform
- Software environment management
- Virtualization on the clusters

The aim is to cover basic as well as advanced usage of the platform. Whether you have no HPC experience or are an advanced user, don't miss this unique opportunity to learn more about the efficient usage of the system.

This fifth edition of the UL HPC School will take place on June 12th and 13th, 2017, on the Belval campus, Location: MSA 4th Floor, rooms 4.510 and 4.520

Participating Members:

- Pascal BOUVRY (Chair)
- Sébastien VARRETTE (Chair, Keynote speaker)
- Clément PARISOT (Organising Committee)
- Valentin PLUGARU (Organising Committee)

IAIT2017 The 9th International Conference on Advances in Information Technology

http://www.iait-conf.org/2017/index.html

Location: Bangkok, Thailand, 22 Nov 2017 – 25 Nov 2017.

Description: IAIT2017 In today's modern life, societies have to embrace digital technologies in their home (office) and use them to enhance the quality of life. The emerging of aging societies around the world prompts more urgent need for having more affordable and easy to set up "Smart Life Environment", as well as assisted technologies used inside a home with high performance and efficient solutions and platforms. Adoption of the Internet of Things technology such as smart tracking devices, smartphones, and other sensors in other smart devices, adds ubiquity and mobility to existing information systems and expands the

horizon of endless possibility in research and development.

The 9th International Conference on Advances in Information Technology (IAIT2017), with the theme "Impact of IoT and Big Data Analytics on Smart Life", will be held in Bangkok, Thailand, November 2017.

The reviewing process of the IAIT conference aims to provide authors with constructive feedback on their papers, even when a submission is rejected. All submissions will be subjected to double-blind peer reviews by at least three (3) reviewers, who are expert or have been experiencing in the related field for years. The accepted papers must be revised, taking into consideration the referees' comments and suggestions, before inclusion in the conference proceedings.

All accepted papers will be discoverable immediately upon the publication in: Google Scholar, Microsoft Academic Research, Crossref database, and Directory of Open Access Resources (part from ISSN organization) and will be considered for SCOPUS index journal.

Participating Members:

- Pascal BOUVRY (International Advisory Committee)

ICA3PP 2017

https://research.comnet.aalto.fi/ICA3PP2017/index.html

Location: Helsinki, Finland, 21 Aug 2017 – 23 Aug 2017.

Description: ICA3PP 2017 is the 17th in this series of conferences started in 1995 that are devoted to algorithms and architectures for parallel processing. ICA3PP is now recognized as the main regular event of the world that is covering the many dimensions of parallel algorithms and architectures, encompassing fundamental theoretical approaches, practical experimental projects, and commercial components and systems.

Participating Members:

- Pascal BOUVRY (Program Committee Member)
- Grégoire DANOY (Program Committee Member)
- Sébastien VARRETTE (Program Committee Member)

ICAC 2017 14th IEEE International Conference on Autonomic Computing

http://icac2017.ece.ohio-state.edu/

Location: Columbus, Ohio, United States of America, 17 Jul 2017 – 21 Jul 2017.

Description: ICAC is the leading conference on autonomic computing techniques, foundations, and applications. Large-scale systems of all types, such as data centers, computer clouds, smart cities, cyber-physical systems, sensor networks, and embedded or pervasive environments, are becoming increasingly complex and burdensome for people to manage. Autonomic computing systems reduce this burden by managing their own behavior in accordance with high-level goals. In autonomic systems, resources and applications are managed to maximize performance and minimize cost, while maintaining predictable and reliable behavior in the face of varying workloads, failures, and malicious threats. Achieving self-management requires and motivates research that spans a wide variety of scientific and engineering disciplines, including distributed systems, artificial intelligence, machine learning, modeling, control theory, optimization, planning, decision theory, user interface design, data management, software engineering, emergent behavior analysis, and bio-inspired computing. ICAC brings together researchers and practitioners from disparate disciplines, application domains and perspectives, enabling them to discover and share underlying commonalities in their approaches to making resources, applications and systems more autonomic.

Participating Members:

- Pascal BOUVRY (Technical Program Committee Member)

ICAIL 2017

https://nms.kcl.ac.uk/icail2017/

Location: London, United Kingdom, 12 Jun 2017 – 16 Jun 2017.

Description: The ICAIL conference is the primary international conference addressing research in Artificial Intelligence and Law, and has been organized biennially since 1987 under the auspices of the International Association for Artificial Intelligence and Law (IAAIL). ICAIL provides a forum for the presentation and discussion of the latest research results and practical applications; it fosters interdisciplinary and international collaboration. The conference proceedings are published by ACM.

Participating Members:

- Livio ROBALDO (Program Committee Member)
- Leon VAN DER TORRE (Program Committee Member)

ICCCT-2011 2nd International Conference on Computer and Communication Technology

http://www.mnnit.ac.in/iccct2017/index.html

Location: Allahabad, India, 24 Nov 2017 – 26 Nov 2017.

Description: The 7th ICCCT-17 is a major multidisciplinary conference organized with the objective of bringing together researchers, developers and practitioners from academia and industry working in all areas of computer and communication technology. It is being organised specifically to help computer industry to derive the advances of next generation computer and communication technology. Researchers invited to speak, will present the latest developments and technical solutions in the areas of Hardware & Software Design, Distributed & Parallel Processing, Advanced software Engineering, etc.

The sixth International Conference on Computer and Communication Technology, ICCCT-2015 has concluded well in the city of Allahabad, India. The ICCCT-2015 gained greatest attention when calling for papers and with your cooperation it already has become an excellent forum for the presentation of new advances and research results in the field of Computer Science and Engineering, Communication and associated fields. The ICCCT has become the premier place to bring together the leading researchers, engineers and scientists in the domain of interest from all around the world.

7th ICCCT-17 will be organized by Motilal Nehru National Institute of Technology Allahabad, Allahabad, India, in academic collaboration with SP Memorial Institute of Technology Kaushambi, Allahabad, India.

Participating Members:

- Pascal BOUVRY (Technical Program Committee Member)

ICUMT 2017

http://www.icumt.info/2017/

Location: Munich, Germany, 6 Nov 2017 – 8 Nov 2017.

Description: The 9th International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT) is an IEEE (R8 + Germany Section) technically co-sponsored (approved) premier international congress providing an open forum for researchers, engineers, network planners and service providers targeted on newly emerging technologies, systems, standards, services, and applications, bringing together leading international players in telecommunications, control systems, automation and robotics. The event is positioned as a major international annual congress for the presentation of original results

achieved from fundamental as well as applied research and engineering works.

Participating Members:

- Grégoire DANOY (Program Committee Member)

IDEA-2k17 International Conference on Data Engineering and Applications 2017

http://ideaconference.in/Commiittee.html

Location: Bhopal, India, 28 Oct 2017 – 29 Oct 2017.

Description: The 1st International Conference on Data, Engineering and Applications 2017 (IDEA-2k17) is being organized during October 28-29, 2017 in Bhopal (The city of Lakes), India. IDEA-2k17 is the premier forum for the presentation of new advances and research results in the fields of Big Data, Computational Intelligence, Data Mining, Machine Learning and their associated learning systems and applications.

The conference will bring together leading academician, scientists, expert from industry and researchers in the domain of interest from around the world. The conference will have pre-conference Tutorial presentations, Invited talks and Research paper and posters presentations. The invited talks and tutorials will be delivered by renowned experts.

Contributions from researchers describing their original, unpublished, research contribution which is not currently under review by another conference or journal and addressing state-of-the-art research are invited to share their work in all areas of Big Data, Computational Intelligence, Data Mining, Machine Learning and their associated learning systems and applications but not limited to the conference tracks.It is planned to publish the best and topmost selected papers of conference IDEA-2k17 as a post-conference proceedings with Springer in their prestigious Communications in Computer and Information Science series (final approval pending).

Participating Members:

- Pascal BOUVRY (Technical Program Committee Member)

IEA/AIE 2017

http://www.cril.univ-artois.fr/ieaaie2017/

Location: Arras, France, 27 Jun 2017 – 30 Jun 2017.

Description: The 30th International Conference on Industrial, Engineering,

Other Applications of Applied Intelligent Systems.

IEA/AIE 2017 continues the tradition of emphasizing applications of applied intelligent systems to solve real-life problems in all areas including engineering, science, industry, automation & robotics, business & finance, medicine and biomedicine, bioinformatics, cyberspace, and human-machine interactions.

Participating Members:

- Giovanni CASINI (Program Committee Member)

IEEE CEC 2017

Location: San Sebastian, Spain, 5 Jun 2017 – 8 Jun 2017.

Description: 2017 IEEE Congress on Evolutionary Computation (CEC)

Participating Members:

- Grégoire DANOY (Program Committee Member)

IEEE CLOUDCOM 2017

http://2017.cloudcom.org

Location: Hong Kong, Hong Kong, 11 Dec 2017 – 14 Dec 2017.

Description: CloudCom is the premier conference on Cloud Computing worldwide, attracting researchers, developers, users, students and practitioners from the fields of big data, systems architecture, services research, virtualization, security and privacy, high performance computing, always with an emphasis on how to build cloud computing platforms with real impact.

Participating Members:

- Grégoire DANOY (Track / Working Group Chair)
- Sébastien VARRETTE (Track / Working Group Chair)
- Valentin PLUGARU (Program Committee Member)

IEEE CLOUDTECH 2017

http://www.macc.ma/cloudtech17/index.html

Location: Rabat, Morocco, 24 Oct 2017 – 26 Oct 2017.

Description: Third International Conference of Cloud Computing Technologies and Applications. CloudTech'17 is the first conference on Cloud Computing

worldwide, attracting researchers, developers, users, students and practitioners from the fields of big data, systems architecture, services research, virtualization, security and privacy, high performance computing, always with an emphasis on how to build cloud computing platforms with real impact.

Participating Members:

- Grégoire DANOY (Program Committee Member)

IEEE Intelligent Transportation Systems Conference (ITSC)

http://www.itsc2017.org/

Location: Yokohama, Japan, 16 Oct 2017 – 19 Oct 2017.

Participating Members:

- Sébastien FAYE (Technical Program Committee Member)

IEEE PDCO 2017

https://pdco2017.sciencesconf.org

Location: Orlando, Florida, United States of America, 29 May 2017 – 2 Jun 2017.

Description: IEEE PDCO 2017, Orlando USA, is the result of the merge of the IEEE Parallel Computing and Optimization (PCO) workshop and the IEEE Nature Inspired Distributed Computing (NIDISC) workshop that have been held in conjunction with the IEEE International Parallel and Distributed Processing Symposium for the past years.

Participating Members:

- Grégoire DANOY (Co-Chair)
- Pascal BOUVRY (Steering Committee Member)

IEEE PICOM 2017

http://cse.stfx.ca/~picom2017/

Location: Orlando, United States of America, 6 Nov 2017 – 10 Nov 2017.

Description: PICom-2017 is the conference on Pervasive Intelligence and Computing, previously held as PCC (Las Vegas, USA, 2003 and 2004), PSC- (Las Vegas, USA, 2005), PCAC (Vienna, Austria, 2006, and Niagara Falls, Canada, 2007) ,

IPC-2007 (Jeju, Korea, December 2007), IPC-2008 (Sydney, Australia, December 2008), and since 2009 as PICom.

Participating Members:

- Grégoire DANOY (Program Committee Member)

IJCAI 2017

https://ijcai-17.org/index.html

Location: Melbourne, Australia, 19 Aug 2017 – 25 Aug 2017.

Description: IJCAI is the International Joint Conference on Artificial Intelligence, the main international gathering of researchers in AI. IJCAI were held biennially in odd-numbered years since 1969. Starting with 2016, IJCAI will be held annually. IJCAI is sponsored jointly by IJCAI and the national AI societie(s) of the host nation(s). The 26th International Joint Conference on Artificial Intelligence will be held in Melbourne, Australia in August 2017.

Participating Members:

- Giovanni CASINI (Program Committee Member)
- Marcos CRAMER (Program Committee Member)
- Leon VAN DER TORRE (Program Committee Member)
- Emil WEYDERT (Program Committee Member)

International Conference on Mathematical Methods, Models and Architectures for Computer Networks Security (MMM-ACNS 2017)

Location: Warsaw, Poland, 28 Aug 2017 – 30 Aug 2017.

Participating Members:

- Alfredo RIAL DURAN (PC Member)

International Conference on Mobile, Secure and Programmable Networking (MSPN 2017)

Location: Paris, France, 29 Jun 2017 – 30 Jun 2017.

Participating Members:

- Sjouke MAUW (Program Committee Member)

International Conference on Security for Information Technology and Communication (SecITC 2017)

Location: Bucharest, Romania, 8 Jun 2017 – 9 Jun 2017.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

International Workshop on Secure Internet of Things (SIoT)

Location: Oslo, Norway, 15 Sep 2017.

Participating Members:

- Alfredo RIAL DURAN (PC Member)

International Workshop on Software Engineering Curricula for Millennials (SECM 2017)

http://secm2017.se-edu.org/wp/index.php/call-for-contributions/

Location: Buenos Aires, Argentina, 27 May 2017.

Description: Educating the new breed of software engineering is tough. Millennials have been dominating the higher education programs for some time. This cohort has unique needs, learning styles, and skills. They are diverse, collaborative, creative, tech-savvy, and keenly interested in emerging technologies. They drive the growth of the software industry, which itself is in a constant state of flux, with new technologies, techniques, paradigms, and application domains popping up with increasing frequency. Companies quickly adjust to this shifting landscape while trying to cater to the needs of their new hires. What about educators? How should software engineering curricula and educators' teaching styles adapt to these changes? Perspectives of students, educators, and prospective employees should be heard. Our goal in this workshop is bring together the main stakeholders through a highly interactive format to discuss the demands and challenges of training future software engineers in higher education and professional settings.

Topics

Topics of interest include, but are not limited to:

- software engineering education for new and emerging technologies;
- novel approaches to designing software engineering curricula;
- needs and expectations of Millennials aspiring to be software engineers;
- skills and continuing education for software engineering educators;

- classroom formats that cater to diverse learning styles;
- teaching approaches that leverage technology-enhanced education in software engineering courses;
- balancing teaching of soft and hard skills
- balancing rigor and practicality;
- experience in educating the Millennials in a software engineering program;
- experience in being educated as a Millennial in a software engineering program;
- experiential and hands-on learning for software engineers;
- employees' needs and expectations of fresh software engineering graduates in a fast changing software landscape; and
- gaps and challenge in professional graduate software engineering programs.

Participating Members:

- Nicolas GUELFI (PC Member)

ISPA 2017

http://trust.gzhu.edu.cn/conference/ISPA2017/

Location: Guangzhou, China, 12 Dec 2017 – 15 Dec 2017.

Description: The IEEE ISPA 2017 (15th IEEE International Symposium on Parallel and Distributed Processing with Applications) is a forum for presenting leading work on parallel and distributed computing and networking, including architecture, compilers, runtime systems, applications, reliability, security, parallel programming models and much more. During the symposium, scientists and engineers in both academia and industry are invited to present their work on concurrent and parallel systems (multicore, multithreaded, heterogeneous, clustered systems, distributed systems, grids, clouds, and large scale machines).

Participating Members:

- Grégoire DANOY (Program Committee Member)

JURIX2017

https://jurix2017.gforge.uni.lu/

Location: Luxembourg, Luxembourg, 13 Dec 2017 – 15 Dec 2017.

Description: For 30 years, the JURIX conference has provided an international forum for research on the intersection of Law, Artificial Intelligence and Information Systems, under the auspices of The JURIX Foundation for Legal Knowledge Systems.

Participating Members:

- Livio ROBALDO (Program Committee Member)
- Leon VAN DER TORRE (Program Committee Member)
- Giovanni CASINI (Organizing Chair)
- Jérémie DAUPHIN (Organising Committee)
- Livio ROBALDO (Organising Committee)

LANET 2017 1st Latin American Conference on Complex Networks

http://www.lanetconference.org/

Location: Puebla, Mexico, 25 Sep 2017 – 29 Sep 2017.

Description: The aim of LANET is to provide with a forum to join all scientists who are somehow related to the research on Network Science in Latin America.

The rapid growth of the field of Network Science in the last two decades has manifested in the form of schools, workshops and conferences in Latin America. However, the creation of LANET as a stable and periodic forum devoted to Network Science will further spur the formation of research groups interested in the field and help to establish it as a discipline across Latin American Universities and Research Institutions.

The first edition will be organized by the Benemérita Universidad Autónoma de Puebla (Puebla, México) and, tentatively, we plan LANET to have a periodicity of two years with different locations in Latin America.

Participating Members:

- Pascal BOUVRY (Organising Committee)

MAMBA - Workshop on Smart Mobility

http://vehicularlab.uni.lu/workshop-smart-mobility/

Location: Luxembourg, Luxembourg, 1 Jun 2017 – 2 Jun 2017.

Description: SECAN-Lab organised a Workshop on Smart Mobility aimed at bringing together European actors from both industry and academia with shared interests in transportation and related topics. In addition to a series of talks from selected speakers, this single-session event also featured demos and poster sessions.

Participating Members:

- Thomas ENGEL (Organizing Chair)
- Sébastien FAYE (Organizing Chair)

MIREL @ ICAIL 2017

http://www.mirelproject.eu/MIRELws/

Location: London, United Kingdom, 16 Jun 2017.

Description: The aim of MIREL-2017 workshop is to bridge the gap between the community working on legal ontologies and NLP parsers and the community working on reasoning methods and formal logic, in line with the objectives of the MIREL (MIning and REasoning with Legal texts) project. The workshop aims at fostering the scientific discussion between approaches based on language technologies applied to the legal domain (representing legal knowledge) and those based on legal reasoning (using the legal knowledge to build specialized services and applications).

Participating Members:

- Livio ROBALDO (Chair)
- Giovanni CASINI (Program Committee Member)
- Xavier PARENT (Program Committee Member)
- Leon VAN DER TORRE (Program Committee Member)

MISTA 2017 Multidisciplinary International Scheduling Conference: Theory and Applications

http://www.schedulingconference.org/

Location: Kuala Lumpur, Malaysia, 5 Nov 2017 – 8 Jan 2018.

Description: This conference series serves as a forum for an international community of researchers, practitioners and vendors on all aspects of multidisciplinary scheduling. The aim is to bring together scheduling researchers and practitioners from all the disciplines that engage with scheduling research.

Participating Members:

- Pascal BOUVRY (Organising Committee)

Network and Distributed System Security Symposium 2017 (NDSS 2017)

http://www.ndss17.org/

Location: San Diego, United States of America, 26 Feb 2017 – 1 Mar 2017.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

Oresund Security Day 2017

Location: Copenhagen, Denmark, 30 May 2017.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

PDCO 2017 7th IEEE Workshop Parallel / Distributed Computing and Optimization

https://pdco2017.sciencesconf.org/

Location: Orlando, Florida, United States of America, 29 May 2017.

Description: The IEEE Workshop on Parallel / Distributed Computing and Optimization aims at providing a forum for scientific researchers and engineers on recent advances in the field of parallel or distributed computing for difficult optimization problems, ranging from theoretical to applied problems.

The latter include 0-1 multidimensional knapsack problems and cutting stock problems, large scale linear programming problems, nonlinear optimization problems and global optimization problems. Emphasis will be placed on new techniques for solving these difficult problems, like cooperative methods for integer programming problems, nature-inspired techniques and hybrid methods. Aspects related to Combinatorial Scientific Computing (CSC) will also be treated. We also solicit submissions of original manuscripts on sparse matrix computations and related topics (including graph algorithms); and related methods and tools for their efficiency on different parallel systems. The use of new approaches in parallel and distributed computing like GPU, MIC, cloud computing, volunteer computing will be considered. Applications combining traditional parallel and distributed computing and optimization techniques as well as theoretical issues (convergence, complexity, etc.) are welcome. Application domains of interest include (but are not limited to) cloud computing, planning, logistics, manufacturing, finance, telecommunications and computational biology.

Participating Members:

- Grégoire DANOY (Chair)
- Pascal BOUVRY (Steering Committee Member)
- Sébastien VARRETTE (Program Committee Member)

PNSE'17 International Workshop on Petri Nets and Software Engineering

https://www.informatik.uni-hamburg.de/TGI/events/pnse17

Location: Zaragoza, Spain, 26 Jun 2017 – 27 Jun 2017.

Participating Members:

- Nicolas GUELFI (PC Member)

PNSE'17 International Workshop on Petri Nets and Software Engineering

http://www.informatik.uni-hamburg.de/TGI/events/pnse17/#Scope

Location: Zaragoza, Spain, 26 Jun 2017 – 27 Jun 2017.

Description: For the successful realization of complex systems of interacting and reactive software and hardware components the use of a precise language at different stages of the development process is of crucial importance. Petri nets are becoming increasingly popular in this area, as they provide a uniform language supporting the tasks of modeling, validation, and verification. Their popularity is due to the fact that Petri nets capture fundamental aspects of causality, concurrency and choice in a natural and mathematically precise way without compromising readability.

The workshop PNSE'17 (Petri nets and Software Engineering) will take place as a satellite event of Petri Nets 2017 and ACSD 2017.

The use of Petri nets (P/T-nets, colored Petri nets and extensions) in the formal process of software engineering, covering modeling, validation, and verification, will be presented as well as their application and tools supporting the disciplines mentioned above.

Topics

We welcome contributions describing original research in topics related to Petri nets in combination with software engineering, addressing open problems or presenting new ideas regarding the relation of Petri nets and software engineering. Furthermore we look for surveys addressing open problems and new applications of Petri nets. Topics of interest include but are not limited to:

- Modeling
  - representation of formal models by intuitive modeling concepts
  - guidelines for the construction of system models

  - representative examples
  - process-, service-, state-, event-, object- and agent-oriented approaches
  - adaption, integration, and enhancement of concepts from other disciplines
  - views and abstractions of systems
  - model-driven architecture
  - modeling software landscapes
  - web service-based software development
- Validation and Execution
  - prototyping
  - simulation, observation, animation
  - code generation and execution
  - testing and debugging
  - efficient implementation
- Verification
  - structural methods (e.g. place invariants, reduction rules)
  - results for structural subclasses of nets
  - relations between structure and behavior
  - state space based approaches
  - efficient model checking
  - assertional and deductive methods (e.g. temporal logics)
  - process algebraic methods
  - applications of category theory and linear logic
- Application of Petri nets in Software Engineering, in particular the use of Petri nets in the domains of
  - flexible manufacturing,
  - logistics,
  - telecommunication,
  - big data,
  - cyper-physical systems,
  - internet-of-things,
  - cloud computing,
  - distributed systems,
  - workflow management and
  - embedded systems.
- Tools in the fields mentioned above

Participating Members:

- Nicolas GUELFI (PC Member)

PPAM 2017 12th International Conference on Parallel Processing and Applied Mathematic

https://www.ppam.pl/

Location: Lubin, Poland, 10 Sep 2017 – 13 Sep 2017.

Description: The PPAM 2017 conference, twelfth in a series, will cover topics in

parallel and distributed computing, including theory and applications, as well as applied mathematics. The focus will be on models, algorithms, and software tools which facilitate efficient and convenient utilization of modern parallel and distributed computing architectures, as well as on large-scale applications, including big data and machine learning problems.

PPAM is a biennial conference started in 1994, with the proceedings published by Springer in the Lecture Notes in Computer Sciences series. In 2017 the PPAM conference will take place in Lublin, the largest Polish city east of the Vistula River, an academic and cultural centre, proud of its rich history and picturesque Old Town.

The PPAM 2017 conference is organized by Czestochowa University of Technology together with Maria Curie-Skłodowska University (UMCS) in Lublin, under the patronage of Committee of Informatics of Polish Academy of Sciences, in technical cooperation with IEEE Computer Society and ICT COST Action IC1305 "Network for Sustainable Ultrascale Computing (NESUS)".

Topics of interest include, but are not limited to:

- Parallel/distributed architectures, enabling technologies
- Cluster and cloud computing
- Multi-core and many-core parallel computing, GPU computing
- Heterogeneous/hybrid computing and accelerators
- Parallel/distributed algorithms: numerical and non-numerical
- Scheduling, mapping, load balancing
- Performance analysis and prediction
- Performance issues on various types of parallel systems
- Autotuning: methods, tools, and applications
- Power and energy aspects of computation
- Parallel/distributed programming
- Tools and environments for parallel/distributed computing
- Security and dependability in parallel/distributed environments
- HPC numerical linear algebra
- HPC methods of solving differential equations
- Evolutionary computing, meta-heuristics and neural networks
- Machine learning and HPC
- HPC interval analysis
- Applied Computing in mechanics, material processing, biology and medicine, physics, chemistry, business, environmental modeling, etc.
- Applications of parallel/distributed computing
- Methods and tools for parallel solution of large-scale problems, including big data and machine learning applications
- Neuromorphic computing

Participating Members:

- Pascal BOUVRY (Program Committee Member, Organizing Chair)

PRIMA2017

https://prima2017.gforge.uni.lu/

Location: Nice, France, 29 Oct 2017 – 3 Nov 2017.

Description: Agent-based Computing addresses the challenges in managing distributed computing systems and networks through monitoring, communication, consensus-based decision-making and coordinated actuation. As a result, intelligent agents and multi-agent systems have demonstrated the capability to use intelligence, knowledge representation and reasoning, and other social metaphors like 'trust', 'game' and 'institution', not only to address real-world problems in a human-like way but also to transcend human performance. This has had a transformative impact in many application domains, particularly in e-commerce, and also in planning, logistics, manufacturing, robotics, decision support, transportation, entertainment, emergency relief & disaster management, and data mining & analytics.

Participating Members:

- Leon VAN DER TORRE (Chair)
- Jérémie DAUPHIN (Web Chair)

Privacy, Security and Trust (PST 2017)

Location: Calgary, Canada, 28 Aug 2017 – 30 Aug 2017.

Participating Members:

- Sjouke MAUW (Program Committee Member)

Proceedings on Privacy Enhancing Technologies (PoPETs)

Location: Minneapolis, United States of America, 18 Jul 2017 – 21 Jul 2017.

Participating Members:

- Alfredo RIAL DURAN (PC Member)

RSA Conference Cryptographers' Track 2017 (CT-RSA 2017)

https://www.rambus.com/ct-rsa-2017/

Location: San Francisco, United States of America, 14 Feb 2017 – 17 Feb 2017.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

RuleML+RR

http://2017.ruleml-rr.org/

Location: London, United Kingdom, 12 Jul 2017 – 15 Jul 2017.

Description: RuleML+RR 2017 is the leading international joint conference in the field of rule-based reasoning, and focuses on theoretical advances, novel technologies, as well as innovative applications concerning knowledge representation and reasoning with rules. Stemming from the synergy between the well-known premier RuleML and RR events, one of the main goals of this conference is to build bridges between academia and industry.

RuleML+RR 2017 aims to bring together rigorous researchers and inventive practitioners, interested in the foundations and applications of rules and reasoning in academia, industry, engineering, business, finance, healthcare and other application areas. It will provide a forum for stimulating cooperation and cross-fertilization between the many different communities focused on the research, development and applications of rule-based systems.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

SDN-NFV Track in SAC Symposium 2017, IEEE International Conference on Communication (ICC 2017)

http://icc2017.ieee-icc.org

Location: Paris, France, 21 May 2017 – 25 May 2017.

Description: SDN-NFV are still in the standardisation process with different stakeholders (SDOs, Fora's and Initiatives) not yet converging. The New IP Agency (NIA) is taking an industry approach by setting an interoperability platform for all Telecom, ISPs and vendors to peer-test and interoperate with each to create a defacto standard. In any case, this is a field still wide open for research and pilot testing work to open up its potential. There is need to exploit high levels of management and increased network agility in software-based deployment. This will impact all network architectures including IoT, Big data, Optical, Edge and Openstack-based cloud and future 5G networks by greatly easing service deployment and smoothening infrastructure management.

Participating Members:

- Latif LADID (Co-Chair)

- Ridha SOUA (Co-Chair)

SECM 2017 - First International Workshop on Software Engineering Curricula for Millennials

http://secm2017.se-edu.org

Location: Buenos Aires, Argentina, 27 May 2017.

Participating Members:

- Nicolas GUELFI (PC Member)

SECM 2017 - International Workshop on Software Engineering Curricula for Millennials

http://secm2017.se-edu.org/wp/index.php/call-for-contributions/

Location: Buenos Aires, Argentina, 27 May 2017.

Description: Educating the new breed of software engineering is tough. Millennials have been dominating the higher education programs for some time. This cohort has unique needs, learning styles, and skills. They are diverse, collaborative, creative, tech-savvy, and keenly interested in emerging technologies. They drive the growth of the software industry, which itself is in a constant state of flux, with new technologies, techniques, paradigms, and application domains popping up with increasing frequency. Companies quickly adjust to this shifting landscape while trying to cater to the needs of their new hires. What about educators? How should software engineering curricula and educators' teaching styles adapt to these changes? Perspectives of students, educators, and prospective employees should be heard. Our goal in this workshop is bring together the main stakeholders through a highly interactive format to discuss the demands and challenges of training future software engineers in higher education and professional settings.

Topics

Topics of interest include, but are not limited to:

- software engineering education for new and emerging technologies;
- novel approaches to designing software engineering curricula;
- needs and expectations of Millennials aspiring to be software engineers;
- skills and continuing education for software engineering educators;
- classroom formats that cater to diverse learning styles;

- teaching approaches that leverage technology-enhanced education in software engineering courses;
- balancing teaching of soft and hard skills
- balancing rigor and practicality;
- experience in educating the Millennials in a software engineering program;
- experience in being educated as a Millennial in a software engineering program;
- experiential and hands-on learning for software engineers;
- employees' needs and expectations of fresh software engineering graduates in a fast changing software landscape; and
- gaps and challenge in professional graduate software engineering programs.

Participating Members:

- Nicolas GUELFI (PC Member)

Second International Joint Conference on Electronic Voting (E-Vote-ID 2017)

Location: Bregenz, Austria, 24 Oct 2017 – 27 Oct 2017.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

SIGMOD Conference

http://sigmod2017.org

Location: Chicago, United States of America, 14 May 2017 – 19 Jan 2018.

Participating Members:

- Martin THEOBALD (Invited Speaker (Workshops))

Software Verication and Testing track at ACM Symposium on Applied Computing 2017 (SAC-SVT'17)

Location: Marrakech, Morocco, 27 Mar 2017 – 31 Mar 2017.

Participating Members:

- Jun PANG (Program Committee Member)

Special Session on Information Management in Human - Centric Systems (IMHCS'17) as an event of the 3 rd IEEE International Conference on Cybernetics (IEEE CYBCONF 2017)

http://cse.stfx.ca/~CybConf2017/

Location: Exeter, United Kingdom, 21 Jun 2017 – 23 Jun 2017.

Description: The Special Session on Information Management in Human - Centric Sys tems (IMHCS '17) is focused on discussing current trends in information acquisition, representation and processing in human - centric systems and applications. We particularly welcome contributions from researchers and practitioners presenting new results in the big area of information and data management with special attention paid to human - centric approaches .

Participating Members:

- Alfredo CAPOZUCCA (PC Member)
- Nicolas GUELFI (PC Member)

Summer School on Verication Technology, Systems & Applications (VTSA 2017)

http://resources.mpi-inf.mpg.de/departments/rg1/conferences/vtsa17/

Location: Saarbrucken, Germany, 31 Jul 2017 – 4 Aug 2017.

Description: The 10th summer school on verication technology, systems & applications takes place at the Max Planck Institute for Informatics at Saarbrücken, Germany from July 31st to August 4th, 2017. All three aspects verication technology, systems & applications strongly depend on each other and that progress in the area of formal analysis and verication can only be made if all three aspects are considered as a whole. Five speakers Rajeev Alur, Christel Baier, Hoon Hong, Andrew Reynolds and Thomas Wies stand for this view in that they represent and will present a particular verication technology and its implementation in a system in order to successfully apply the approach to real world verication problems. There were about 30 participants for the summer school. More information can be found at http://resources.mpi-inf.mpg.de/departments/rg1/conferences/vtsa17/.

Participating Members:

- Jun PANG (Organizing Chair)

TAFA 2017 @ IJCAI 2017

http://homepages.abdn.ac.uk/n.oren/pages/TAFA-17/index.html

Location: Melbourne, Australia, 19 Aug 2017 – 20 Aug 2017.

Description: Recent years have witnessed a rapid growth of interest in formal models of argumentation and their application in diverse sub-fields and domains of application of AI, including reasoning in the presence of inconsistency, non-monotonic reasoning, decision making, inter-agent communication, the semantic web, grid applications, ontologies, recommender systems, machine learning, neural networks, trust computing, normative systems, social choice theory, judgement aggregation and game theory, and law and medicine. Argumentation thus shows great promise as a theoretically-grounded tool for a wide range of applications.

This workshop aims at contributing to the realisation of this promise, by promoting and fostering uptake of argumentation as a viable AI paradigm with wide ranging application, and providing a forum for further development of ideas and the initiation of new and innovative collaborations. We therefore invite submission of papers on formal theoretical models of argumentation and application of such models in (sub-fields of) AI; evaluation of models, both theoretical (in terms of formal properties of existing or new formal models) and practical (in concretely developed applications); theories and applications developed through inter-disciplinary collaborations.

The workshop will solicit papers dealing with, but not limited to, the following topics:

- Properties of formal models of argumentation
- Instantiations of abstract argumentation frameworks
- Relationships amongst different argumentation frameworks
- Practical applications of formal models of argumentation
- Argumentation and other Artificial Intelligence techniques
- Evaluation of formal models of argumentation
- Validation and evaluation of applications of argumentation

This year, TAFA-17 also includes a system track in order to provide a forum for presenting and discussing argumentation solvers, algorithms, implementation details and empirical evaluations. The track is particularly suited for, but not limited to, ICCMA participants. Submissions for the system track should not be longer than 5 pages.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

The 10th International Conference on Network and System Security (NSS 2017)

Location: Helsinki, Finland, 21 Aug 2017 – 23 Aug 2017.

Participating Members:

- Zhe LIU (Track / Working Group Chair)

The 11th International Conference on Provable Security (ProvSec 2017)

Location: Xi'an, China, 23 Oct 2017 – 25 Oct 2017.

Participating Members:

- Vincenzo IOVINO (Program Committee Member)
- Zhe LIU (PC Member)

The 13th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2017)

Location: Niagara Falls, Canada, 22 Oct 2017 – 25 Oct 2017.

Participating Members:

- Zhe LIU (PC Member)

The 13th International Conference on Information Security Practice and Experience. (ISPEC 2017)

Location: Melbourne, Australia, 13 Dec 2017 – 15 Dec 2017.

Participating Members:

- Zhe LIU (PC Member)

The 15th IEEE conference on Pervasive Intelligence and Computing (PICom 2017)

Location: Orlando, United States of America, 6 Nov 2017 – 10 Nov 2017.

Participating Members:

- Zhe LIU (PC Member)

The 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2017)

Location: Sydney, Australia, 1 Aug 2017 – 4 Aug 2017.

Participating Members:

- Zhe LIU (PC Member)

The 16th International Conference on Cryptology And Network Security (CANS 2017)

Location: Hong Kong, Hong Kong, 29 Nov 2017 – 2 Dec 2017.

Participating Members:

- Zhe LIU (PC Member)

The 20th Annual International Conference on Information Security and Cryptology (ICISC 2017)

Location: Seoul, South Korea, 29 Nov 2017 – 1 Dec 2017.

Participating Members:

- Zhe LIU (PC Member)

The 20th International Symposium on Wireless Personal Multimedia Communications

http://wpmc2017.org/

Location: Yogakarta, Indonesia, 17 Dec 2017 – 20 Dec 2017.

Description: This event provides us good opportunities to exchange knowledge and information on the latest researches, strengthening relationships amongst us, as well as a perfect time to enjoy the relaxing yet entertaining environment of Yogyakarta.

Inaugurated in 1998, WPMC has been established as a global platform for mutual cooperation and discussions in the field of wireless multimedia communications. Held in Asia, Europe and America, WPMC has established itself as a unique global conference dedicated to wireless multimedia convergence. Continuing the series, the 20th WPMC is now, for the first time, held in Indonesia, where it was planned to be held in Bali, but due to some concern of volcano activity, it is moved to Yogyakarta.

Various advance technologies in the wireless multimedia communication field,

started to put the intelligences in many segments and subsystems of a communication system. Novel methodologies and approaches are introduced to achieve higher level of communication quality of service. Nevertheless, human life and quality of experience is still a very important aspect to be considered in each development of technologies, including communication technology.

We have also witnessed the rise of broad smart digital technologies on the devices, sensors, networks, controls and not to mentions millions of applications. Those smart technologies spun from computing, broadcasting and media, platforms, applications and contents, big data & data-mining, advertising and social media.

Accordingly, under the theme of "Interconnecting Wireless Personal Multimedia Communications", WPMC 2017 will provide good opportunity for us to discuss these advancements.

In this WPMC-2017, the event is locally organized by IEEE Communication Society Indonesia Chapter, and Telkom University, and we are more than happy to support the NICT, YRP and WPMC Steering Committees members.

Participating Members:

- Pascal BOUVRY (Organising Committee)

The 3rd International Workshop on Cyber Security

Location: Wuhan, China, 2 May 2017 – 4 May 2017.

Participating Members:

- Zhe LIU (Keynote speaker)

The 9th International Congress on Ultra Modern Telecommunications and Control Systems

http://www.icumt.info/2017/

Location: Munich, Germany, 6 Nov 2017 – 8 Nov 2017.

Description: ICUMT is an IEEE (R8 + Germany Section) technically co-sponsored (approved) premier international congress providing an open forum for researchers, engineers, network planners and service providers targeted on newly emerging technologies, systems, standards, services, and applications, bringing together leading international players in telecommunications, control systems, automation and robotics. The event is positioned as a major international annual congress for the presentation of original results achieved from fundamental as well as applied research and engineering works.

Following the success of the previous events normally attracting around 120 participants from both academia and industry, ICUMT 2017 is planned as a three-

day event offering a number of plenary sessions, technical sessions, and specialized workshops.

We look forward to seeing you in beautiful city of Munich – rapidly expanding centre of advanced technologies, art, culture, finance, innovations, education, business, and tourism in Germany and Europe!

Participating Members:

- Grégoire DANOY (Technical Program Committee Member)
- Pascal BOUVRY (Organising Committee)

The Fourth International Workshop on Graphical Models for Security (GraMSec 2017)

http://www.gramsec.uni.lu/2017/

Location: Santa Barbara, United States of America, 21 Aug 2017.

Description: Graphical security models provide an intuitive but systematic methodology to analyze security weaknesses of systems and to evaluate potential protection measures. Formal methods and computer security researchers, as well as security professionals from industry and government, have proposed various graphical security modeling schemes. Such models are used to capture different security facets (digital, physical, and social) and address a range of challenges including security assessment, risk analysis, automated defensing, secure services composition, policy validation and verification. The objective of GraMSec is to contribute to the development of well-founded graphical security models, efficient algorithms for their analysis, as well as methodologies for their practical usage.

Participating Members:

- Sjouke MAUW (Chair)

Theory of Quantum Computation, Communication and Cryptography

Location: Paris, France, 14 Jun 2017 – 16 Jun 2017.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

Twenty-fifth International Workshop on Security Protocols

Location: Cambridge, United Kingdom, 20 Mar 2017 – 22 Mar 2017.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

Very Large Databases (VLDB)

http://www.vldb.org/2017/

Location: Munich, Germany, 28 Aug 2017 – 1 Sep 2017.

Participating Members:

- Martin THEOBALD (Short Papers, Posters, and Demo Co-Chair)

Workshop on Formal Methods in Systems Biology (FMSB 2017)

http://satoss.uni.lu/fmsb/

Location: Belval, Luxembourg, 21 Nov 2017.

Description: This workshop aims at sharing the research experiences in the interdisciplinary fields of formal methods and systems biology. We invite researchers from University of Twente, bo Akademi University, and University of Luxembourg to present their work in these fields.

Participating Members:

- Qixia YUAN (Organising Committee)

Workshop Universtiy of Luxembourg / University of Paderborn

Location: Luxembourg, Luxembourg, 13 Feb 2017.

Participating Members:

- Thomas ENGEL (Organizing Chair)
- Sébastien FAYE (Organizing Chair)

WTMC 2017 International Workshop on Traffic Measurements for Cybersecurity

http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=58149&copyownerid=4495

Location: San Jose, CA, United States of America, 25 May 2017.

Description: Current communication networks are increasingly becoming pervasive, complex, and ever-evolving due to factors like enormous growth in the number of network users, continuous appearance of network applications, increasing amount of data transferred, and diversity of user behaviors. Understanding and measuring traffic in such networks is a difficult yet vital task for network management but recently also for cybersecurity purposes. Network traffic measuring and monitoring can, for example, enable the analysis of the spreading of malicious software and its capabilities or can help to understand the nature of various network threats including those that exploit users' behavior and other user's sensitive information. On the other hand network traffic investigation can also help to assess the effectiveness of the existing countermeasures or contribute to building new, better ones. Recently, traffic measurements have been utilized in the area of economics of cybersecurity e.g. to assess ISP "badness" or to estimate the revenue of cyber criminals.

The aim of this workshop is to bring together the research accomplishments provided by the researchers from academia and the industry. The other goal is to show the latest research results in the field of cybersecurity and understand how traffic measurements can influence it. We encourage prospective authors to submit related distinguished research papers on the subject of both: theoretical approaches and practical case reviews. This workshop presents some of the most relevant ongoing research in cybersecurity seen from the traffic measurements perspective.

The workshop will be accessible to both non-experts interested in learning about this area and experts interesting in hearing about new research and approaches.

Topics of interest include, but are not limited to:

- Measurements for network incidents response, investigation and evidence handling
- Measurements for network anomalies detection
- Measurements for economics of cybersecurity
- Network traffic analysis to discover the nature and evolution of the cybersecurity threats
- Measurements for assessing the effectiveness of the threats detection/prevention methods and countermeasures
- Novel passive, active and hybrid measurements techniques for cybersecurity purposes
- Traffic classification and topology discovery tools for monitoring the evolving status of the network from the cybersecurity perspective
- Correlation of measurements across multiple layers, protocols or networks for cybersecurity purposes
- Novel visualization approaches to detect network attacks and other threats
- Analysis of network traffic to provide new insights about network structure and behavior from the security perspective
- Measurements of network protocol and applications behavior and its impact on cybersecurity and users' privacy
- Measurements related to network security and privacy

Participating Members:

- Pascal BOUVRY (Technical Program Committee Member)

C.2 Doctoral Thesis Defense Committee Memberships

Javed Ahmed, University of Bologna

Date: 29 Sep 2017
Location: Bologna, Italy

PhD Defense Jury Members:

- Leon VAN DER TORRE (Supervisor)

Diego Agustin Ambrossio, University of Luxembourg

Date: 4 May 2017
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Sjouke MAUW (Chairman)
- Leon VAN DER TORRE (Supervisor)
- Marcos CRAMER (Member)

PhD Defense Jury External Partners:

- Marc Denecker (Vice-chairman)
- Christian Strasser (Member)

Eniafe Festus Ayetiran, University of Bologna

Date: 31 Jan 2017
Location: Bologna, Italy

PhD Defense Jury Members:

- Leon VAN DER TORRE (Co-supervisor)

Benjamin Behringer, University of Luxembourg

Date: 21 Jul 2017
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Denis ZAMPUNIERIS (Chairman)
- Steffen ROTHKUGEL (Supervisor)

PhD Defense Jury External Partners:

- Thorsten Berger (Member)

- Martina Lehser (Vice-chairman)
- Ina Schäfer (Member)

Walter Bronzi, University of Luxembourg

Date: 13 Oct 2017
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Thomas ENGEL (Supervisor)

PhD Defense Jury External Partners:

- Jérôme Härri (Vice-chairman)

PhD Advisory Board Members:

- Raphaël FRANK (Member)

PhD Advisory Board External Partners:

- Thomas Scherer (Member)

Jean-Thomas Camino, LAAS-CNRS

Date: 22 Jun 2017
Location: Toulouse, France

PhD Defense Jury Members:

- Grégoire DANOY (Member)

Massimo Chenal, University of Luxembourg

Date: 23 Jan 2017
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Jean-Sébastien CORON (Chairman)
- Peter Y. A. RYAN (Supervisor)

Samuel Cremer, University of Mons

Date: 18 Dec 2017
Location: Mons, Belgium

PhD Defense Jury Members:

- Pascal BOUVRY (Examiner)
- Pascal BOUVRY (Examiner)

PhD Advisory Board Members:

- Pascal BOUVRY (Examiner)

Denis DARQUENNES, Université de Namur

Date: 7 Dec 2017
Location: Namur, Belgium

PhD Defense Jury Members:

- Denis ZAMPUNIERIS (Invited member)

Afonso Delerue Arriaga, University of Luxembourg

Date: 17 Jan 2017
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Jean-Sébastien CORON (Chairman)
- Peter Y. A. RYAN (Supervisor)

PhD Defense Jury External Partners:

- David Naccache (Member)

Bilel Derbel, University of Lille

Date: 11 Dec 2017
Location: Lille, France

PhD Defense Jury Members:

- Pascal BOUVRY (Examiner)

PhD Advisory Board Members:

- Pascal BOUVRY (Examiner)

Dumitru-Daniel Dinu, University of Luxembourg

Date: 29 Nov 2017
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Volker MÜLLER (Chairman)
- Peter Y. A. RYAN (Vice-chairman)
- Alexei BIRYUKOV (Supervisor)

PhD Defense Jury External Partners:

- Benedikt Gierlichs (Member)
- Daniel Page (Member)

Loïc Gammaitoni, University of Luxembourg

Date: 16 Oct 2017
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Ulrich SORGER (Chairman)
- Nicolas NAVET (Vice-chairman)
- Pierre KELSEN (Supervisor)

PhD Defense Jury External Partners:

- Benoît Combemale (Member)
- Alcinho Cunha (Member)

Brau Guillaume, University of Luxembourg

Date: 13 Mar 2017
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Pierre KELSEN (Chairman)
- Nicolas NAVET (Supervisor)

PhD Defense Jury External Partners:

- Pierre de Saqui-Sannes (Vice-chairman)
- Grolleau Emmanuel (Examiner)
- Jérôme Hugues (Co-supervisor)
- Frank Singhoff (Examiner)

Meng Guozhu, Nanyang Technological University

Date: 15 May 2017
Location: Singapore, Singapore

PhD Defense Jury Members:

- Sjouke MAUW (Examiner)

Sairam Gurajada, Max Planck Institute Informatics

Date: 6 Feb 2017
Location: Saarbruecken, Germany

PhD Defense Jury Members:

- Martin THEOBALD (Co-supervisor)

Sabbir Hasan, INSA de Rennes

Date: 3 May 2017
Location: Rennes, France

PhD Defense Jury Members:

- Pascal BOUVRY (Examiner)
- Pascal BOUVRY (Examiner)

PhD Advisory Board Members:

- Pascal BOUVRY (Examiner)

Santiago Iturriaga, Universidad de la Republica

Date: 21 Sep 2017
Location: Montevideo, Uruguay

PhD Defense Jury Members:

- Grégoire DANOY (Examiner)
- Pascal BOUVRY (Member)

Sven Kiljan, Open University of the Netherlands

Date: 15 Jul 2017
Location: Heerlen, Netherlands

PhD Defense Jury Members:

- Sjouke MAUW (Member)

Yunbo Li, University of Rennes

Date: 12 Jun 2017
Location: Rennes, France

PhD Defense Jury Members:

- Pascal BOUVRY (Examiner)
- Pascal BOUVRY (Examiner)

PhD Advisory Board Members:

- Pascal BOUVRY (Examiner)

Alessandra Malerba, University of Bologna

Date: 26 Jun 2017
Location: Bologna, Italy

PhD Defense Jury Members:

- Leon VAN DER TORRE (Co-supervisor)

Robert Muthuri, University of Bologna

Date: 29 Sep 2017
Location: Bologna, Italy

PhD Defense Jury Members:

- Leon VAN DER TORRE (Co-supervisor)

Dat Ba Nguyen, Max Planck Institute Informatics

Date: 1 Dec 2017
Location: Saarbruecken, Germany

PhD Defense Jury Members:

- Martin THEOBALD (Co-supervisor)

Léo Perrin, University of Luxembourg

Date: 25 Apr 2017
Location: Belval, Luxembourg

PhD Defense Jury Members:

- Jean-Sébastien CORON (Chairman)
- Volker MÜLLER (Vice-chairman)

PhD Defense Jury External Partners:

- Henri Gilbert (Member)
- Gregor Leander (Member)

PhD Advisory Board Members:

- Alexei BIRYUKOV (Supervisor)

George Plataniotis, Radboud University

Date: 4 Apr 2017
Location: Nijmegen, Netherlands

PhD Defense Jury Members:

- Qin MA (Co-supervisor)

Sylwia Polberg, Technische Universität Wien

Date: 17 Aug 2017
Location: Vienna, Austria

PhD Defense Jury Members:

- Leon VAN DER TORRE (Member)

Martin Riener, TU Wien

Date: 20 Jul 2017
Location: Vienna, Austria

PhD Defense Jury Members:

- Christoph Ewald BENZMÜLLER (Member)

Marjan Skrobot, University of Luxembourg

Date: 13 Jan 2017
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Sjouke MAUW (Chairman)
- Peter Y. A. RYAN (Supervisor)

Cristiana Teixeira Santos, Universitat de Barcelona

Date: 30 Jan 2017
Location: Barcelona, Spain

PhD Defense Jury Members:

- Leon VAN DER TORRE (Co-supervisor)

Shane Tuohy, National University of Ireland Galway.

Date: 31 Jan 2017
Location: Galway, Ireland

PhD Defense Jury Members:

- Nicolas NAVET (Examiner)

Marc van Zee, University of Luxembourg

Date: 6 Apr 2017
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Pierre KELSEN (Chairman)
- Leon VAN DER TORRE (Supervisor)

PhD Defense Jury External Partners:

- Farhad Arbab (Member)
- Dragan Doder (Expert)
- Andreas Herzig (Member)
- Erik Proper (Expert)
- Wiebe van der Hoek (Vice-chairman)

Jiali Wang, University of Luxembourg, Life Science Department

Date: 23 Feb 2017
Location: Belval, Luxembourg

PhD Defense Jury Members:

- Christoph SCHOMMER (Co-supervisor)

Qixia Yuan, University of Luxembourg

Date: 29 Nov 2017
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Jun PANG (Vice-chairman)
- Sjouke MAUW (Supervisor)

PhD Defense Jury External Partners:

- Ion Petre (Member)
- Jaco van de Pol (Member)

C.3 Awards

Best paper, 20 Jul 2017

Recipients: François FOUQUET, Thomas HARTMANN, Yves LE TRAON, Assaad MOAWAD

Paper title: The next evolution of MDE: a seamless integration of machine learning into domain modeling, 2017 ACM/IEEE 20th International Conference on

Model Driven Engineering Languages and Systems (MODELS) (2017)

Best paper award at IEEE CybConf 2017, 23 Jun 2017

Recipients: Pascal BOUVRY, Matthias BRUST, Grégoire DANOY

Matthias R. Brust, Grégoire Danoy and Pascal Bouvry received a best paper award at the 3rd IEEE International Conference on Cybernetics (CYBCONF) for their article "Target Tracking Optimization of UAV Swarms Based on Dual-Pheromone Clustering". This work is also co-authored with three students from the MICS since it is based on their project from the Optmization for Computer Science lecture given by Prof. Bouvry and Dr. Danoy.

Best Paper Award Honorable Mention at SETTA 2017, 14 Oct 2017

Recipients: Andrzej MIZERA, Jun PANG, Qixia YUAN

Mizera A., Pang J., Qu H., Yuan Q. A New Decomposition Method for Attractor Detection in Large Synchronous Boolean Networks. In: Larsen K., Sokolsky O., Wang J. (eds) Dependable Software Engineering. Theories, Tools, and Applications. SETTA 2017. Lecture Notes in Computer Science, vol 10606. Springer, Cham.

Best Poster Award, 20 May 2017

Recipients: Qixia YUAN

Mizera A., Pang J., Qu H., Yuan Q. ASSA-PBN: A Toolbox for Probabilistic Boolean Networks. Bridging the GAP, the rst student research fair at University of Luxembourg

Foundation ISAE-SUPAERO Phd Award, 2 Dec 2017

Recipients: Guillaume BRAU

Guillaume Brau received the best Phd Award 2017 for Doctoral Schools: Computer Science, Mathematics and Telecommunication from ISAE-SUPAERO foundation (Toulouse, France). The thesis entitled "Modelling and analysis of non-functional properties in MDE for critical systems" was supervised by Nicolas Navet (CSC/Lassy) and Jérôme Hugues (ISAE).

Teaching Award, 12 Oct 2017

Recipients: Pierre KELSEN

Traditionally marking the start of the academic year, the "Séance de la Rentrée académique" introduced on Thursday 12 October its new concept: the "Teaching Awards" and the "Student Initiative Awards", rewarding respectively two university teachers from each faculty, as well as students whose commitment stands out. At the Faculty of Science, Technology and Communication (FSTC), Prof. Pierre Kelsen (Computer Science) and Dr. Alexandre Salsmann (Biology) were awarded with the 2017 University of Luxembourg Teaching Award for the outstanding quality of their teaching. The award-winners were chosen by the

students in a popular vote with the trophies handed out during the “Rentrée académique” ceremony.

C.4 Media Appearances

Smart ICT for Business Innovation (Paperjam Plus - ICT)

Article (Internet), 8 Dec 2017 4:06 p.m.
Members: Pascal BOUVRY

http://paperjam.lu/

Automation of Gödel’s Proof of God’s Existence (Decision Management Community)

Blog (Internet), 18 Nov 2017
Members: Christoph Ewald BENZMÜLLER

https://dmcommunity.org/2017/11/18/automation-of-godels-proof-of-gods-existence/

“*Two scientists have formalized a theorem regarding the existence of God penned by renowned Austrian mathematician Kurt Gödel. Using an ordinary MacBook computer, they have shown that Gödel’s proof was correct — at least on a mathematical level.*” You can read more in this article. It is interesting that one of them, Prof. Christoph Benzmüller, is the chair of the Luxembourg Logic for AI Summit that will include DecisionCAMP 2018.

KLOERTEXT - ADRESSENVIELFALT IM NETZ (LËTZEBUERGER Journal)

Article (Magazine), 18 Nov 2017
Members: Thomas ENGEL, Latif LADID

Moxa NPort Devices Vulnerable to Remote Attacks (Security Week)

Article (Internet), 17 Nov 2017
Members: Florian ADAMSKY, Thomas ENGEL

http://www.securityweek.com/moxa-nport-devices-vulnerable-remote-attacks

Berechnende Mathematik (Berliner Mathematische Gesellschaft)

Interview (TV), 9 Nov 2017
Members: Christoph Ewald BENZMÜLLER

http://www.math.berlin/veranstaltungen/dokumente/BMG-Tag2017_Ankuendigungsposter.pdf

Die Berliner Mathematische Gesellschaft lädt zum 3. BMG-Tag ein, bei dem die Grenzen der mathematischen Berechnungen anhand neuester Resultate aus der Logik ausgereizt sowie unter künstlerischer Sicht aus ganz andersARTiger Perspektive betrachtet werden. Eingeladen sind alle, die sich für Mathematik interessieren.

Automobility: Where research & development will make history (HAPPEN MAGAZINE)

Interview (Magazine), 8 Nov 2017 , issue 20, p. 042-043
Members: Thomas ENGEL

RTL Journal (RTL.lu)

Interview (TV), 8 Nov 2017 7:30 p.m.
Members: Pierre KELSEN

http://tele.rtl.lu/emissiounen/de-journal/3108069.html

Within the context of the student fair interview with Professor Pierre Kelsen regarding prospects of computer science graduates in Luxembourg. It is also mentioned that the interviewee is a recent recipient of a teaching award.

Wéi géint de Stau op eise Stroosse virgoen? (RTL.lu)

Interview (Radio), 24 Oct 2017 8:40 a.m.
Members: Thomas ENGEL

http://radio.rtl.lu/emissiounen/reportage/2058739.html

Wir sehen uns in der Schule (Die Welt)

Article (Internet), 18 Sep 2017
Members: Christoph Ewald BENZMÜLLER

https://www.welt.de/print/welt_kompakt/webwelt/article168734451/Wir-sehen-uns-in-der-Schule.html

Roboter werden bald als Lehrer eingesetzt, davon sind Experten überzeugt. Nur was das für die Schüler und Lehrer bedeutet, ist eine Frage, über die dringend diskutiert werden müsste

FNR Spotlight on Young Researchers: Zhe Liu (Luxembourg National Research Fund)

Interview (Internet), 17 Aug 2017
Members: Zhe LIU

https://www.fnr.lu/research-with-impact-fnr-highlight/spotlight-on-young-researchers-zhe-liu/

https://www.fnr.lu/research-with-impact-fnr-highlight/spotlight-on-young-researchers-zhe-liu/

Schlüssellose Autos sollen sicherer werden (SR.de)

Article (Internet), 8 Jul 2017 11:12 a.m.
Members: Florian ADAMSKY, Thomas ENGEL

http://www.sr.de/sr/home/nachrichten/panorama/sichere_austoschluessel_luxemburg100.html

Honda und Uni Luxemburg arbeiten am sicheren Fahrzeugschlüssel (Springer Professional)

Article (Internet), 7 Jul 2017
Members: Florian ADAMSKY, Thomas ENGEL

https://www.springerprofessional.de/automobilelektronik---software/verschluesselung/honda-und-uni-luxemburg-arbeiten-am-sicheren-fahrzeugschluessel/13287344

Luxembourg Uni Researchers Join Honda to Overcome Car Key Fob Attacks (Info Security)

Article (Internet), 7 Jul 2017
Members: Florian ADAMSKY, Thomas ENGEL

https://www.infosecurity-magazine.com/news/luxembourg-uni-boffins-join-honda/

Uni and Honda in ICT security collaboration (DELANO)
Article (Internet), 7 Jul 2017
Members: Florian ADAMSKY, Thomas ENGEL

http://delano.lu/d/detail/news/uni-and-honda-ict-security-collaboration/150500

Luxembourg researchers work on solution to car theft through remote starters (Luxembourg Times)
Article (Internet), 7 Jul 2017
Members: Florian ADAMSKY, Thomas ENGEL

https://luxtimes.lu/archives/1735-luxembourg-researchers-work-on-solution-to-car-theft-through-remote-starters

L'Uni collabore avec Honda sur les clés «sans contact» (Paperjam.lu)
Article (Internet), 7 Jul 2017 6:47 a.m.
Members: Florian ADAMSKY, Thomas ENGEL

http://paperjam.lu/news/luni-collabore-avec-honda-sur-les-cles-sans-contact

Honda invests in car key security research with SnT (Digital Luxembourg)
Article (Internet), 6 Jul 2017
Members: Florian ADAMSKY, Thomas ENGEL

http://www.digital-luxembourg.public.lu/en/actualites/innovation/2017/20170706_uni-honda/index.html

Honda invests in car key security research (EurekAlert!)
Article (Internet), 6 Jul 2017
Members: Florian ADAMSKY, Thomas ENGEL

https://www.eurekalert.org/pub_releases/2017-07/uol-hii070617.php

Wéi performant wäert dëse sinn? (RTL TV station)

Interview (TV), 5 Jul 2017 4:02 p.m.
Members: Pascal BOUVRY

http://www.rtl.lu/lifestyle/tech-world/1053704.html

Zu Lëtzebuerg gëtt et schonn eng Partie esou "High Performance"-Computeren. Ma de Grand-Duché kritt elo säin éischte nationale Superrechner!

Virreider a neien Technologien sinn d'USA. Déi gréissten a performantste Computeren huet d'NASA. Ënnert anerem déi impressionant Animatioune vum Weltall entstinn an de Recherchezentren vun der Weltraumagence. Et si riseg Datebase mat Millioune vun Informatiounen. Haut si Saache méiglech déi ee sech fréier net konnt virstellen.

Lëtzebuerg kritt also elo 2018 ee nationale Supercomputer, dee net grad esou performant ass wéi dee vun der NASA. De Lëtzebuerger HPC kann an der Sekonn eng Billard Rechenoperatioune maachen. Dat ass eng 1 mat 15 Nullen. Ee Supercomputer ass am Prinzip eng Zesummeschaltung vu lauter eenzele Computeren, fir esou eng ganz performant Maschinn ze kréien. Koordinéiert gëtt de Projet vun der Universitéit um Belval, hei gëtt et een Zenter fir HPC'en.

HotspotID - crowdsourced WiFi security project (100komma7.lu)

Interview (Radio), 2 Jun 2017 9:15 a.m.
Members: Thomas ENGEL

https://www.100komma7.lu/program/episode/169765/201710132220-201710132230

Roboterethik: Die Maschinen werden autonom (Deutschlandfunk)

Article (Internet), 10 May 2017
Members: Christoph Ewald BENZMÜLLER

http://www.deutschlandfunk.de/roboterethik-die-maschinen-werden-autonom.724.de.html?dram:article_id=385826

Die EU hat das weltweit teuerste zivile Förderprogramm für die Entwicklung von Robotern auf den Weg gebracht. Doch was Roboter können sollen und ob

es ethische Grenzen ihrer Aufgaben geben muss, dazu gibt es in Europa bislang keine Regeln.

Robotorethik: Die Maschinen werden autonom (Deutschlandfunk)

Interview (Radio), 10 May 2017
Members: Christoph Ewald BENZMÜLLER

http://www.deutschlandfunk.de/roboterethik-die-maschinen-werden-autonom.724.de.html?dram:article_id=385826

How to Mange your own Cloud (Delano)

Article (Internet), 20 Apr 2017 4:14 p.m.
Members: Pascal BOUVRY

http://Delano.lu

Firwat brauch Lëtzebuerg en ultra-performante Computer? (RTL TV station)

Interview (TV), 8 Apr 2017 3:55 p.m.
Members: Pascal BOUVRY

http://www.rtl.lu/letzebuerg/1023471.html

Firwat brauch Lëtzebuerg en ultra-performante Computer?

An enger digitaliséierter Welt ginn all Sekonn Milliarde vun Informatioune gesammelt. Fir dës Quantitéiten un Donnéeë séier kënnen ze verschaffen, brauch een déi sougenannt Super-Computeren.

Smart ICT for Business Innovation (Paperjam Plus - ICT)

Article (Magazine), 1 Mar 2017 4:08 p.m.
Members: Pascal BOUVRY

http://paperjam.lu/

Datenkrake Auto (LËTZEBUERGER Land)

Interview (Internet), 27 Jan 2017
Members: Thomas ENGEL, Sasan JAFARNEJAD

http://www.land.lu/page/article/908/332908/FRE/index.html

Un calcolo matematico dimostra l'esistenza di Dio (CN24)

News (Internet), 22 Jan 2017
Members: Christoph Ewald BENZMÜLLER

http://www.cn24tv.it/news/147822/un-calcolo-matematico-dimostra-l-esistenza-di-dio.html

Secondo uno studioso tedesco, Kurt Gödel, si può dimostrare l'esistenza di Dio con un teorema matematico. "Se Dio è possibile, allora esiste necessariamente. Ma Dio è possibile. Quindi esiste necessariamente". Questo in estrema sintesi il Teorema, del quale due ricercatori, Christoph Benzmuller della Libera Università di Berlino e Bruno Woltzenlogel Paleo dell'Università Tecnica di Vienna, avrebbero dimostrato la correttezza grazie alla capacità di calcolo di un computer portatile.

Radiokolleg - Die Welt begreifen: Warum wir nicht wie Maschinen lernen (Ö1 (ORF))

Interview (Radio), 11 Jan 2017
Members: Christoph Ewald BENZMÜLLER

http://oe1.orf.at/programm/20170111/459531

Angeblich gibt es 302 unterschiedliche Lernstrategien. Zu dieser Erkenntnis kommen australische Wissenschafter/innen in einer Studie, die vor kurzem im Wissenschaftsmagazin "Nature" veröffentlicht wurde. Wille, Motivation, Fähigkeiten und Umgebung sind demnach Parameter, die das Lernen beeinflussen. Aber nur ein paar Ausgaben später liest man im selben Magazin eine Studie von Neurologen, die erkannt haben wollen, dass man lernen kann, wenn man nicht lernt, und die Lernumgebung für das Lernen keine Rolle spielt. An was man sich erinnert, diese Frage wird im Zusammenhang mit Lernen oft unter der Rubrik "Effizienz" diskutiert. Ein Etikett, das vor allem das Lernen der Maschinen prägt. Nur, von ihnen erwartet man nicht, dass sie irgendwas verstehen. Für sie reicht es aus, mit Daten gefüttert zu werden und Antworten zu liefern, die "intelligent" erscheinen. Lernen, so könnte man mutmaßen, ist mehr als mechanisches Zerlegen und Zusammenfügen von Aussagen. Aber ist es das wirklich?

Für das ”Radiokolleg” begibt sich Marianne Unterluggauer auf die Suche nach dem Unterschied von maschinellen und menschlichen Lernansätzen und ihre gegenseitige Beeinflussung.

IPv6 Life Time Achievement Award for Latif Ladid (SnT News)

News (Internet), 10 Jan 2017
Members: Thomas ENGEL, Latif LADID

http://wwwen.uni.lu/snt/news_events/ipv6_life_time_achievement_award_for_latif_ladid

C.5 Guest Researchers

The following guest researchers were invited to the CSC:

Prof. Laura Alonso Alemany (University of Cordoba)

Period: 10 Jul 2017 – 23 Jul 2017
Hosted by: Leon VAN DER TORRE
Reason: Guest researcher in the context of the MIREL project.

Dr. Ryuta Arisaka

Period: 5 Dec 2017 – 8 Dec 2017
Hosted by: Leon VAN DER TORRE

Prof. Guido Boella (Universita’ degli studi di Torino)

Period: 27 Nov 2017
Hosted by: Leon VAN DER TORRE

Dr. Richard Booth (Cardiff University)

Period: 24 Jul 2017 – 28 Jul 2017
Hosted by: Leon VAN DER TORRE

Dr. Ioana Boureanu (University of Surrey)

Period: 31 Aug 2017 – 6 Sep 2017
Hosted by: Rolando TRUJILLO RASUA

Dr. Hauke Bush (Universität zu Lübeck)

Period: 13 Feb 2017
Hosted by: Jun PANG

Richard Clayton
Period: 29 Mar 2017
Hosted by: Peter Y. A. RYAN
Reason:

SRM seminar

Prof. Célia da Costa Pereira (Université de Nice Sophia Antipolis)
Period: 11 Sep 2017 – 15 Sep 2017
Hosted by: Leon VAN DER TORRE

Prof. Marc Denecker (Katholieke Universiteit Leuven)
Period: 20 Mar 2017 – 21 Mar 2017
Hosted by: Leon VAN DER TORRE

Prof. Dr. Falko Dressler (University of Paderborn)
Period: 13 Feb 2017
Hosted by: Thomas ENGEL
Reason: Attendance in a research workshop organazied by Prof. Dr. Thomas Engel and Dr. Sébastien Faye.

Dr. Sébastien Faye (Luxembourg Institute of Science and Technology (LIST), Luxembourg)
Period: 18 Dec 2017 – 19 Dec 2017
Hosted by: Thomas ENGEL
Reason: Annual SECAN-Lab Dagstuhl seminar.

Dr. Raul Fervari (University of Cordoba)
Period: 15 Jun 2017 – 13 Aug 2017
Hosted by: Leon VAN DER TORRE
Reason: Visit related to the MIREL project.

Dr. Daniel Fischer (European Space Agency (ESA), Germany)
Period: 18 Dec 2017 – 19 Dec 2017
Hosted by: Thomas ENGEL
Reason: Annual SECAN-Lab Dagstuhl seminar.

Dr. Markus Forster (KYC3, Luxembourg)
Period: 18 Dec 2017 – 19 Dec 2017
Hosted by: Thomas ENGEL
Reason: Annual SECAN-Lab Dagstuhl seminar.

Jed Grant (KYC3, Luxembourg)
Period: 18 Dec 2017 – 19 Dec 2017
Hosted by: Thomas ENGEL
Reason: Annual SECAN-Lab Dagstuhl seminar.

Professor Frédéric Guinand (University of Le Havre, France)
Period: 25 Sep 2017 – 29 Sep 2017
Hosted by: Pascal BOUVRY
Reason: Research visit - Collaboration on virtual parking area optimisation for car sharing.

Ass.-Prof. Dr. Jérôme Härri (Eurecom - Communication systems, Biot Sophia Antipolis, France)
Period: 13 Oct 2017
Hosted by: Thomas ENGEL
Reason: Member of a PhD defense committee.

Ross Horne (NTU Singapore)
Period: 6 Nov 2017 – 10 Nov 2017
Hosted by: Sjouke MAUW

Hugo Jonker (Open University NL)
Period: 5 Sep 2017
Hosted by: Sjouke MAUW

Prof. Souhila Kaci (Université de Montpellier, LIRMM)
Period: 29 Nov 2017 – 30 Nov 2017
Hosted by: Leon VAN DER TORRE

Stefan Klikovits (Université de Genève, Switzerland)
Period: 7 Sep 2017 – 8 Sep 2017
Hosted by: Nicolas GUELFI, Benoit RIES
Reason: Guest on the topics of CREST a continuous Reactive System DSL and its usage on the BiCS lab projects.

Dr. Christian Köbel (Honda R&D Europe (Germany) GmbH)
Period: 25 Sep 2017
Hosted by: Florian ADAMSKY, Thomas ENGEL
Reason: Presentation of project results

Dr. Fabian Lanze (Huf Secure Mobile GmbH, Velber, Germany)
Period: 4 Dec 2017
Hosted by: Thomas ENGEL
Reason: Supervision of a PhD student.

Professor Kittichai Lavangnananda (KMUTT, Thailand)
Period: 23 Oct 2017 – 27 Oct 2017
Hosted by: Pascal BOUVRY
Reason: Research visit and distinguished talk on ”Application of Genetic Algorithm in Spatial Economics : Emergence of Cities”

Dr. Cheng-Te Li (National Cheng Kung University)
Period: 30 Mar 2017 – 2 Apr 2017
Hosted by: Jun PANG

Prof. Beishui Liao (Zhejiang University)
Period: 3 Jul 2017 – 29 Sep 2017
Hosted by: Leon VAN DER TORRE
Reason: Visit related to the MIREL project.

Ass.-Prof. Dr. Nicolas Louveton (Université de Poitiers, France)
Period: 18 Dec 2017 – 19 Dec 2017
Hosted by: Thomas ENGEL
Reason: Annual SECAN-Lab Dagstuhl seminar.

Hugues Mandon (ENS de Cachan)
Period: 4 Dec 2017 – 7 Dec 2017
Hosted by: Jun PANG

Dr. Samuel Marchal (Aalto University, Finland)
Period: 18 Dec 2017 – 19 Dec 2017
Hosted by: Thomas ENGEL
Reason: Annual SECAN-Lab Dagstuhl seminar.

Dr. Vanina Martinez (Universidad Nacional del Sur)
Period: 5 Nov 2017 – 5 Dec 2017
Hosted by: Leon VAN DER TORRE
Reason: Guest researcher hosted in the context of the MIREL project.

Dr. Roderick McCall (Luxembourg Institute of Science and Technology (LIST), Luxembourg)
Period: 18 Dec 2017 – 19 Dec 2017
Hosted by: Thomas ENGEL
Reason: Annual SECAN-Lab Dagstuhl seminar.

Guozhu Meng (Nanyang Technological University)
Period: 1 Sep 2017 – 30 Nov 2017
Hosted by: Olga GADYATSKAYA, Sjouke MAUW

Prof. Tommie Meyer (University of Cape Town)
Period: 24 Jul 2017 – 28 Jul 2017
Hosted by: Leon VAN DER TORRE

Dr. Jedrzej Musial (Poznan University of Technology (PUT), Poland)
Period: 1 Jul 2017 – 31 Aug 2017
Hosted by: Pascal BOUVRY
Reason: Visiting researcher - collaboration on Cloud brokering and Cloud pricing optimization problems.

David Naccache
Period: 2 May 2017
Hosted by: Peter Y. A. RYAN

David Naccache
Period: 17 Jan 2017
Hosted by: Peter Y. A. RYAN

Professor Fabienne Nouvel (INSA Rennes)
Period: 18 Sep 2017 – 29 Sep 2017
Hosted by: Nicolas NAVET

Katerina Papaioannou (University of Zurich)
Period: 4 Dec 2017 – 8 Dec 2017
Hosted by: Martin THEOBALD

Prof. Gabriella Pigozzi (Université Paris Dauphine)
Period: 1 Mar 2017 – 3 Mar 2017
Hosted by: Leon VAN DER TORRE

Dr. Hongyang Qu (University of Sheeld)
Period: 20 Mar 2017
Hosted by: Jun PANG

Dr. Thomas Scherer (Telindus S.A., Strassen, Luxembourg)
Period: 26 Jun 2017
Hosted by: Thomas ENGEL
Reason: Supervision of a PhD student.

Dr. Thomas Scherer (Telindus S.A., Strassen, Luxembourg)
Period: 13 Oct 2017
Hosted by: Thomas ENGEL
Reason: Member of a PhD defense committee.

Dr. Thomas Scherer (Telindus S.A., Strassen, Luxembourg)
Period: 18 Dec 2017 – 19 Dec 2017
Hosted by: Thomas ENGEL
Reason: Annual SECAN-Lab Dagstuhl seminar.

Dr. Christoph Schommer (University of Luxembourg)
Period: 13 Feb 2017
Hosted by: Thomas ENGEL
Reason: Attendance in a research workshop organazied by Prof. Dr. Thomas Engel and Dr. Sébastien Faye.

Alain Schumacher (SICAP, Luxembourg)
Period: 18 Dec 2017 – 19 Dec 2017
Hosted by: Thomas ENGEL
Reason: Annual SECAN-Lab Dagstuhl seminar.

Carlo Simon (Research fellow, University of Luxembourg)
Period: 18 Dec 2017 – 19 Dec 2017
Hosted by: Thomas ENGEL
Reason: Annual SECAN-Lab Dagstuhl seminar.

Prof. Dr. Otto Spaniol (RWTH Aachen University)
Period: 28 Mar 2017
Hosted by: Thomas ENGEL
Reason: Supervision of Phd student.

Dr. Eugen Staab (N4 Group, Germany)
Period: 18 Dec 2017 – 19 Dec 2017
Hosted by: Thomas ENGEL
Reason: Annual SECAN-Lab Dagstuhl seminar.

Prof. Dr. Julia Stoyanovich (Drexel University)
Period: 6 Dec 2017 – 7 Dec 2017
Hosted by: Martin THEOBALD

Prof. Ivan Varzinczak (Université d'Artois)
Period: 24 Jul 2017 – 28 Jul 2017
Hosted by: Leon VAN DER TORRE

Prof. Dr. Yannis Velegrakis (University of Trento)
Period: 11 Sep 2017
Hosted by: Martin THEOBALD

Pierre Weber (CREOS, Luxembourg)
Period: 26 Oct 2017
Hosted by: Florian ADAMSKY, Thomas ENGEL
Reason: Presentation of project results

Tim Willemse (Eindhoven University of Technology)
Period: 20 Nov 2017 – 1 Dec 2017
Hosted by: Sjouke MAUW

Dr. Dinghao Wu (The Pennsylvania State University)
Period: 9 Jul 2017 – 10 Jul 2017
Hosted by: Jun PANG

Dr. Shin Yoo (KAIST)
Period: 23 Jul 2017 – 24 Jul 2017
Hosted by: Dongsun KIM

Dr. Chengyi Zhang (JiNan University)
Period: 1 May 2017 – 5 May 2017
Hosted by: Jun PANG

Dr. Yang Zhang (Saarland University)
Period: 16 Oct 2017 – 17 Oct 2017
Hosted by: Jun PANG

Dr. Zhiming Zhao (University of Amsterdam)
Period: 30 Jun 2017
Hosted by: Jun PANG

Yury Zhauniarovich (Qatar Computing Research Institute)
Period: 6 Mar 2017 – 7 Mar 2017
Hosted by: Olga GADYATSKAYA

Dr. Zhiqiang Zhong (Paris Dauphine Universit)
Period: 13 Oct 2017
Hosted by: Jun PANG

C.6 Visits

The following visits by CSC members to external organisations took place:

Gergely BANA
Institution: Jagiellonian University
Location: Krakow, Poland
Period: 19 Mar 2017 – 24 Mar 2017.
Reason: Seminar Presentation, Collaboration on Lewis's Principal Principle

Gergely BANA
Institution: Polish Academy of Sciences
Location: Gdansk, Poland
Period: 26 Mar 2017 – 30 Mar 2017.
Reason: Seminar Presentation, Collaboration with Wojczech Jamroga

Gergely BANA
Institution: Keio University
Location: Tokyo, Japan
Period: 15 Apr 2017 – 1 May 2017.
Reason: Collaboration with Prof Mitsuhiro Okada, and presentation at Franco-Japanese workshop

Gergely BANA
Institution: Université Paris-Est Créteil
Location: Paris, France
Period: 10 Jun 2017 – 14 Jun 2017.
Reason: Collaboration with Wojciech Jamroga

Gergely BANA
Institution: Keio University
Location: Tokyo, Japan
Period: 25 Jul 2017 – 18 Aug 2017.
Reason: Collaboration with Mitsuhiro Okada

Gergely BANA
Institution: ENS de Cachan
Location: Cachan, France
Period: 27 Nov 2017 – 29 Nov 2017.
Reason: Presentation, discussions with Hubert Comon, Catuscia Palamidessi

Gergely BANA
Institution: Polish Academy of Sciences
Location: Warsaw and Gdansk, Poland
Period: 30 Nov 2017 – 8 Dec 2017.
Reason: Seminar Presentation, Collaboration with Wojczech Jamroga and his team

Christoph Ewald BENZMÜLLER
Institution: Alpen-Adria-Universitat Klagenfurt
Location: Klagenfurt, Austria
Period: 10 Apr 2017 – 11 Apr 2017.

Christoph Ewald BENZMÜLLER
Institution: LORIA
Location: Nancy, France
Period: 1 Jun 2017 – 2 Jun 2017.

Christoph Ewald BENZMÜLLER
Institution: Cambridge University
Location: Cambridge, United Kingdom
Period: 11 Jul 2017 – 13 Jul 2017.

Christoph Ewald BENZMÜLLER
Institution: University of Campinas
Location: Campinas, Brazil
Period: 17 Jul 2017 – 21 Jul 2017.

Christoph Ewald BENZMÜLLER
Institution: Technische Universitat Wien
Location: Vienna, Austria
Period: 11 Oct 2017 – 12 Oct 2017.

Christoph Ewald BENZMÜLLER
Institution: Miami University
Location: Oxford, Ohio, United States of America
Period: 17 Oct 2017 – 20 Oct 2017.

Christoph Ewald BENZMÜLLER
Institution: Pontifícia Universidade Católica do Rio Grande do Sul
Location: Porto Alegre, Brazil
Period: 2 Dec 2017 – 7 Dec 2017.

Pascal BOUVRY
Institution: NECTEC
Location: Bangkok, Thailand
Period: 2 Sep 2017 – 11 Sep 2017.
Reason: Visiting the NECTEC research center giving some lectures about cloud computing and HPC.

Alfredo CAPOZUCCA
Institution: Innopolis University
Location: Innopolis, Russia
Period: 12 Jan 2017 – 14 Jan 2017.
Reason: Invited Professor - Software engineering course responsible at Bachelor and Master levels

Alfredo CAPOZUCCA

Institution: Innopolis University
Location: Innopolis, Russia
Period: 27 Apr 2017 – 29 Apr 2017.
Reason: Invited Professor - Software engineering course responsible at Bachelor and Master levels

Alfredo CAPOZUCCA

Institution: Universidad Nacional de Rosario
Location: Rosario, Santa Fe, Argentina
Period: 28 Aug 2017 – 3 Oct 2017.
Reason: Invited Professor - Software engineering course responsible at Bachelor and Master levels

Given a seminar : "Messir: a scientific method for the software engineer", invited speaker in the context of the course named "Final Project", which is part of the 5-years degree Informatic Systems Engineering at the Universidad Interamericana, Rosario, Santa Fe, Argentina.

Giovanni CASINI

Institution: Istituto di Scienza e Tecnologia dell'informazione (ISTI)
Location: Pisa, Italy
Period: 22 May 2017 – 29 May 2017.

Giovanni CASINI

Institution: Centre de Recherche en Informatique de Lens (CRIL)
Location: Lens, France
Period: 10 Jul 2017 – 14 Jul 2017.

Giovanni CASINI

Institution: Istituto di Scienza e Tecnologia dell'informazione (ISTI)
Location: Pisa, Italy
Period: 29 Jul 2017 – 7 Aug 2017.

Giovanni CASINI

Institution: University of Cape Town
Location: Cape Town, South Africa
Period: 10 Aug 2017 – 24 Sep 2017.
Reason: Visit done for the MIREL project:
The visiting researcher has worked with Prof. Thomas Meyer in extending Description Logics with Deontic Modalities, in order to define a formalism that is appropriate for the development of Ontologies formalising normative information, and of the correlated reasoners, aimed at executing relevant reasoning tasks as regulatory compliance.

Giovanni CASINI
Institution: Istituto di Scienza e Tecnologia dell'informazione (ISTI)
Location: Pisa, Italy
Period: 7 Nov 2017 – 10 Nov 2017.

Boonyarit CHANGAIVAL
Institution: Université du Havre
Location: Le Harve, France
Period: 26 Jun 2017 – 8 Jul 2017.
Reason: The visit aim was to extend the research topic by broadening the horizon of the application and also by approaching the problem in different angles.

Jérémie DAUPHIN
Institution: National Institute of Informatics
Location: Tokyo, Japan
Period: 1 Jun 2017 – 10 Jul 2017.
Reason: I have met with Prof. Ken Satoh and his research group in the context of the MIREL project. We have started a collaborative work on argumentative reasoning and persuasion. Two papers resulting from this visit have been submitted at a conference and a third one is still in progress.

Olga GADYATSKAYA
Institution: TU Munich
Location: Munich, Germany
Period: 20 Nov 2017.

Nicolas GUELFI
Institution: Innopolis University
Location: Innopolis, Russia
Period: 12 Jan 2017 – 14 Jan 2017.
Reason: Invited Professor - Software engineering course responsible at Bachelor and Master levels

Nicolas GUELFI
Institution: Innopolis University
Location: Innopolis, Russia
Period: 9 Feb 2017 – 11 Feb 2017.
Reason: Invited Professor - Software engineering course responsible at Bachelor and Master levels

Nicolas GUELFI
Institution: Innopolis University
Location: Innopolis, Russia
Period: 27 Apr 2017 – 29 Apr 2017.
Reason: Invited Professor - Software engineering course responsible at Bachelor and Master levels

Shohreh HADDADAN

Institution: Université Cote d'Azur, CNRS, INRIA, I3S
Location: Nice, France
Period: 6 Nov 2017 – 10 Nov 2017.
Reason: I visited Serena Villata from the WIMMICS research team to discuss the research plan in argumentation mining pipeline.

Abdallah Ali Zainelabden Abdallah IBRAHIM

Institution: NECTEC
Location: Bangkok, Thailand
Period: 2 Sep 2017 – 11 Sep 2017.
Reason: Visiting the NEC TEC research center giving some lectures about cloud computing and HPC.

Zhe LIU

Institution: Newcastle University
Location: Newcastle upon Tyne, United Kingdom
Period: 1 Aug 2017 – 16 Aug 2017.
Reason: Visiting Dr. Feng Hao, discussion about possibilities to improve the performance of the J-PAKE protocol.

Zhe LIU

Institution: Pusan National University and Hansung University
Location: Busan and Seoul, South Korea
Period: 1 Dec 2017 – 11 Dec 2017.
Reason: Visiting Prof. Howon Kim and Prof. Hwajeong Seo, discussion about implementation of Elliptic Curve Cryptography.

Qin MA

Institution: Department of Computer Science and Technology, Nanjing University
Location: Nanjing, China
Period: 25 Aug 2017 – 31 Aug 2017.

Sjouke MAUW

Institution: NUS and NTU
Location: Singapore, Singapore
Period: 18 Feb 2017 – 27 Feb 2017.

Sjouke MAUW

Institution: COST meeting
Location: Sutomore, Montenegro
Period: 13 Mar 2017 – 16 Mar 2017.

Sjouke MAUW
Institution: SUTD and NTU
Location: Singapore, Singapore
Period: 31 May 2017 – 8 Jun 2017.

Sjouke MAUW
Institution: Open University NL
Location: Maastricht, Netherlands
Period: 9 Jun 2017.

Sjouke MAUW
Institution: E-VOTE-ID'17
Location: Bregenz, Austria
Period: 24 Oct 2017 – 27 Oct 2017.

Sjouke MAUW
Institution: TU Munich
Location: Munich, Germany
Period: 20 Nov 2017 – 23 Nov 2017.

Jun PANG
Institution: University of Twente
Location: Enschede, Netherlands
Period: 15 Feb 2017 – 17 Feb 2017.

Xavier PARENT
Institution: Standord University
Location: Stanford, United States of America
Period: 4 Jan 2017 – 22 Jan 2017.
Reason: Visit done for the MIREL project.

Xavier PARENT
Institution: University of Calabria
Location: Rende, Italy
Period: 18 May 2017 – 19 May 2017.

Valentin PLUGARU
Institution: National Electronics and Computer Technology Center (NECTEC)
Location: Bangkok, Thailand
Period: 4 Sep 2017 – 8 Sep 2017.
Reason: Invited speaker at the National Electronics and Computer Technology Center (NECTEC), statutory government organization under the National Science and Technology Development Agency, Ministry of Science and Technology

of Thailand. NECTEC is responsible for undertaking, supporting and promoting the research and development of electronics and computer technologies for the industrial sector and social development. I held 5 HPC focused sessions on the following topics: Modern facilities for research, Multi-physics workflows, HPC debugging, profiling and performance analysis, and HPC systems administration.

Andrei POPLETEEV

Institution: University of Trento
Location: Trento, Italy
Period: 28 Apr 2017.
Reason: Dr. Andrei Popleteev was an evaluation committee member of the PhD defense of Alban Maxhuni.

Andrei POPLETEEV

Institution: Aalto University
Location: Espoo, Finland
Period: 22 Aug 2017.
Reason: Dr. Andrei Popleteev visited the Ambient Intelligence Group at Aalto University to discuss areas of common interest and extend the collaboration network.

Yunior RAMIREZ CRUZ

Institution: University of Cadiz
Location: Algeciras, Spain
Period: 9 Oct 2017 – 13 Oct 2017.

Benoit RIES

Institution: Innopolis University
Location: Innopolis, Russia
Period: 9 Feb 2017 – 11 Feb 2017.
Reason: Invited Professor - Software engineering course responsible at Bachelor and Master levels

Benoit RIES

Institution: Innopolis University
Location: Innopolis, Russia
Period: 27 Apr 2017 – 29 Apr 2017.
Reason: Invited Professor - Software engineering course responsible at Bachelor and Master levels

Livio ROBALDO

Institution: Stanford University
Location: Stanford, United States of America
Period: 1 Oct 2017 – 15 Dec 2017.
Reason: Visit done for the MIREL project.

Peter Y. A. RYAN
Institution: ENS Paris
Location: Paris, France
Period: 1 Sep 2017 – 30 Sep 2017.
Reason: Visiting Professor

Ridha SOUA
Institution: Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services
Location: Luxembourg, Luxembourg
Period: 7 Nov 2017.
Reason: Dr. Ridha Soua is a national normalization delegate expert in Internet of Things (IoT). He was invited to discuss the position of University of Luxembourg for ISO/IEC DIS 30141 Internet of Things Reference Architecture (IoT RA) under ballot.

Jorge Luis TORO POZO
Institution: ETH Zurich
Location: Zurich, Switzerland
Period: 11 Dec 2017 – 14 Dec 2017.

Rolando TRUJILLO RASUA
Institution: University of Eindhoven
Location: Eindhoven, Netherlands
Period: 3 Feb 2017 – 7 Feb 2017.

Rolando TRUJILLO RASUA
Institution: Open University of the Netherlands
Location: Heerlen, Netherlands
Period: 6 Mar 2017.

Rolando TRUJILLO RASUA
Institution: University of Cadiz
Location: Algeciras, Spain
Period: 9 Oct 2017 – 13 Oct 2017.

Leon VAN DER TORRE
Institution: Stanford University
Location: Stanford, United States of America
Period: 4 Jan 2017 – 22 Jan 2017.
Reason: Visit done for the MIREL project.

Leon VAN DER TORRE
Institution: Université de Montpellier
Location: Montpellier, France
Period: 6 Mar 2017 – 9 Mar 2017.
Reason: Visit to continue collaborative work with Prof. Souhila Kaci.

Leon VAN DER TORRE
Institution: National Institute of Informatics
Location: Tokyo, Japan
Period: 8 Apr 2017 – 23 Apr 2017.
Reason: Visit done for the MIREL project.

Leon VAN DER TORRE
Institution: National Institute of Informatics
Location: Tokyo, Japan
Period: 29 Aug 2017 – 13 Sep 2017.
Reason: Visit done for the MIREL project.

Leon VAN DER TORRE
Institution: Zhejiang University
Location: Hangzhou, China
Period: 29 Sep 2017 – 17 Oct 2017.
Reason: Visit done for the MIREL project.

Appendix D

Software Developments

Accord

https://accord.uni.lux

License: Internal use only

Members: Bertrand DESSART (Analyst, Architect), Christian GLODT (Analyst, Architect, Designer, Developer, Tester)

Description: Accord is a the successor to the CSC Information System and is intended to provide services to all FSTC research units. It manages research information and allows the automatic generation of reports and websites.

Changes: Numerous improvements have been made to Accord in 2017. Most importantly, there have been significant improvements to website and report generation, refinements to the user-permission system, and support for more detailed funding and budget information in research projects.

ADTool

http://satoss.uni.lu/software/adtool

License: free use

Members: Piotr KORDY (Developer), Sjouke MAUW (Analyst)

Description: The attack–defense tree language formalizes and extends the attack tree formalism. It is a methodology to graphically analyze security aspects of scenarios. With the help of attributes on attack–defense trees, also quan-

titative analysis can be performed. As attack–defense tree models grow, they soon become intractable to be analyzed by hand. Hence computer support is desirable. Software toll, called the ADTool, has been implemented as a part of the ATREES project to support the attack–defense tree methodology for security modeling. The main features of the ADTool are easy creation, efficient editing, and quantitative analysis of attack–defense trees. The tool is available at http://satoss.uni.lu/software/adtool. The tool was realized by Piotr Kordy and its manual was written by Patrick Schweitzer.

Algorithms for Probabilistic Argumentation

License: Creative Common

Members: Leon VAN DER TORRE (Architect)

Description: We developed efficient algorithms for computing probabilistic argumentation. These algorithms were implemented in Java, and tested on a machine with an Intel CPU running at 2.26 GHz and 2.00 GB RAM. Please refer to the following paper in details.

1. Beishui Liao, Kang Xu, Huaxin Huang. Formulating Semantics of Probabilistic Argumentation by Characterizing Subgraphs: Theory and Empirical Results, Jurnal of Logic and Computation, to appear. http://arxiv.org/abs/1608.00302

ASSA-PBN

http://satoss.uni.lu/software/ASSA-PBN/

License: free use

Members: Jun PANG (Analyst)

Description: ASSA-PBN is a tool specially designed for approximate steady-state analysis of large probabilistic Boolean networks (PBNs). The approximate steady-state analysis is crucial for large PBNs, which naturally arise in the domain of Systems Biology. ASSA-PBN provides different solutions for different size PBNs. In particular, ASSA-PBN provides the two-state Markov chain approach and the Skart approach for large PBNs. The latest version of the package was released in Nov. 2014 and is available from http://satoss.uni.lu/software/ASSA-PBN/.

bagit

http://demos.uni.lux/bagit

License: non-redistributable, for internal use only

Members: Christian GLODT (Designer, Developer, Tester)

Description: An internal web-based tool that provides assistance to research groups by storing, pooling, tagging and indexing papers and other publications.

Baumüller ProMaster

License: UL

Members: Surena NESHVAD (Developer), David NORTA (Developer)

Description: Baumüller ProMaster is the software to operate the inverter and electrical machines in the lab.

BiCS Management Tool (BMT)

https://messir.uni.lu/bmt/login

License: Eclipse Public License 1.0

Members: Nicolas GUELFI (Analyst), Benjamin JAHIC (Developer), Benoit RIES (Analyst)

Description: Development of the BiCS Management Tool, a web application for managing the BiCS Semester Projects.

Changes: First version has been deployed in production on September 22, 2017. and maintenance has been performed since then.

BlueScanner

License: MIT

Members: Walter BRONZI (Developer)

Description: The scope of the application is to collect Bluetooth beacons whilst in a driving scenario and send them to a server. In this context was performed a 2-month collection campaign within SnT. More than 20 participants where collected for this stage.

CheckMasks

https://github.com/coron/checkmasks

License: GPL v2

Members: Jean-Sébastien CORON (Designer)

Description:

CheckMasks: formal verification of side-channel countermeasures for cryptographic implementations

This is an implementation in Common Lisp of the techniques described in the paper:

[Cor17b] Jean-Sebastien Coron. Formal Verification of Side-Channel Countermeasures via Elementary Circuit Transformations. IACR eprint archive. https://eprint.iacr.org/2017/879.pdf

Generic verification of security properties:

- Generic verification of the t-SNI of multiplication-based refreshing
- Generic verification of the t-SNI of multiplication
- Generic verification of some properties of RefreshMasks: lemmas 5, 6, 7, 8 of [Cor17a], and Lemma 3 from [CRZ18].
- Generic verification of the t-SNI property of the Boolean to arithmetic conversion algorithm from [Cor17a].

Polynomial-time verification fo security properties:

- Poly-time verification of the t-SNI of multiplication-based refreshing [Cor17b, Lemma 3]
- Poly-time verification of some properties of RefreshMasks: [Cor17b, Lemma 4] corresponding to [Cor17a, Lemma6], and [Cor17b, Lemma 5] corresponding to [Cor17a, Lemma 5]
- Poly-time verification of the t-SNI of multiplication [Cor17b, Lemma 6]

Automatic generation of security proof:

- Automatic poly-time verification of t-SNI of multiplication-based refreshing, and of the two previous properties of RefreshMasks.

Reference: [Cor17a] Jean-Sebastien Coron. High-order conversion from boolean to arithmetic masking. Proceedings of CHES 2017.

[CRZ18] Jean-Sébastien Coron, Franck Rondepierre, Rina Zeitoun. High Order Masking of Look-up Tables with Common Shares. To appear at TCHES 2018. IACR Cryptology ePrint Archive 2017: 271 (2017)

CollaTrEx

License: N/A

Members: Jean BOTEV (Architect)

Description: CollaTrEx is framework for collaborative context-aware mobile exploration and training. It is particularly designed for the in-situ collaboration within groups of learners performing together diverse educational activities to explore their environment in a fun and intuitive way.

Aside from employing both absolute and relative spatio-temporal context for determining the available activities, different buffering levels are an important conceptual feature supporting seamless collaboration in spite of temporary connection losses or when in remote areas.

CollaTrEx comprises a prototypical front-end implementation for tablet devices, as well as a web-based back-end solution for the creation and management of activities which can be easily extended to accommodate both future technologies and novel activity types.

CSC Information System

http://demos.uni.lux/csc

License: Internal use only

Members: Bertrand DESSART (Analyst, Architect), Christian GLODT (Analyst, Architect, Designer, Developer, Tester)

Description: The CSC Information System is a web-based interface for the management of information related to the CSC, such as research projects, research areas, research groups, and many other elements related to the CSC and its member's activities. The CSC Information System is built using the Django Framework.

Data acquisition platform

License: MIT

Members: Andrei POPLETEEV (Developer)

Description: The INDOORS project has created an open-source data acquisition platform (DAQ), which is designed to facilitate data collection for indoor localization experiments. The DAQ platform allows recording of raw radio signal samples from multiple bands simultaneously with ground-truth location and environment state (weather and crowd dynamics) metadata. The platform employs an Ettus Research USRP B210 software-defined radio to collect short raw samples of FM, GSM downlink, Wi-Fi and several active DVB-T channels. Ground truth location is specified manually by the operator by selecting one of the predefined reference points on an interactive map; the detailed weather information, in turn, is automatically fetched from an online service. By collecting raw radio-frequency (RF) signal samples from a software-defined radio receiver, this tool separates data acquisition from the extraction of location-dependent signal features, thus offering unprecedented flexibility for the evaluation of classic and novel localization methods (potentially including those yet to be devised).

DBVerify

http://satoss.uni.lu/software/DBVerify/

License: Open source

Members: Sjouke MAUW (Designer), Zachary Daniel SMITH (Developer), Jorge Luis TORO POZO (Designer), Rolando TRUJILLO RASUA (Designer)

Description: DBVerify is a set of Tamarin implementation of several state-of-the-art distance-bounding protocols as well as their MSC representation. It intends to show the usage of the causality-based verication methodology proposed in our paper "Distance-Bounding Protocols: Verication without Time and Location" (to appear at IEEE S&P'18). It was developed by Zach Smith (ZS) and Jorge Toro-Pozo (JT).

Democles

http://democles.lassy.uni.lu/

License: Freely redistributable, see details at: http://democles.lassy.uni.lu/license.html

Members: Christian GLODT (Architect, Designer, Developer, Tester)

Description: Democles is a modeling tool that supports the EP language developed by LASSYs MDE group. It is mainly developed by Christian Glodt.

Digraph3

http://leopold-loewenhein.uni.lu/docDigraph3

License: GNU General Public License v.2+

Members: Raymond Joseph BISDORFF (Developer)

Description: Digraph3 is a collection of Python3 modules and resources for implementing decision aiding algorithms for selecting, ranking, sorting or rating, and clustering with multiple incommensurable criteria. These computing resources are useful in the field of Algorithmic Decision Theory and more specifically in outranking based multiple criteria decision aiding.

ELRA Language Corpus

License: LC/ELDA/DISTR-S/2014-11/001-UNILU

Members: Christoph SCHOMMER (Designer)

Description: The *deL1L2IM* corpus, created between May and August 2012 and last updated in August 2014, has been collected within the framework of a PhD project (Mrs. Sviatlana Höhn, geb. Danilava) on the development of a learning method implying conversations with an artificial companion. This PhD work is presented as a qualitative investigation of instant messaging dialogues on a long-term basis (four months) between advanced learners of German and German native speakers, chatting about whatever topic they wish.

The dataset is composed of 72 dialogues, each of them having a duration of 20 to 45 minutes. The whole corpus contains ca. 52,000 words and 4,800 messages and has a file size of 0,5 Mb. Nine pairs of participants – i.e. nine learners and four native speakers – were required, with 8 dialogues per pair.

The interactions have undergone linguistic analysis whereby the annotation will be performed only on repair/correction sequences (incomplete learner error annotation). The goal of the project was to create an application for language modelling and to improve learner language applications, tutoring softwares and dialogue systems.

The corpus is delivered in one written text file (in XML format, customized under TEI P5).

Excalibur

https://messir.uni.lu/confluence/display/EXCALIBUR/Excalibur

License: Eclipse Public License 1.0

Members: Alfredo CAPOZUCCA (Developer), Nicolas GUELFI (Developer), Benoit RIES (Developer)

Description: Excalibur is a tool supporting the Messir methodology, a Scientific Method for the Software Engineering Master, used in Software Engineering Lectures at bachelor and master levels.

Excalibur tool covers the phase of Requirements Analysis and its main features are requirements analysis specification (its own DSL), requirements report generation (latex/pdf) and requirements simulation (prolog). It relies on Eclipse technologies as XText for textual specification and Sirius for graphical views of the textual specifications.

It is available here: http://messir.uni.lu

Changes:

- Excalibur v1.7 for BINFO semester 4 students and for Innopolis University (Russia)
  - http://messir.uni.lu:8085/jira/browse/EX/fixforversion/12900
- Excalibur v1.8 for BINFO semester 3 students, LL-BINFO lifelong learning students bachelor and MICS master students
  - http://messir.uni.lu:8085/jira/browse/EX/fixforversion/12500

IDP

http://icr.uni.lu/mcramer/index.php?id=3

License: Public

Members: Diego Agustin AMBROSSIO (Tester), Marcos CRAMER (Tester)

Description: implementation of revocation schemes according to the classification proposed by Hagström et al. (2001)

J-NERD/J-REED

https://people.mpi-inf.mpg.de/~datnb/

License: BSD

Members: Martin THEOBALD (Architect)

Description: Open-source information extraction libraries

LEO-III

https://github.com/leoprover/Leo-III

License: BSD

Members: Christoph Ewald BENZMÜLLER (Developer)

Description: An automated theorem prover for classical higher-order logic (with choice)

Leo-III [SWB16] is an automated theorem prover for (polymorphic) higher-order logic which supports all common TPTP dialects, including THF, TFF and FOF as well as their rank-1 polymorphic derivatives [SWB17]. It is based on a paramodulation calculus with ordering constraints and, in tradition of its predecessor LEO-II [BP15], heavily relies on cooperation with external (mostly first-order) theorem provers for increased performance. Nevertheless, Leo-III can also be used as a stand-alone prover without employing any external cooperation.

Leo-III won the 2nd place in the world championships in higher-order automated theorem proving.

Lightning

http://lightning.gforge.uni.lu/

License: binary only, freely redistributable without modification

Members: Loïc GAMMAITONI (Analyst, Architect, Designer, Developer, Tester), Christian GLODT (Architect, Designer, Developer, Tester)

Description: Lightning is a lightweight language workbench based on Alloy and Eclipse.

Lightning allows the definition of Languages via the specification of Alloy models, thus allowing the lightweight analysis of its components.

The focus of Lightning is to provide support to language engineers to efficiently design their DSLs.

LuST-LTE

License: MIT

Members: Thierry DERRMANN (Developer)

Description: A Simulation Package for Pervasive Vehicular Connectivity.

LuST-LTE is a package of open-source simulation tools that allows the simulation of vehicular traffic along with pervasive LTE connectivity. Most importantly, LuST-LTE provides handover functionality and adds LTE infrastructure of a mobile network operator to the LuST road traffic simulation scenario of Luxembourg City.

Changes: In 2017, the software tool LuST-LTE was extended to reflect the actual Luxembourg LTE network needed for the research within the project MAMBA. The improved version of the tool was presented at IEEE ITSC 2017.

MaRCo Model Editor

http://marco.gforge.uni.lu/tools.html

License: binary only, freely redistributable without modification

Members: Christian GLODT (Architect, Designer, Developer, Tester)

Description: The MaRCo Model Editor is an Eclipse plugin that provides functionality for creating and editing XBPNM and Policy models, as well as transformation capabilities allowing to generate an Alloy representation of an XBPNM model.

MDPRevision

https://github.com/marcvanzee/mdp-plan-revision

License: Creative Commons

Members: Marc VAN ZEE (Developer)

Description: Read a more detailed description of the conceptual underpinnings and experimental results in the following paper:

Intention Reconsideration as Metareasoning (Marc van Zee, Thomas Icard), In Bounded Optimality and Rational Metareasoning NIPS 2015 Workshop, 2015.

Summary: This project implements an agent that is situated on a Markov Decision Process (MDP). The agent is able to compute the optimal policy through

Value Iteration. The MDP is changing over time, and the agent can respond to this change by either acting (i.e. executing the optimal action according to its current policy) or thinking (i.e. computing a new policy). The task is to learn the best meta-reasoning strategy, i.e. deciding when to think or act, based on the characteristics of the environment.

This general setup is quite complex, so we have simplified the environment (i.e. the MDP) to the TIleworld environment. This consists of an agent that is situated on a grid. It can move up, down, left, or right and has to fill holes, which means it has to reach specific states in the grid. It cannot move through obstacles.

We then develop several metareasoning strategies that the agent can use.

MiCS Management System

http://demos.uni.lux/mics

License: non-redistributable, for internal use only

Members: Christian GLODT (Designer, Developer, Tester)

Description: An internal web-based tool developed for the management of modules, courses and profiles of the Master in Information and Computer Sciences. Developed by Christian Glodt.

MinUS

http://satoss.uni.lu/software/MinUS

License: free use

Members: Jun PANG (Analyst)

Description: This tool, MinUS, integrates the technologies of trajectory pattern mining with the state-of-the art research on discovering user similarity with trajectory patterns. Specifically, with MinUS, we provide a platform to manage movement datasets, and construct and compare users trajectory patterns. Tool users can compare results given by a series of user similarity metrics, which allows them to learn the importance and limitations of different similarity metrics and promotes studies in related areas, e.g., location privacy. Additionally, MinUS can also be used by researchers as a tool for preliminary process of movement data and parameter tuning in trajectory pattern mining. The tool is available at http://satoss.uni.lu/software/MinUS.

Mobility Profiler

License: MIT

Members: Sébastien FAYE (Developer)

Description: This profiler is able to estimate a user's mobility profile based on anonymized and lightweight smartphone data. In particular, this system is composed of (1) a web analytics platform, able to analyze multimodal sensing traces and improve our understanding of complex mobility patterns, and (2) a smartphone application, able to show a user's profile generated locally in the form of a spider graph. In particular, this system uses anonymized and privacy-friendly data and methods, obtained thanks to the combination of Wi-Fi traces, activity detection and graph theory, made available independent of any personal information.

Model Decomposer

http://democles.lassy.uni.lu/documentation/TR_LASSY_10_06.pdf

License: free to use, binary redistribution permitted

Members: Christian GLODT (Architect, Developer), Qin MA (Analyst)

Description: An Eclipse plugin that implements a generic model decomposition technique which is applicable to Ecore instances and EP models, and is described in a paper published in the proceedings of the FASE 2011 conference.

PREXT

https://github.com/karim-emara/PREXT

License: GNU GPL

Members: Karim Ahmed Awad El-Sayed EMARA (Developer)

Description: PREXT is a unified and extensible framework that simulate pseudonym change schemes (i.e. privacy schemes) in VANET. It supports seven privacy schemes of different approaches including silent period, context-based and mix-zone and can be easily extended to include more schemes. It includes adversary modules that can eavesdrop vehicle messages and track their movements. This adversary is used in measuring the gained privacy in terms of several popular metrics such as entropy, traceability and pseudonym usage statistics.

RationalGRL

https://github.com/RationalArchitecture/RationalGRL

License: Creative Common

Members: Marc VAN ZEE (Developer)

Description: Goal modeling languages, such as i* and the Goal-oriented Requirements Language (GRL), capture and analyze high-level goals and their relationships with lower level goals and tasks. However, in such models, the rationalization behind these goals and tasks and the selection of alternatives are usually left implicit.Rationalization consists of arguments for and against certain goals and solutions, which allow checking whether a particular goal model is a correct rendering of the relevant stakeholders' opinions and discussions. To better integrate goal models and their rationalization, we develop the RationalGRL framework, in which argument diagrams can be mapped to goal models. Moreover, we integrate the result of the evaluation of arguments and their counterarguments with GRL initial satisfaction values. We develop an interface between the argument web tools OVA and TOAST and the Eclipse-based tool for GRL called jUCMNav.

SWIPE: Monitoring Human Dynamics using Smart Devices

https://github.com/sfaye/SWIPE/

License: MIT

Members: Sébastien FAYE (Developer)

Description: SWIPE is a platform for sensing, recording and processing human dynamics using smart devices. The idea behind this type of system, which exists for the most part on smartphones, is to consider new metrics from wearables — in our case smartwatches. These new devices, used in parallel with traditional smartphones, provide clear indicators of the activities and movements performed by the users who wear them. They can also sense environmental data and interactions. The SWIPE architecture is structured around two main elements, namely (1) an Android application deployed directly on the devices, allowing them to synchronize and collect data; and (2) a server for storing and processing the data.

TESMA

License: Eclipse Public License 1.0

Members: Nicolas GUELFI (Analyst), Benjamin JAHIC (Developer), Sandro REIS (Developer), Benoit RIES (Analyst)

Description: Tool for the Specification, Management and Assessment of Teaching Programs.

Nicolas Guelfi, Benjamin Jahic and Benoît Ries, TESMA: Towards the Development of a Tool for Specification, Management and Assessment of Teaching Programs, published in the Proceedings of the 2nd International Conference on Applications in Information Technology (ICAIT-2016)

http://orbilu.uni.lu/handle/10993/28607

TriAD

https://people.mpi-inf.mpg.de/~gurajada/

License: BSD

Members: Martin THEOBALD (Architect)

Description: Open-source, distributed graph database

ULHPC-credits

https://gitlab.uni.lu/vplugaru/ulhpc-tools

License: GPLv3

Members: Valentin PLUGARU (Designer)

ULHPC-platform-usage

License: GPLv3

Members: Valentin PLUGARU (Designer)

Description: Tool used on the UL HPC platform (Gaia/Chaos clusters: 'ulhpc_platform_usage') to monitor per-user resource utilization, with configurable email alerting.

Combined with the ULHPC-credits tool, it allows for a more comprehensive understanding of platform utilization.

Visual Contract Builder

http://vcl.gforge.uni.lu/

License: free to use, binary redistribution permitted

Members: Christian GLODT (Architect, Designer, Developer)

Description: A suite of Eclipse plugins that provide support for graphically editing and typechecking VCL (Visual Contract Language) diagrams.

Web-based itinerary planner for Luxembourg

http://sfaye.com/vehicularlab/OTP.zip

License: MIT

Members: Sébastien FAYE (Developer)

Description: The first prototype allows users to plan trips using several intermediate location points. In particular, users can choose between different modes of transport or a combination of several modes, including those with time-dependent availability (i.e. bike-sharing). The system automatically computes interesting trips and suggested the best ones to the user. Current modes of transportation include car, bicycle, Veloh, public transport and walking.

WFP toolbox

License: TBA

Members: Karim Ahmed Awad El-Sayed EMARA (Developer), Daniel FORSTER (Developer), Asya MITSEVA (Developer), Andriy PANCHENKO (Developer)

Description: The website fingerprinting toolbox consists of multiple scripts and binaries that allow a user to carry out research related to the website fingerprinting attack. The toolbox enables a user to automate the visit of websites, record the traffic traces, clean the traffic traces from wrong instances, extract features from the traffic traces and finally train a machine learning classifier.

XDEM (eXtended Discrete Element Method)

http://luxdem.uni.lu/

License: Internal use only

Members: Bernhard PETERS (Developer), Alban ROUSSET (Developer), Sébastien VARRETTE (Developer)

Description: The eXtended Discrete Element Method (XDEM), formerly Discrete Particle Method (DPM), is an advanced numerical simulation tool which deals with both motion and chemical conversion of particulate material such as coal or biomass in furnaces. However, predictions of solely motion or conversion in a de-coupled mode are also applicable. The Discrete Particle Method uses object oriented techniques that support objects representing three-dimensional particles of various shapes such as cylinders, discs or tetrahedrons for example, size and material properties. This makes it a highly versatile tool dealing with a large variety of different industrial applications of granular matter. A user interface allows easily extending the software further by adding user-defined models or material properties to an already available selection of materials, properties and reaction systems describing conversion. Thus, the user is relieved of underlying mathematics or software design, and therefore, is able to direct his focus entirely on the application. The Discrete Particle Method is organised in a hierarchical structure of C++ classes and works both in Linux and XP environments also on multi-processor machines. This software is developed by the XDEM research team, led by Prof. Bernhard Peters from the Research Unit in Engineering Science (RUES) in collaboration with the Computer Science and Communications (CSC) research unit.

Changes: The work on XDEM is now focusing on the performance optimization. The following improvement add in the code:

New load-balancing algorithms have been validated and added in XDEM [10993/32810]

- Zoltan (RIB, RCB, PhG), METIS and SCOTCH have been added
- Different strategies regarding the relative cost between computation and communication have been studied

Better Broadphase Collision Detection algorithms for XDEM [10993/32261]

- Implementation of many classical Collision Detection algorithms
- First implementations in parallel using OpenMP and Thrust (work-in-progress)

Support for parallel execution for coupled simulation XDEM-OpenFOAM [10993/32256]

- Identification of the constraints on the DEM and CFD domains

OpenMP parallelization, in order to target hybrid execution OpenMP/MPI (work-in-progress)

- parallelization of the main loops

Yactul

License: N/A

Members: Steffen ROTHKUGEL (Architect)

Description: Yactul is a game-based student response framework for interactive education.

Appendix E

Staff Statistics

Note: Statistics in this chapter count staff numbers using FTE (Full-Time Equivalent) units. The FTE number takes into account the occupancy of the position (half-time, full-time or similar), as well as the start or end of the employment of the staff member during the course of the year.

An FTE number of 1.0 indicates a staff member being employed at full time for the duration of the whole year.

E.1 Number of Staff by Category (Full-Time Equivalent)

Category	Number
Doctoral Candidate	49.48
Research Associate (Post-doc)	38.87
Professor	16.61
Research Scientist	13.5
Research Associate	10.79
Student with Limited Contract	10.25
Administrative Aid	6.5
Associate Professor	6
Technical Support Staff Member	4.61
Intern	3.35
Technician on Project	2.05
Senior Lecturer	2
Director of Interdisciplinary Center	1.0
Scientific Support Staff Member	0.99
Student with Seasonal Position	0.77
Project Support Staff Member	0.63
Total	*167.4*

Table E.1: Number of Staff by Category

E.2 Distribution of Staff by Category

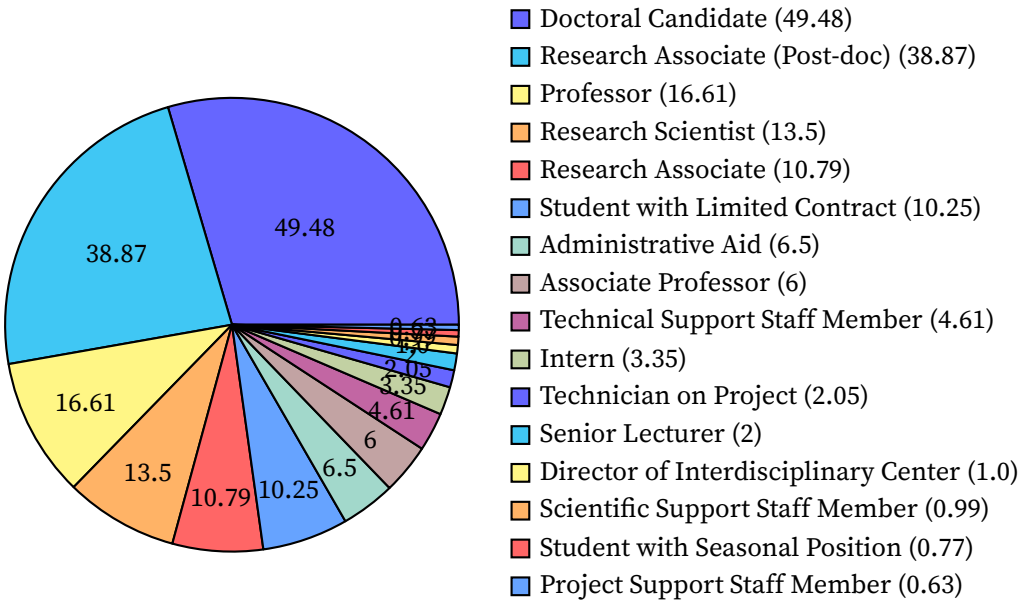


Figure E.1: Staff Distribution

E.3 List of Members by Category

Note: In the following list, staff members without an explicitly shown FTE number implicitly have an FTE number of 1.0.

Position	Last Name	First Name
Professor	BIRYUKOV	Alexei
	BISDORFF	Raymond Joseph (0.7 FTE)
	BOUVRY	Pascal
	BRIAND	Lionel
	ENGEL	Thomas
	ESTEVES VERISSIMO	Paulo
	GUELFI	Nicolas
	KELSEN	Pierre
	LE TRAON	Yves
	LEPREVOST	Franck
	MAUW	Sjouke
	RYAN	Peter Y. A.
	SACHAU	Juergen
	SORGER	Ulrich

Position	Last Name	First Name
	THEOBALD	Martin (0.91 FTE)
	VAN DER TORRE	Leon
	ZAMPUNIERIS	Denis
Associate Professor	CORON	Jean-Sébastien
	MÜLLER	Volker
	NAVET	Nicolas
	ROTHKUGEL	Steffen
	SCHOMMER	Christoph
	STEENIS	Bernard
Research Associate (Post-doc)	ADAMSKY	Florian
	ALEKSANDROVA	Marharyta (0.16 FTE)
	BANA	Gergely (0.84 FTE)
	BENZMÜLLER	Christoph Ewald (0.84 FTE)
	BLEUSE	Raphaël (0.13 FTE)
	BRUST	Matthias
	CASINI	Giovanni
	CASTIGNANI	German (0.49 FTE)
	COGLIATI	Benoît-Michel
	CRAMER	Marcos
	DASHEVSKYI	Stanislav (0.29 FTE)
	DECOUCHANT	Jérémie
	DELERUE ARRIAGA	Afonso (0.96 FTE)
	EMARA	Karim Ahmed Awad El-Sayed (0.62 FTE)
	FAYE	Sébastien (0.66 FTE)
	GADYATSKAYA	Olga
	GAMMAITONI	Loïc (0.08 FTE)
	HARTMANN	Thomas
	HU	Tingting
	HUYNEN	Jean-Louis (0.45 FTE)
	IOVINO	Vincenzo
	JHAWAR	Ravi (0.49 FTE)
	KHOVRATOVICH	Dmitry (0.23 FTE)
	KIM	Dongsun
	KUBLER	Sylvain (0.66 FTE)
	LEE	Moon Sung
	LI	Li
	LIU	Zhe (0.75 FTE)
	MIZERA	Andrzej (0.58 FTE)
	NAVEH	David (0.75 FTE)
	NESHVAD	Surena (0.91 FTE)
	OSTREV	Dimiter
	OUCHANI	Samir (0.33 FTE)
	PARENT	Xavier
	PAUL	Soumya (0.71 FTE)

Position	Last Name	First Name
	POPLETEEV	Andrei (0.83 FTE)
	RAHLI	Vincent
	RAMIREZ CRUZ	Yunior
	RIAL DURAN	Alfredo
	ROBALDO	Livio
	ROBERT	Jérémy
	RODRIGUEZ LERA	Francisco Javier
	ROENNE	Peter
	ROSALIE	Martin
	SCHIFFNER	Stefan (0.25 FTE)
	SKROBOT	Marjan (0.96 FTE)
	SOUA	Ridha
	TABATABAEI	Masoud (0.62 FTE)
	TRUJILLO RASUA	Rolando
	VELICHKOV	Vesselin (0.28 FTE)
Research Associate	BOTEV	Jean
	FORSTER	Daniel (0.66 FTE)
	FOUQUET	François
	FUEHRER	Detlef (0.25 FTE)
	GLODT	Christian
	GROSZSCHÄDL	Johann
	KOZHAYA	David
	KUSHNIAROU	Artsiom (0.71 FTE)
	LAMORTE	Luca (0.83 FTE)
	MACHALEK	Aurel
	MOAWAD	Assaad (0.04 FTE)
	PLUGARU	Valentin
	TURCANU	Ion (0.29 FTE)
	YU	Jiangshan
Research Scientist	BERNARD	Nicolas
	BISSYANDE	Tegawendé François d Assise
	CAPOZUCCA	Alfredo
	DANOY	Grégoire
	FRANCK	Christian
	FRANK	Raphaël
	MA	Qin (0.5 FTE)
	PANCHENKO	Andriy
	PANG	Jun
	PAPADAKIS	Mike
	RIES	Benoit
	VARRETTE	Sébastien
	VOLP	Marcus
	WEYDERT	Emil
Administrative Aid	EDWARDSDOTTIR	Helga
	FLAMMANG	Danièle (0.75 FTE)
	OCHSENBEIN	Anne

Position	Last Name	First Name
	OESTLUND	Stefanie (0.7 FTE)
	SCHMITZ	Fabienne
	SCHROEDER	Isabelle (0.5 FTE)
	THÜR	Claudia (0.72 FTE)
	VIAU-COURVILLE	Mathieu (0.33 FTE)
	WOLTERS	Nicola (0.5 FTE)
Technical Support Staff Member	DUNLOP	Dominic (0.73 FTE)
	LE CORRE	Yann
	PARISOT	Clément (0.88 FTE)
	REIS	Sandro
	STEMPER	André
Technician on Project	CHARPIOT	Louise (0.06 FTE)
	EDDS	Liam (0.21 FTE)
	JAHIC	Benjamin
	KORDY	Piotr (0.49 FTE)
	VUKOTIC	Ivana (0.28 FTE)
Scientific Support Staff Member	LADID	Latif (0.99 FTE)
Project Support Staff Member	BRANT	Florence (0.34 FTE)
	JIMENEZ LAREDO	Juan Luis (0.29 FTE)
Doctoral Candidate	AMBROSSIO	Diego Agustin (0.33 FTE)
	ATASHPENDAR	Arash
	BRAU	Guillaume (0.2 FTE)
	BRONZI	Walter (0.78 FTE)
	BRÜHL	Manuel (0.53 FTE)
	CAPPONI	Andrea
	CHANGAIVAL	Boonyarit
	CHENAL	Massimo (0.08 FTE)
	DAUPHIN	Jérémie
	DE LA CADENA RAMOS	Augusto Wladimir (0.96 FTE)
	DELERUE ARRIAGA	Afonso (0.04 FTE)
	DERRMANN	Thierry
	DI MAIO	Antonio
	DINU	Dumitru-Daniel (0.91 FTE)
	FARJAMI	Ali
	FERNANDES	Maria
	FISCARELLI	Antonio Maria (0.84 FTE)
	GAMMAITONI	Loïc (0.83 FTE)
	GENÇ	Ziya Alper
	GREVISSE	Christian

Position	Last Name	First Name
	GUO	Siwen
	HADDADAN	Shohreh (0.29 FTE)
	HURIER	Médéric
	HÖHN	Winfried (0.93 FTE)
	IBRAHIM	Abdallah Ali Zainelabden Abdallah
	JAFARNEJAD	Sasan
	JIMENEZ	Matthieu
	KAMLOVSKAYA	Ekaterina (0.63 FTE)
	KIEFFER	Emmanuel
	KLEIN	Johannes
	LAMBERT	Christoph (0.13 FTE)
	LAMHAR	Salima (0.33 FTE)
	LI	Daoyuan
	LIU	Chao (0.21 FTE)
	LOPEZ BECERRA	José Miguel
	LOUNIS	Karim (0.53 FTE)
	MITSEVA	Asya
	MOULINE	Ludovic
	NEYENS	Gilles
	NORTA	David (0.2 FTE)
	NOTARNICOLA	Luca (0.33 FTE)
	NOTARNICOLA	Massimo (0.33 FTE)
	PARRY	Gowher (0.38 FTE)
	PEJO	Balazs
	PEREIRA	Vitor (0.71 FTE)
	PERRIN	Léo Paul (0.37 FTE)
	PIERINA BRUSTOLIN	Dayana
	SPAGNUELO	
	PILGUN	Aleksandr
	SALA	Petra (0.75 FTE)
	SAMIR LABIB	Nader (0.25 FTE)
	SANCHEZ GUINEA	Alejandro
	SKROBOT	Marjan (0.04 FTE)
	SMITH	Zachary Daniel
	SOROUSH	Najmeh (0.42 FTE)
	STOJKOVSKI	Borce (0.13 FTE)
	SU	Cui
	SUNDHARAM	Sakthivel Manikandan
	TAWAKULI	Amal (0.59 FTE)
	TORCHYAN	Khachatur (0.91 FTE)
	TORO POZO	Jorge Luis
	UDOVENKO	Aleksei
	VAN ZEE	Marc (0.16 FTE)
	VAZQUEZ SANDOVAL	Itzel
	VUKOTIC	Ivana (0.71 FTE)
	WANG	Jun

Position	Last Name	First Name
	WASIM	Muhammad Umer (0.25 FTE)
	YUAN	Qixia
	ZOLLINGER	Marie-Laure (0.42 FTE)
Senior Lecturer	KLEIN	Jacques
	LENZINI	Gabriele
Director of Interdisciplinary Center	OTTERSTEN	Björn
Student with Limited Contract	CHRISNACH	Maurice (0.11 FTE)
	CZARNUCH	Steve (0.25 FTE)
	DE SA E MATOS	Carlos Antonio (0.49 FTE)
	GASHI	Dren (0.16 FTE)
	GIFFRA	Alessandro (0.08 FTE)
	HALE	Miriam-Linnea (0.41 FTE)
	HENTGES	Laurent Philippe (0.54 FTE)
	IONESCU	Andrei-Sabin (0.08 FTE)
	JAHIC	Alen (0.13 FTE)
	JAYAKUMAR	Raji (0.33 FTE)
	KOGUE	DOMINIQUE WOLA (0.49 FTE)
	KREMER	Michel (0.08 FTE)
	KRUETANI	Maril (0.66 FTE)
	KRYVCHENKO	Roman (0.62 FTE)
	LECLERC	Joe (0.25 FTE)
	LENOU-TAGO	Cyrille (0.49 FTE)
	MAYER	Joe (0.04 FTE)
	MIETIELIEVA	Liubov (0.87 FTE)
	NIKONIENKOV	Anton (0.04 FTE)
	NOTARNICOLA	Luca (0.38 FTE)
	NOTARNICOLA	Massimo (0.38 FTE)
	OLLIVIERRE	Marcel Alexandre (0.08 FTE)
	PEREIRA DE ALMEIDA	Morgane (0.49 FTE)
	PEREIRA GONÇALVES	Mike (0.29 FTE)
	RETUNSKAIA	Tatiana (0.5 FTE)
	ROLAND	Romain (0.04 FTE)
	SCHWEICH	Tonie (0.42 FTE)
	SIMONETTO	Thibault Jean Angel (0.33 FTE)
	SOROUSH	Najmeh (0.16 FTE)
	THEVENOUX	Antoine (0.49 FTE)

Position	Last Name	First Name
	VIDONI	Tamara (0.49 FTE)
	YAMAN	Kendal (0.06 FTE)
Student with Seasonal Position	CHARPIOT	Louise (0.15 FTE)
	CHRISNACH	Maurice (0.11 FTE)
	GASHI	Dren (0.05 FTE)
	JAHIC	Alen (0.08 FTE)
	PEREIRA GONÇALVES	Mike (0.05 FTE)
	ROLAND	Romain (0.08 FTE)
	SIMONETTO	Thibault Jean Angel (0.12 FTE)
	VIDONI	Tamara (0.11 FTE)
Intern	ANDREUX	Jordan (0.32 FTE)
	CHARPIOT	Louise (0.49 FTE)
	COSTAMAGNA	Juan (0.5 FTE)
	DALOZE	Florian (0.03 FTE)
	LAMBERT	Christoph (0.5 FTE)
	PICARD	Noé (0.32 FTE)
	SCHAAL	Max (0.16 FTE)
	TANGUY	Titouan (0.22 FTE)
	TOMASONI	Mattia (0.42 FTE)
	VITELLO	Piergiorgio (0.38 FTE)

Appendix F

List of Acronyms

ComSys: Communicative Systems Laboratory
CSC: Computer Science & Communications
HPC: High Performance Computing
ILIAS: Interdisciplinary Laboratory for Intelligent and Adaptive Systems
LACS: Laboratory of Algorithmics, Cryptology and Security
LASSY: Laboratory for Advanced Software Systems
SnT: Interdisciplinary Centre for Security Reliability and Trust
UL: University of Luxembourg
FNR: Fonds National de la Recherche Luxembourg

http://csc.uni.lu

Computer Science & Communications (CSC) Research Unit
University of Luxembourg
Faculty of Science, Technology and Communication
6, avenue de la Fonte
L-4364 Esch-sur-Alzette
Luxembourg

Administrative Contact:

Danièle Flammang, Isabelle Glemot-Schroeder, Fabienne Schmitz and Nicola Wolters
Email: csc@uni.lu