CSC | Computer Science and Communications

UNIVERSITY OF LUXEMBOURG

FACULTY OF SCIENCE, TECHNOLOGY AND COMMUNICATION

Computer Science and Communications

Activity Report 2018

CSC | Computer Science and Communications

Computer Science and Communications

Activity Report 2018

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

Computer Science and Communications
Activity Report 2018

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

Editor: Christian Glodt
Release date: 2019-04-30
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 2018, including our research projects, organized events, awarded papers, visiting researchers and publications.

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 184 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^{2}DH 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

- 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 2018 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 2018 annual report for information regarding the activities and contributions of professors Briand and Ottersten and their respective groups.

Chapter 3

CSC: A Personal View

by Leon van der Torre, CSC Head 2015-2018

For three years I had the privilege of leading the computer science department of the University of Luxembourg. We received an excellent evaluation during the first scientific evaluation of departments at our young university, we moved to Belval, and we became involved in setting up the interdisciplinary space master. Here I present a personal outlook for the coming three years.

Research

The computer science department supports academic freedom and sees the pursuit of long-term scientific goals reflecting the strengths of its research groups as a crucial task. In comparison with other academic disciplines, computer science is a young, fast moving area, characterized by interdisciplinarity, which is why diversity and agility are central concerns. In fact, the department is establishing more and more links with other UL research groups, exemplified for instance by social robotics (for autism), LegalTech, Fintech, Cognitive systems, or Digital history.

Three strategic topics have been identified over the past year, relevant for research and teaching, and for each topic a new professor will be hired.

The first topic is machine learning and artificial intelligence, also related to the FSTC priority on data science. A new professorship in machine learning has been opened in CSC as well as in SnT, and they are expected to start in 2020. A complementary area of growing importance is human-centered and explainable AI. Here it is crucial to participate to European initiatives such as CLAIRE, where substantial steps have been made. In addition, there need to be even more efforts to strengthen our links with leading AI researchers in China, the US, and the rest of the world.

The second topic is space informatics and robotics. A professor position for space informatics is currently advertized, also to support the interdisciplinary space master and profit from the opportunities offered by the governmental space priority.

The third topic is human-computer interaction (HCI). A new professorship will be launched in 2020, with a focus on NLP (e.g. dialogue systems, conversational interfaces, chatbots) and/or vision (e.g image understanding, graphics, gaming, VR/AR.

A fast changing area like computer science also calls for more guest professors and researchers. One idea is to set up an AI exchange center for regular short-term guests (1 week to 1 year) to boost research and teaching in relevant emerging topics, to strengthen networking, and to prepare bigger research initiatives. In addition to the usual procedure, we started to experiment with more flexible expert contracts for visiting professors.

Finally, we should fight, either to reinstall the AFR postdocs at FNR, or to increase the number of structural postdocs substantially. In my opinion, by cancelling the AFR-Postdoc, FNR has taken away the most powerful and flexible instrument to produce excellent research in all areas.

Teaching

The teaching of the university will be evaluated during the coming years, which will be an excellent occasionn to develop and improve our teaching vision and strategies. Besides the Interdisciplinary Space Master, involving both FSTC & FDEF and starting in September 2019, the certificate in Smart and Secure ICT is extended to a full master program, and discussions about a data science master have started. After the creation of a competence center in 2018, the project of an AI Academy is gaining speed.

Another reason for paying more attention to teaching in the coming years is the increasing world-wide shortage of people educated in computer science and IT, especially in the booming areas of data science and artificial intelligence.

Our teaching programs promote interdisciplinarity, our students come both from Luxembourg and from all over the world, with English being therefore the dominant language. For our teaching strategy, we need reliable data on Luxembourg's needs in CS education at any level, we need to understand other related developments in Luxembourg such that we can influence and adapt ourselves to them. A national plan for IT-related teaching established in cooperation with the university would be useful. Last but not least, we have to identify the needs for computer-science-related teaching in other disciplines and evaluate how they are met best.

The existing teaching rooms need to undergo an external evaluation. They may need an upgrade or we may need a new teaching building with standard facilities to address our real needs. The current conditions in Belval strongly limit our possibilities.

We need a plan for CSC teaching labs, including a permanent space for the BICSlab, the labs under development for the space master, and the relations with other FSTC teaching labs.

CSC has a currently Google-sheets-based teaching management, which also guides the distribution of courses among professorial teams. It should be replaced by a flexible, university-wide system. A university-wide scheme for teaching compensations/reductions would allow to equilibrate and stabilise the relation with the ICs.

The teaching directors should have the power to do their job properly but in the spirit of collegiality.

We need a fair but flexible FSTC- or university-wide agreement on the yearly teaching load for PhD students, postdocs, and research scientists, which however respects the character of a research university.

We should do everything possible to attract better students for the academic programs but we also need to address the needs of weaker students.

Organisation

The organizational structure we adopted in March 2016 seems to be working quite well and I would therefore suggest to adopt the same structure for the departments foreseen by the law. Since CSC is responsible for research and education performed by its members, the head of the department has to take care of both, leading both, the education and the research management committee. For transparency and communication, the CSC processes and procedures are described in the CSC handbook, which may actually be used more widely. Additional support is provided by the ACCORD CSC information system, which also generates our website and our annual reports. It now forms the base of the ACCORD FSTC information system, whose possibilities are just starting to be explored.

In the history of CSC, the role and importance of the individual research groups of CSC has been growing, while the labs remain useful for collaboration and organization purposes. The budget is distributed over five budget lines, one for each of the labs and one for shared activities. The professors within a lab manage their expenses collegially. I think however it should become easier to create new labs or move from one lab to another, and that we should profit from the creation of departments to reconsider the functioning of labs.

The main challenge I see for the CSC organization is the possibility to build joint research groups with LIST, and possibly even industrial partners which could strategically support CSC and FSTC. Given the potential impact of the new UL law on the relation between FSTC and the ICs, it should be made more explicit. It certainly cannot be reduced to an often artificial difference between fundamental and applied research, because CSC is also involved in application.

A reasonable merit-based system for resource allocation has been adopted at the CSC strategy day 2018. Very roughly, we distribute structural positions in CSC in two phases. In phase 1, each professor gets a set of structural positions: in practice, all professors have currently one PhD student, and some professors have moreover a postdoc due to teaching or research merits. If these positions become open, the professor can rehire automatically. In phase 2, the remaining positions are again distributed based on merit, with further considerations for ties, but when they become available again, they will go back to CSC for redistribution according to an updated merit assessment. The process is described by several guidelines, where the merit judgment is left to the RMC and must be validated by the CSC professors. To ensure flexibility in allocating CSC resources, a more formal approach may be counterproductive. Moreover, the focus should not be on how to distribute the resources, but on attracting more resources and more generally improving the working environment and conditions of CSC research groups.

Various changes are coming due to the new university law. A university wide merit-based system will be introduced that takes into account not only research, but also teaching. This requires a university wide PI-based data collection similar to the one we have in ACCORD, also to better understand the roles and contributions of CSC professors within the ICs. The first step is to implement the ACCORD system in all research units of the FSTC. Hierarchical relations and the the hiring process are or will be clarified, in particular for permanent researcher positions. I suggest to make personal meetings of the head of department with professors into a yearly tradition. The resources associated with PEARL and ATTRACT candidates during the grant and afterwards need to be clarified. Similarly for the role of the faculty in the supervision of the secretaries and research facilitators. There also should be a place to discuss MNO related issues such as the basement labs, inconveniences like lift noise, and last but not least, office space for new professorial groups.

Chapter 4

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^{2}DH, 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)** and the **Departments of Law and Humanities**, 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, Sentiment Analysis, the use of Natural Language Processing for a ChatBot design, 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 Optimization**: 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, for example within the RoboLab or within the Robo-Football Team, and prepare them for new upcoming disciplines in Artificial Intelligence, Machine Learning, and beyond. The *2018 ILIAS Distinguished Lecture Series* of 8 talks, given by international recognized experts from industry, politics, and science, were followed by more than 160 listeners. We are in 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 5

Research Groups

5.1 Applied Crypto Group (ACG)

Head of research group: 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 2018

- ERC Advanced Grant for Jean-Sebastien Coron (2.5 M€)

Three most interesting publications in 2018

• **Jean-Sébastien Coron**: Formal Verification of Side-Channel Countermeasures via Elementary Circuit Transformations. ACNS 2018: 65-82 We describe a new technique for the formal verification of side-channel countermeasures

• Luk Bettale, **Jean-Sébastien Coron**, Rina Zeitoun: Improved High-Order Conversion From Boolean to Arithmetic Masking. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(2): 22-45 (2018) We describe a new countermeasure against side-channel attacks

• **Benoît Cogliati**, Yevgeniy Dodis, Jonathan Katz, Jooyoung Lee, John P. Steinberger, Aishwarya Thiruvengadam, Zhe Zhang. Provable Security of (Tweakable) Block Ciphers Based on Substitution-Permutation Networks. CRYPTO (1) 2018: 722-753 We improve the security bound for certain constructions of block-ciphers.

5.2 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 also has expertise in the socio-technical aspects of security and trust.

Summary of the group's achievements in 2018

2018 was a fruitful year for APSIA: three new CORE and Junior-CORE proposals were awarded. The group grew to around 25 members and is set to grow further in 2019. 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 a Crypto. The Verifiable Voting Workshop in association with Financial Crypto, founded by Ryan in 2016, had its third edition in Curacao. 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. 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.

Three most interesting publications in 2018

Becerra J., Ostrev D., **Škrobot M.** (2018) Forward Secrecy of SPAKE2. In: Baek J., Susilo W., Kim J. (eds) Provable Security. ProvSec 2018. Lecture Notes in Computer Science, vol 11192. Springer, Cham

Currently, the Simple Password-Based Encrypted Key Exchange (SPAKE2) protocol of Abdalla and Pointcheval (CT-RSA 2005) is being considered by the IETF for standardization and integration in TLS 1.3. Although it has been proven secure in the Find-then-Guess model of Bellare, Pointcheval and Rogaway (EUROCRYPT 2000), whether it satisfies some notion of *forward secrecy* remains an open question.

In this work, we prove that the SPAKE2 protocol satisfies the so-called *weak forward secrecy* introduced by Krawczyk (CRYPTO 2005). Furthermore, we demonstrate that the incorporation of key-confirmation codes in SPAKE2 results in a protocol that provably satisfies the stronger notion of *perfect forward secrecy*.

As forward secrecy is an explicit requirement for cipher suites supported in the TLS handshake, we believe this work could fill the gap in the literature and facilitate the adoption of SPAKE2 in the recently approved TLS 1.3.

Arash Atashpendar, G. Vamsi Policharla, Peter B. Rønne, **Peter Y. A. Ryan**: **Revisiting Deniability in Quantum Key Exchange - via Covert Communication and Entanglement Distillation.** NordSec 2018: 104-120

In this paper we examine how the classical notions of deniability map into the quantum realm.

This paper revisits the notion of deniability in quantum key exchange (QKE), a topic that remains largely unexplored. We provide more insight into the nature of this attack and how it extends to other constructions such as QKE obtained from uncloneable encryption. We then adopt the framework for quantum authenticated key exchange, developed by Mosca et al., and extend it to introduce the notion of coercer-deniable QKE, formalized in terms of the indistinguishability of real and fake coercer views. Next, we apply results from a recent work by Arrazola and Scarani on covert quantum communication to establish a connection between covert QKE and deniability. We propose DC-QKE, a simple deniable covert QKE protocol, and prove its deniability via a reduction to the security of covert QKE. Finally, we consider how entanglement distillation can be used to enable information-theoretically deniable protocols for QKE and tasks beyond key exchange.

No Random, NO Ransom: A Key to Stop Cryptographic Ransomware, Genç, Ziya Alper; **Lenzini, Gabriele**; **Ryan, Peter** in Giuffrida, Cristiano; Bardin, Sébastien; Blanc, Gregory (Eds.) *Proceedings of the 15th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2018)* (2018)

Cryptographic ransomware can have different disruptive strength. The worst ones, implement strong encryption, and for that they requires a good source of random numbers. With this insight, we propose a strategy to combat cryptographically strong ransomware by controlling access to the reliable source of randomness in an OS. Our strategy, tested against active real-world ransomware samples is capable to stops among others, WannaCry, Locky, CryptoLocker and CryptoWall, BatRabbit, but also nullifies NotPetya, the latest offspring of the family which has so far eluded all defenses.

5.3 BigData, Data Science & Databases (BigData)

Head of research group: Prof. Dr. Martin Theobald

The ”Big Data” group at the University of Luxembourg 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 two PhD students at the University of Luxembourg, Amal Tawakuli and Paul Meder, and one post-doctoral researcher, Dr. Vinu Venugopal. Three more PhD students will be jointly supervised in the context of a new FNR-PRIDE doctoral training unit (DTU) on “Data-Driven Computational Modeling and Applications”, of which Martin Theobald serves as a co-PI. A further PhD student, Maarten Van den Heuvel, is jointly supervised with the University of Antwerp. We currently have one open PostDoc position in the context of a new FNR-CORE project, called “BigText”, which we intend to fill in early 2019.

Our research activities continue to focus on the following three main areas:

1. Information Extraction & Knowledge-Base Construction In collaboration with the Max-Planck-Institute in Saarbruecken, 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 has been accepted for funding at the University of Luxembourg in 2017, and for which the Max-Planck-Institute kindly serves as external collaborator. A kick-off workshop for the project is planned for early 2019.

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 has been defended at the University of Zurich in 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. As a follow-up project at the University of Luxembourg, we intensively worked on the development of our new AIR asynchronous stream-processing engine over the past year, which carries over a number of concepts from TriAD to the real-time processing of continuous data streams. Initial experiments demonstrate significant performance gains over the default platforms for processing these kinds of data streams, such as Apache Spark and Flink. 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”, have been introduced into the curriculum in 2018. In addition, we organize three new modules, ”Information Management I-III”, in the newly established BiCS program of the University. The group is also intensively involved in the new “Space Master” program at the University of Luxembourg, which will be launched in the Winter Term of 2019.

Summary of the group’s achievements in 2018

Katerina Papaioannou, **Martin Theobald**, Michael H. Böhlen: Supporting Set Operations in Temporal-Probabilistic Databases. ICDE 2018: 1180-1191

Maarten Van den Heuvel, Floris Geerts, Wolfgang Gatterbauer, **Martin Theobald**: A General Framework for Anytime Approximation in Probabilistic Databases. StarAI Workshop, CoRR abs/1806.10078 (2018)

Claudia d’Amato, **Martin Theobald** (Edts.): Reasoning Web. Learning, Uncertainty, Streaming, and Scalability - 14th International Summer School 2018, Esch-sur-Alzette, Luxembourg, September 22-26, 2018, Tutorial Lectures. Lecture Notes in Computer Science 11078, Springer 2018, ISBN 978-3-030-00337-1

PhD Defenses: Katerina Papaioannou: “Negation in Temporal-Probabilistic Databases”, PhD Thesis defended at the University of Zurich in November 2018 (External Supervision)

5.4 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 2018

The COaST group counted 4 members (1 professor, 1 senior researcher, 2 PhD students) and 5 publications in 2018. The group’s research in the context of the ongoing projects CoCoDA2, CollaTrEx and Yactul, appeared in renowned academic publications and was presented at various international conferences, inclusive of a keynote talk and again winning a best paper award. Furthermore, the group managed to secure an FNR-INTER grant for the project DELICIOS. Members of the group were involved in the organization of various international scientific events and conferences such as IEEE SASO 2018, SAOS 2018, and the SOS/ABS event as part of the larger LuxLogAI summit. The VR/AR Lab, managed by the group, was represented at the FNR Researchers’ Days 2018 with a very well-received stand. The COaST group's teaching activities comprised numerous lectures and seminars in the different bachelor and master programs (BINFO, BICS, MICS, BINFO-FC) offered by the University of Luxembourg, as well as guest lecturing abroad. Johannes Klein successfully defended his PhD thesis.

Three most interesting publications in 2018

1) **Christian Grévisse**, **Jeff Meder**, **Jean Botev**, **Steffen Rothkugel**. Ontology Coverage Tool and Document Browser for Learning Material Exploration. In Proc. 13th International Conference on Digital Information Management, pp.185-190, 2018. Best Paper Award. This paper introduces an ontology visualization inclusive of a dedicated browsing function for documents associated with different concepts. The presented, visual query process overcomes the limitations of traditional file explorers, allowing for both quickly identifying relevant learning material and gaining an overview of topic coverage within the collection. Implemented as web application, the software can easily be integrated into different e-learning platforms to enhance the workflow of the users.

2) Kirstie Bellman, **Jean Botev**, Ada Diaconescu, Lukas Esterle, Christian Gruhl, Chris Landauer, Peter R. Lewis, Anthony Stein, Sven Tomforde, Rolf P. Würtz. Self-Improving System Integration – Status and Challenges. In Proc. 5th International Workshop on Self-Improving System Integration, pp.160-167, 2018. This survey article summarizes and categorizes the research efforts in self-improving system integration. This area recently emerged in response to a systems engineering trend towards the organization of open, interconnected systems integrating a large set of heterogeneous and autonomous subsystems which assess and maintain their own integration status within the overall system composition.

3) Rubén Manrique, **Christian Grévisse**, Olga Mariño, **Steffen Rothkugel**. Knowledge Graph-based Core Concept Identification in Learning Resources. In Proc. 8th Joint International Semantic Technology Conference, pp.36-51, 2018. This paper discusses a set of strategies for automatic core concept identification based a semantic representation using the open and available information in knowledge graphs. Different unsupervised weighting strategies, as well as a supervised method operating on the semantic representation, were implemented for core concept identification and evaluated against a human-expert annotated dataset of 96 learning resources extracted from MOOCs.

5.5 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). New cooperation just started at the end of 2018 with the group of Prof. Viti (Mobilab). 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.

Three important publications in 2018

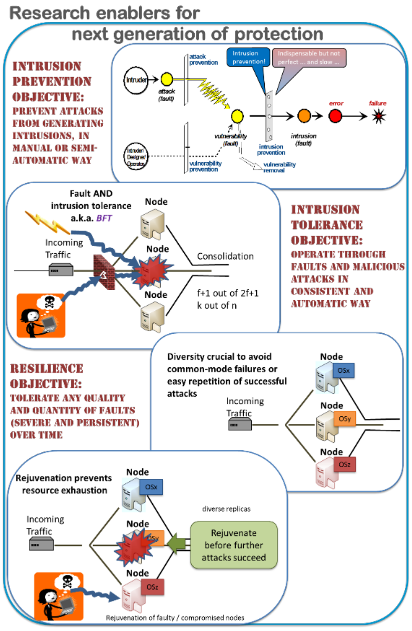
- **Franck, Christian**; **Groszschädl, Johann**; **Le Corre, Yann**; Lenou Tago, Cyrille, "Energy-Scalable Montgomery-Curve ECDH Key Exchange for ARM Cortex-M3 Microcontrollers", in Proceedings of the 6th International Conference on Future Internet of Things and Cloud Workshops (W-FICLOUD 2018) (2018)
- M. Tomasoni, **A. Capponi**, C. Fiandrino, D. Kliazovich, F. Granelli, **P. Bouvry**, "Why energy matters? Profiling energy consumption of mobile crowdsensing data collection frameworks", in Pervasive and Mobile Computing, Volume 51, 2018, Pages 193-208, ISSN 1574-1192,
- P. Vitello, **A. Capponi**, C. Fiandrino, P. Giaccone, D. Kliazovich, **U. Sorger**, & **P. Bouvry**, "Collaborative Data Delivery for Smart City-oriented Mobile Crowdsensing Systems", in IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, UAE, 2018.

5.6 Critical and Extreme Security and Dependability (CritiX)

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

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 operation, 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 midterm 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 2018


Research enablers for
next generation of protection
INTRUSION PREVENTION OBJECTIVE:
PREVENT ATTACKS FROM GENERATING INTRUSIONS, IN MANUAL OR SEMI-AUTOMATIC WAY
Intruder
attack (fault)
attack prevention
Intrusion prevention!
Indispensable but not perfect ... and slow ...
vulnerability (fault)
intrusion prevention
intrusion (fault)
error
failure
Intruder/ Designer/ Operator
vulnerability prevention
vulnerability removal
Fault AND intrusion tolerance a.k.a. BFT
Incoming Traffic
Node
Node
Node
Consolidation
f+1 out of 2f+1
k out of n
INTRUSION TOLERANCE OBJECTIVE:
OPERATE THROUGH FAULTS AND MALICIOUS ATTACKS IN CONSISTENT AND AUTOMATIC WAY
RESILIENCE OBJECTIVE:
TOLERATE ANY QUALITY AND QUANTITY OF FAULTS (SEVERE AND PERSISTENT) OVER TIME
Diversity crucial to avoid common-mode failures or easy repetition of successful attacks
Incoming Traffic
Node
OSx
Node
OSy
Node
OSz
Rejuvenation prevents resource exhaustion
Incoming Traffic
Node
OSx
Node
OSy
Node
OSz
diverse replicas
Rejuvenate before further attacks succeed
Rejuvenation of faulty / compromised nodes

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. The INTEL partnership is reaching cruise speed, with very promising prospects, after a successful workshop in Portland, US. Informal collaboration with LCSB continues, having good perspectives. Several papers (reported in Orbilu) have been published, some of which giving visibility to CritiX through presentations in conferences. A significant highlight was the organisation of the IEEE/IFIP DSN 2019 conference in Luxembourg, of which PJV was General Chair, which further put Luxembourg, UL and SnT on the map of systems and networks dependability and security. Some other actions also took place, amongst which: IFIP WG10.4 Winter Workshop, Goa, IN; Debate on Data Privacy at the Portuguese Parliament, Lisboa, PT; Distinguished Lecture, TU Darmstadt, DE; ICRI-CARS Annual Workshop, Intel, Portland, US; Keynote, ADA Europe, Lisboa, PT; Keynote, DSN BCRB , Luxembourg, LU; IFIP WG10.4 Summer Workshop, Clervaux, LU; Invited talk at CREW@QRS 2018, Lisboa, PT; Debate with Luxembourgish MEPs, Belval, LU; FNR Workshop on National Research Priorities, Schuttrange, LU.

Focused Research Activity results from 2018 (relevant papers can be found in the group's ORBILU web page):

The group had several papers published, amongst which ten CORE A or A* papers, in the areas of: Design of novel BFT algorithms; R/T Byzantine resilient communication and consensus; Resilient software defined networking (SDN);

BFT protocol verification based on proof assistants; Enhancements to ITP theory and practice; Early DNA long-reads filtering and alignment with masked info; Architectures for blockchain threat mitigation and resilience. - One fundamental result led to IP protection initiatives, through patent application. Some group members, after a successful FNR supported Pathfinder, were pleased to see a succeeding PoC, GenoMask, accepted. That project lies substantially on IP protection secured earlier. - PJV mentored the participation of SnT@LU in several proposals for the recent call for Cybersecurity Competence Networks in H2020. Luxembourg, by virtue of this dynamics, is extremely well positioned, participating to three of the approved four Networks in this phase. CritiX is involved in two of them.

5.7 Critical Real-Time Embedded Systems (CRTES)

Head of research group: Associate 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 2018

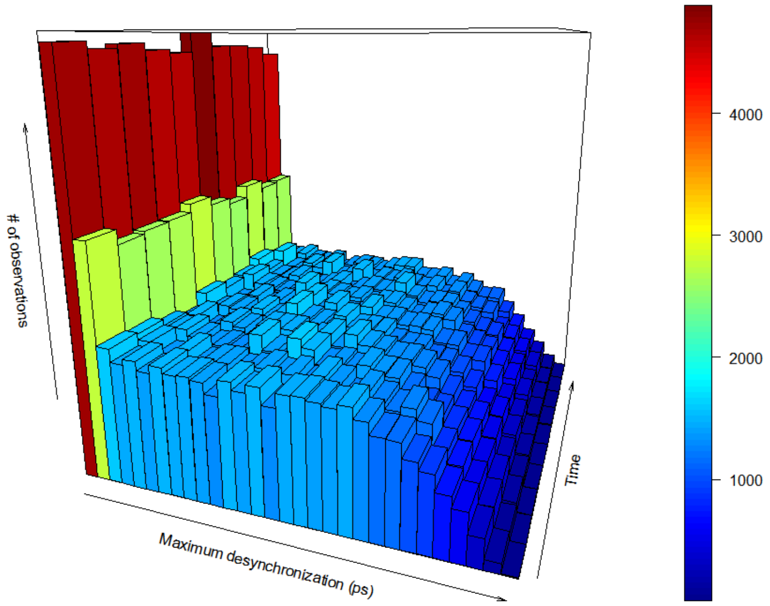
In 2018 the CRTES group was made up of 4 members (1 associate-professor, 1 postdoc, 2 PhD students) and had 9 publications published or accepted, including 4 journal papers. In the field of Model-Driven Engineering (MDE) for critical embedded systems, we completed a design framework based on timing tolerance contracts and co-simulation to specify and verify the satisfaction of both control engineering and software engineering requirements. This approach based on model interpretation has for main advantage that a controller model, verified in the design phase, can be then executed on the target hardware with the exact same temporal behavior and control performance as predicted at the design stage. This latter contribution is the outcome of the Phd thesis of S. M. Sundharam, to be defended in March 2019. Most of our work was in the field of real-time communication systems with contributions about well-established networks like CAN, prototype networks like CAN XR, or emerging protocols that are important from an industrial viewpoint like the protocols developed in the IEEE Time Sensitive Networking (TSN) working group. In particular, in a joint work with Renault, we proposed a new traffic shaping policy that has shown on realistic case-studies to be as efficient as the standardized Credit-Based Shaper without the need for dedicated hardware components. In a joint study with CNES, we performed an experimental assessment of the reliability of the TTEthernet network considered for use in next-generation orbital space launchers, and shown its ability to maintain communication under realistic error conditions. This work won a best paper award at the ERTS'2018 conference. Prof. Navet was in the defense board of 1 Phd thesis, was in 3

Phd supervisory committees and contributed to CSC teaching programs in particular by facilitating with the other group's members 4 new courses this year, both at the Bachelor (professional and academic) and Master levels. Dr. Hu co-organized the WiP session of WFCS, the main IEEE conference in industrial communication systems, and was member of two program committees.

Three most interesting publications in 2018

1) **S. M. Sundharam, N. Navet**, S. Altmeyer, L. Havet, ”A Model-Driven Co-design Framework for Fusing Control and Scheduling Viewpoints”, special issue “Design and Implementation of Future CPS”, Sensors, 18(2), MDPI, 2018. A design framework and development environment based on the CPAL modeling language that addresses the gaps between control and real-time software engineering, and allows validate both functional and non-functional requirements in the early design phases.

2) L. Fejoz, B. Régnier, P. Miramont, **N. Navet**, “Simulation-Based Fault Injection as a Verification Oracle for the Engineering of Time-Triggered Ethernet networks”, Best paper award, Proc. Embedded Real-Time Software and Systems (ERTS 2018), Toulouse, France, January 31-February 2, 2018. Experimental assessment of the TTEthernet protocol clock synchronization precision and overall robustness by simulation based fault-injection (right-hand side figure: variability over time of the distribution of node clock desynchronization).



3) **N. Navet**, J. Migge, J. Villanueva, M. Boyer, ”Pre-shaping bursty transmissions under IEEE802.1Q as a simple and efficient QoS mechanism”, Proc. WCX18: SAE World Congress Experience, Detroit, Mi, April 2018. Extended version to appear in SAE International Journal of Passenger Cars—Electronic and Electrical

Systems. A fully software-implemented traffic shaping strategy for Ethernet allowing a drastic reduction of the communication latencies for best-effort and video streams while enabling meeting the timing constraints for the critical part of traffic (e.g., dynamics control, ADAS).

5.8 CryptoLux team

Head of research group: Prof. Dr. Alex Biryukov

The CryptoLux group is part of both LACS/CSC/FSTC 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. CryptoLux is also doing research on privacy. Information about the group is available at http://cryptolux.org.

Summary of the group's achievements in 2018

In 2018 the CryptoLux group consisted of 9 members (1 professor, 1 senior researcher (shared), 3 postdocs, 4 PhD students), who published a total of 8 papers in major international journals and conference proceedings. In summer 2018 the group has started a new FNR CORE project FinCrypt (Financial Cryptography). Research highlights in 2018 were publication of a paper on whitebox cryptography, work on a new lightweight cipher, authenticated encryption for the upcoming NIST competition. Professor Biryukov served on the technical program committee of numerous conferences including top security conferences like Eurocrypt , ACM CCS, Usenix ATC and on the editorial board of the IACR journal for Transactions on Symmetric Cryptography (ToSC). CryptoLux members taught various courses in the bachelor and master programs and supervised student projects. The team organized a workshop about cryptography and blockchain for kids at the public outreach event Researcher's Days 2018 in Esch-Belval.

The three most interesting achievements in 2018

1. Léo Perrin has won the best Ph.D. thesis award for University of Luxembourg (Rolf Tarrach prize) 2018 His thesis was in the framework of FNR CORE project ACRYPT, and dealt with design and analysis of lightweight cryptography. Leo currently works in cryptography research group at Inria, Paris.

2. Aleksei Udovenko presented his paper "Attacks and Countermeasures for White-box Designs" at ASIACRYPT, 2018 In the traditional symmetric cryptography, the adversary has access only to the inputs and outputs of a cryptographic primitive. In the white-box model the adversary is given full access to the implementation. He can use both static and dynamic analysis as well as fault analysis in order to break the cryptosystem, e.g. to extract embedded secret key. Implementations secure in such model

have many applications in industry. However, creating such implementations turns out to be a very challenging if not an impossible task. In this paper we investigate possibility possibility to use masking against DCA attacks and also present multiple generic attacks against masked white-box implementations. As a result, we deduce new constraints that any secure white-box implementation must satisfy. We suggest partial countermeasures against the attacks. Some of our attacks were successfully applied to the WhibOx 2017 challenges.

3. Qingju Wang presented her paper at CRYPTO, 2018 ”Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly” The cube attack is an important technique for the cryptanalysis of symmetric key primitives, especially for stream ciphers. Aiming at recovering some secret key bits, the adversary reconstructs a superpoly with the secret key bits involved, by summing over a set of the plaintexts/IV which is called a cube. Traditional cube attack only exploits linear/quadratic superpolies. This limit was first overcome by the division property based cube attacks proposed by Todo et al. at CRYPTO 2017. In this paper, we introduced several techniques to improve the division property based cube attacks by exploiting various algebraic properties of the superpoly. As an illustration, we apply our techniques to attack the initialization of several round-reduced ciphers: Trivium, Kreyvium, Grain-128a and Acorn.

5.9 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 2 members in 2018: Qin Ma (research scientist, half-time) and Christian Glodt (research and development specialist). The research group explores fundamental questions in the area of model-driven engineering but also interests itself in concrete applications (e.g., enterprise architecture and smart grids).

Summary of the group’s achievements in 2018

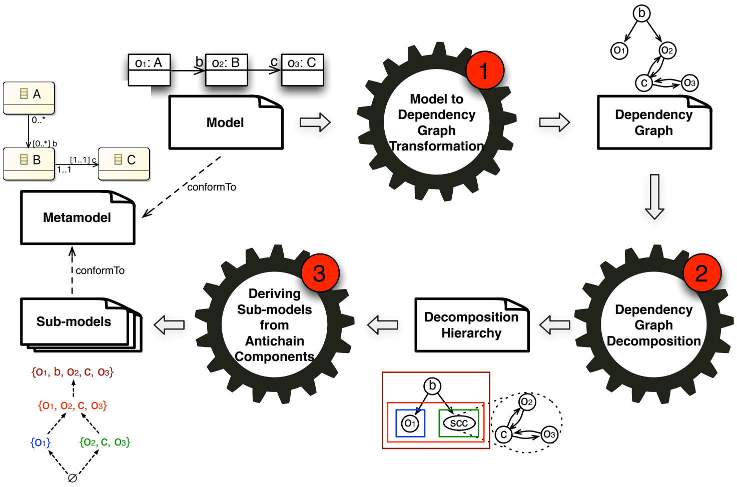
Pierre Kelsen has initiated this year a new research thread on lightweight modeling. The idea for this research is born out of the realization that most of the existing modeling frameworks require a steep learning curve due to the complexity of the involved languages and tools. Publications and a tool related to our new approach are expected for the coming year 2019. Qin Ma collaborated with other group members and colleagues from LIST and the University of Duisburg-Essen in the field of model driven software engineering, enterprise architecture, and conceptual modeling, resulting in four publications. Qin Ma was a PC member of the WFCS 2018 conference. Qin Ma also participated in the teaching of lab sessions for the ”Programming Fundamentals 1” course in the BICS program. Christian Glodt improved ”Accord”, the research information database used by the CSC. He participated in a leading role in the implementation of a new information management system for the ”Master in Information and Computer Sciences” degree, and also participated in the organisation of lab sessions for the ”Programming Fundamentals 1” course in the ”Bachelor in Computer Science” degree. He did initial development of a language support plugin for the ”Atom” editor for a new lightweight modeling language.

Three most interesting publications in 2018

1. **Qin Ma** and **Pierre Kelsen**. ”Decomposing Models Through Dependency Graphs”. In Proceedings of the 12th IEEE International Symposium on Theoretical Aspects of Software Engineering, pp. 138-143, 2018. We propose a model decomposition technique for reducing model size and consequently complexity by exploiting the notion of dependency graphs. Compared to its predecessor, this new model decomposition technique is more effective in terms of both the number of derived sub-models (more), the size of sub-models (finer), and the quality of sub-models (better).

2. Monika Kaczmarek-Heß, Sybren de Kinderen, **Qin Ma**, and Iva´n S. Razo-Zapata. “Modeling in Support of Multi-Perspective Valuation of Smart Grid Initiatives”. In Proceedings of the 12th IEEE International Conference on Research Challenges in Information Science, pp. 1-12, 2018. We identify requirements towards an approach for understanding the value proposition of a smart grid initiative, and propose a first step towards such an approach in the form of a landscape of modeling languages complemented by a process model for valuation. We evaluate the proposed approach, among others, by applying it to a blockchain-based initiative in the energy sector.

3. Iva´n S. Razo-Zapata, Eng K. Chew, **Qin Ma**, Loïc Gammaitoni, and Henderik Proper. ”Enabling Value Co-Creation in Customer Journeys with VIVA”. This paper has received the best paper award at the International Conference on Service Science and Innovation (2018). We present VIVA, a domain specific visual language to design value co-creation for a given business from a customer perspective. We validate VIVA’s abstract syntax and concrete syntax using Lightning, which leads to the improvement of VIVA as well as to the definition of constraints governing the use of VIVA.



5.10 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 centers and research units: like 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 the formal sciences. In 2018, ICR also started to develop Space AI, which will contribute to the UL priority of space education and research. Its Space AI subgroup currently involves 4 people.

Summary of the group's achievements in 2018

ICR hosted 21 researchers: 1 full prof., 3 visiting and 1 guest prof., 1 senior researcher, 6 resident and 4 visiting postdocs, 3 local PhD students and 2 LAST-JD PhD students. MIREL (Mining and Reasoning with Legal Texts), a H2020-MSCA-RISE network coordinated by ICR, entered its 3rd year and brought a number of fruitful short- to longterm exchange activities. ICR continued to be involved in the ERASMUS+ exchange network LAST-JD (Joint International Doctoral Degree in Law, Science, and Technology), with 3 completed PhDs in 2018, supplemented by 1 PhD in socio-spatial ontology (Smart Cities), in a cotutuelle with Turin. ICR has been strongly involved in creating "Legal Informatics Luxembourg (LuxLI)", a community of legal and ICT experts to foster interdisciplinary collaboration. It builds a bridge between industry and specialized workforce, e.g. by supporting LegTech start-ups and promoting industrial partnerships for PhD students. ICR also helped to create a local chapter of “Legal Hackers”, a global initiative of lawyers, policymakers, designers, technologists, and academics at the intersection of law and technology. ICR organized the First International Workshop on Legal Design as Academic Discipline, co-located with JURIX. The main highlight 2018 was the ”Luxembourg Logic for AI Summit - LuxLogAI 2018 (Sep 17-26, Campus Belval, FNR-RESCOM), with a focus on “Responsible AI”. It attracted 220 registered participants from academia, industry and public institutions, with 11 high-ranked invited speakers, 101 regular research talks/papers and 12 tutorials, organised in 11 diverse sub-events (e.g. the 2nd Joint Int. Conf. on Rules and Reasoning (RuleML+RR 2018), the 4th Global Conf. on AI (GCAI 2018), the 14th Reasoning Web Summer School (RW 2018), or AI and Art). A public high-level panel discussion on the future of European AI, at KPMG Luxembourg, was a huge success. The AI-Robolab presented “My life as a robot” at the Researchers’ day, using virtual reality to explain robot perception. The success story of the ICR spinoff LuxAI (social robotics, e.g. the QT robot for autistic children) went on with the CES innovation award and an IEEE-article. ICRs editorial achievements include the Handbook on Normative Multiagent Systems, the Handbook on Formal Argumentation, as well as a new textbook “Introduction to Deontic Logic and Normative Systems”. The collaboration with our longterm visitor Prof. D. Gabbay opened several very promising perspectives for increasing the international role of ICR and Luxembourg in the areas of Logic and AI. Together with the guest professor Prof. B. Liao from Zhejiang University (FNR Mobility), ICR started furthermore to lay the foundations for a close collaboration with this top university. Last but not least, our DEON 2018 paper received the best paper award.

Three interesting publications in 2018

C. Benzmüller, **A. Farjami**, **X. Parent**. A Dyadic Deontic Logic in HOL. DEON 2018: 33-49, Utrecht, NL.

G. Pigozzi, **L. van der Torre**. Arguing about constitutive and regulative norms. Journal of Applied Non-Classical Logics 28(2-3): 189-217, 2018.

A. P. Costa, L. Charpiot, **F. J. R. Lera**, P. Ziafati et al. More Attention and Less Repetitive and Stereotyped Behaviors using a Robot with Children with Autism. 27th IEEE International Symposium on Robot and Human Interactive Communication, RO-MAN 2018: 534-539 , Nanjing, China.

5.11 Knowledge Discovery and Mining (MINE)

Head of research group: Prof. Christoph Schommer

The MINE research group follows an interdisciplinary research approach and is embedded in an area that primarily addresses the use of Artificial Intelligence systems. In this context, we cooperate with colleagues from the C2DH (Prof. Fickers, Prof Majerus), the Dept of Linguistics (Prof. Gilles), and the Dept of Cognitive Science (Prof Greiff, Prof Koenig) as well as with industrial partners (RTL, KPMG). MINE is a small group, consisting of 6 members (1 prof, 2 PostDocs, 3 PhD candidates), whose research targets fields like Artificial Chatbots, Sentiment Analysis, Topic Modeling and other Machine Learning applications. A central focus lies in the education of students on Bachelor, Master, and Doctoral Levels with courses on Machine Learning, Knowledge Discovery, Data Science, Information Retrieval and Leanring, and Databases. Current research projects are: STRIPS (with RTL), PERSEUS, TMAA (Topic Modeling of Australian Aborigines Literature), and ACC (Artificial Chatbots and Companions).

Selected Achievements in 2018

The 2018 highlights concern both research and teaching aspects as well as a diverse outreach activities for the research community as well as for the Luxembourgish society. In April 2018, Sviatlana Höhn and Christoph Schommer have founded the ”Artificial Chatbots and Companions” (ACC) lab and have established a Meetup group with currently more than 150 members, mostly from Luxembourg industry. Regular meetings have shown a strong commercial interest in our work and particularly in Artificial Intelligence. Furthermore, Sviatlana Höhn has organised an open debate titled ”Artificial Intelligence: Truth or Dare”, which has been a workshop that was held during the LuxAI conference in September 2018. She also has given a workshop titled ”Build a Chatbot in 90 minutes”, which was a hands-on workshop for school pupils of the Lycée Technique, Esch-sur-Alzette. Both Delano (”Riding the Chatbot Train”, September 2018) and the Tageblatt (”Künstliche Intelligenz: Sophia, Watson, und der Hype”, 10 September 2018) have reported about her work. Prof Schommer has given a speech within the Biergerforum event, which was organised by the Luxemburgische Zentrum für Politische Bildung, about ”Roboter und Künstliche Intelligenz - Forum citoyen avec des députés européens ” and has participated as expert to the Séminaire du Bureau du Parlament Européen au Luxembourg regarding ”Le RGPD: une stratégie de gouvernance au-delà de la protection?”. Furthermore, he has led the ILIAS Lab and has been also instrumental in the success of the Distinguished Lecture Series, hosting worldwide guests. Prof Schommer was invited as Guest Lecturer at the University of Potsdam (Summer 2018) as well as is now a permanent Guest Lecturer at the Freie Universität Berlin. He has reviewed more than 40 papers at 12 international conferences and has - among accepted papers at research conferences - published several articles in the Luxemburger Wort (”Die Maschinen nach menschlichem Vorbild”, 31 August 2018 as well as ”Ein europäisches CERN für die Künstliche Intelligenz”, 22/23 Dezember 2018). Finally, he successfully led one of his doctoral students to the PhD degree. Also, he has been interviewed by Radio 100,7 about the industrial future in the scope of Artificial Intelligence. Prof Schommer is an elected member of the Faculty Council, a member of the Management Board of the Doctoral Training Unit “Digital History and Hermeneutics”, and a full member of “Legal Informatics”, a Europe-wide project. He is strongly supporting CLAIRE, a European initiative to foster a CERN for the Artificial Intelligence.

Selected Publications in 2018

- Bustan S, Gonzalez-Roldan A, **Schommer, C.**, Kamping S, Löffler M, Brunner M, Flor H, and Anton, F. (2018, July). Psychological, cognitive factors and contextual influences in pain and pain-related suffering as revealed by a combined qualitative and quantitative assessment approach. Journal PLoS ONE.
- **Guo, S.**, **Höhn, S.**, Xu, F., and **Schommer, C.** (2018). PERSEUS: A Personalization Framework for Sentiment Categorization with Recurrent Neural Network. International Conference on Agents and Artificial Intelligence, Funchal 16-18 January 2018 (pp. 9).
- **Guo, S.**, and **Schommer, C.** (2018, September 10). A Bilingual Study for Personalized Sentiment Model PERSEUS. Paper presented at PhD Forum at the European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD), Dublin, Ireland.
- Vijayakumar, B., **Höhn, S.**, and **Schommer, C.** (2018). Quizbot: Exploring For-

mative Feedback with Conversational Interfaces. In Vijayakumar, B., Höhn, S. & Schommer, C. Springer.
- **Kamlovskaya, E., Schommer, C.**, and Sirajzade, J. (2018). A Dynamic Associative Memory for Distant Reading. International Conference on Artificial Intelligence Humanities, Book of Abstracts. Seoul, Korea: Chung-Ang University.

5.12 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. Our group focuses on methods and tools for Software Engineering, DevOps and Artificial Intelligence in order to improve the quality of IT systems. Our methods and tools are developed using sound scientific basis. We develop open source tools to support our languages and to allow for research collaboration or technology transfer with industrial partners. Our aim is to offer novel and efficient approaches for the engineers to ensure system development and deployment. Specific fields are currently under important development: - DevOps and Agile methods - software engineering methods and tools for neural networks engineering - software engineering methods and tools for ecological cyber physical systems.

Highlights in 2018

The group has played a key role in the management of, and teaching support for the first and second-year students of the recently opened Bachelor in Computer Science (BiCS) at the University of Luxembourg. In this context, the BiCS Management Tool (BMT) has been improved by the team to ease the management of the projects students perform every semester along with either staff of the university or external collaborators. Another highlight, was the the successful completion of the first BiCS Challenge, which had a two-fold goal: spread the voice about the BiCS while attracting motivated and talented high-school students to follow such an educational track. A number of industrial sponsors have supported this event by providing prices for the students. Last but not least, the BicsLab, a R&D student laboratory has been setup with the supervision of a number of student semester projects around software, greenware, and senseware; a first industrial partnership agreement has been signed resulting in 2 semester projects in the company; a BiCS students voluntary cell has been started around positive IT solutions.

Three most interesting publications (or other achievements) in 2018

1. **Ries, Benoît**; **Capozucca, Alfredo**; **Guelfi, Nicolas**. "Messir: A Text-First DSL-Based Approach for UML Requirements Engineering (Tool Demo)".

Proceedings of the 11th ACM SIGPLAN International Conference on Software Language Engineering SLE'18. This paper presents the design and tool-support of Messir, our approach developed during the last years by our group, centered on textual DSLs supported by Excalibur, our open-source UML requirements engineering tool. The novelty of our approach is the actual integration in a single workbench of textual DSLs richly covering the requirements and analysis phases; the read-only visualisation of UML requirements views; the generation of scientific requirements analysis documents in LaTeX; and the formal simulation of test cases requirements.

2. **Capozucca, Alfredo**; **Guelfi, Nicolas**; **Ries, Benoît**. "Design of a (yet another?) DevOps course", In J.-M., Bruel, M., Mazzara, & B., Meyer (Eds.), Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment (Revised Selected Papers). Cham, Switzerland: Springer. This paper presents the design of an academic master-level course aimed at DevOps. The specification of the course design is done using the SWEBOK Guide and Bloom's taxonomy to enhance the quality of the course design specification, and ease its assessment once delivered.

3. Yasir Imtiaz Khan, Alexandros Konios, and **Nicolas Guelfi**. 2018. "A Survey of Petri Nets Slicing". ACM Computing Surveys 51, 5, Article 109 (November 2018), 32 pages. In this article, different slicing techniques are studied along with their algorithms. A noteworthy use of this survey is for the selection and improvement of slicing techniques for optimizing the verification of state event models.

5.13 Parallel Computing and Optimisation Group (PCOG)

Head of research group: Prof. Dr. Pascal Bouvry
Deputy Head of research group: Dr. Grégoire Danoy

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/.

Summary of the group's achievements in 2018

In 2018, the PCOG team counted 14 members (1 professor, 2 senior researchers, 3 postdocs, 8 PhD students) and produced a total of 23 publications (1 book (published by Dunod), 6 journal articles, 1 book chapter, 14 conference articles, 1 report). 1 PhD student co-supervised by Prof. Bouvry successfully defended his thesis in 2018, as part the H2020 Erasmus+ LAST-JD “Joint International Doctoral Degree in Law, Science and Technology”. In the context of the “Digital Trust in Smart ICT” project conducted in collaboration with the Institut luxembourgeois de la normalisation, de l’accréditation, de la sécurité et qualité des produits et services (ILNAS), PCOG and ILNAS have published a joint white paper on “Data Protection and Privacy”. The latter was officially presented during the World Standards Day on October 12, 2018.

PCOG acquired three fundings in the field of drone swarming in 2018. The 3-year HUNTED (Heterogeneous multi-swarms of UNmanned auTonomous systEms for mission Deployment) research project is the first project funded by the Office of Naval Research Global (ORNG – US Navy) in Luxembourg. Two technology transfer projects have also been awarded, AURORA (unpredictable Uav swaRms fOr surveillance) and SIMMS (Swarms of Intelligent Missions systeMS) funded respectively by the FNR Pathfinder and Proof-of-Concept programs. PCOG additionally obtained one H2020 project: PRACE-6IP. This project is the 6th implementation phase of the “Partnership for Advanced Computing”, which is a permanent pan-European High Performance Computing service.

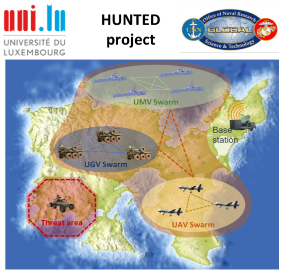
PCOG also received two awards in 2018. Pascal Bouvry and Grégoire Danoy received an award from the ONRG (US Navy) for their research on drone swarming and Abdallah Ibrahim, Sébastien Varrette and Pascal Bouvry received a best paper award at the IEEE ICOIN 2018 conference.

PCOG team members taught in several Bachelor, Master and PhD programs (BINFO, Bachelor en Sciences de la Vie, MICS, Doctoral School in Computer Science). PCOG is also involved in the University Certificate “Smart ICT for business innovation” in collaboration with the ILNAS.

PCOG is in charge of the management of the High-Performance Computing (HPC) of the University, those developments as well as the associated expert IT team managing and supporting it, are led by Pascal Bouvry (”Chargé de Mission auprès du Recteur pour la stratégie HPC”) and Sébastien Varrette (Deputy head HPC for research).

Three most interesting publications (or other achievements) in 2018

1) ONRG Award and HUNTED Project



PCOG’s research on swarms of unmanned autonomous systems has been recognised by a prestigious award from the Office of Naval Research Global (ONRG – US Navy). The ONRG also granted a 3-year funding for the HUNTED (Heterogeneous multi-swarms of UNmanned auTonomous systEms for mission Deployment) project.

2) The High-Performance Computing platform of the UL

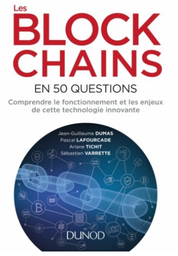
Managed by Prof. Bouvry and Dr. Varrette, it is currently the largest facility of this type in Luxembourg (after GoodYear's industrial R&D Center). End of 2018, the HPC platform featured a computational power of 1062 TFlops (11084 computing cores) and 9.8 PBytes for storage (incl. 1 PB for backups), serving 469 users.

3) Best paper award at IEEE ICOIN 2018

Abdallah Ibrahim, Sébastien Varrette and Pascal Bouvry received a best paper award at the 32nd International Conference on Information Networking (ICOIN) for their article "*PRESENCE: Toward a Novel Approach for Performance Evaluation of Mobile Cloud SaaS Web Services*".

4) Book "Les blockchains en 50 questions", published by Dunod

Jean-Guillaume Dumas, Pascal Lafourcade, Ariane Tichit and Sébastien Varrette published with Dunod a book (in French) explaining the distributed ledger concept and their impact for our society under the form of 50 answered questions.



Les BLOCK CHAINS
EN 50 QUESTIONS
Comprendre le fonctionnement et les enjeux de cette technologie innovante
Jean-Guillaume DUMAS
Pascal LAFOURCADE
Ariane TICHIT
Sébastien VARRETTE
DUNOD

5.14 Proactive Computing

Head of research group: Prof. Dr. Denis Zampuniéris

This small group, counting 3 members (1 professor, 1 PhD students, 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 2018

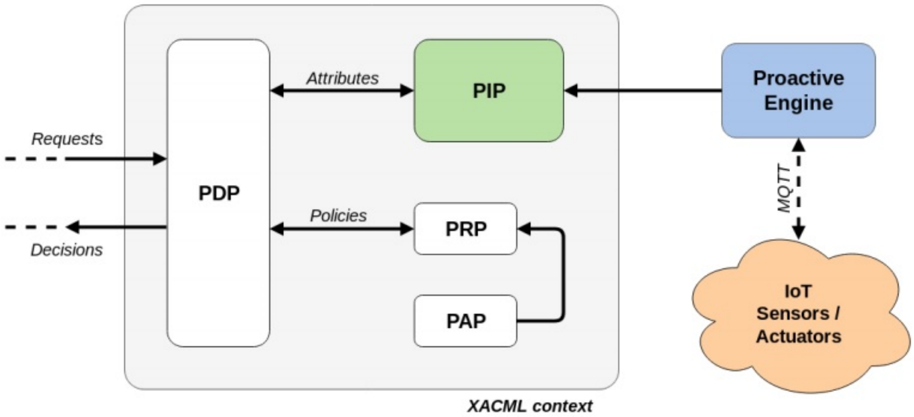
Apart from their regular research and publication work and their participation in teaching programmes offered by our Faculty, the group members welcomed and supervised several students (local or from universities abroad) in internship for their Bachelor or Master thesis.

Most interesting publications in 2018

1. **Gilles Neyens** and **Denis Zampuniéris**. A rule-based approach for self-optimisation in autonomic eHealth systems. In Proc. Workshop on "Self-Optimisation in Autonomic & Organic Computing Systems" in 31st International Conference on Architecture of Computing Systems, Braunschweig (Germany), 2018. Advances in machine learning techniques in

recent years were of great benefit for the detection of diseases/medical conditions in eHealth systems, but only to a limited extend. In fact, while for the detection of some diseases the data mining techniques were performing very well, they still got outperformed by medical experts in about half of the tests done. In this paper, we propose a hybrid approach, which will use a rule-based system on top of the machine learning techniques in order to optimise the results of conflict handling. The goal is to insert the knowledge from medical experts in order to optimise the results given by the classification techniques.

2. Noé Picard, Jean-Noël Colin and **Denis Zampuniéris**. Context-aware and Attribute-based Access Control Applying Proactive Computing to IoT System. In Proc. International Conference on Internet of Things, Big Data and Security, Madeira (Portugal), 2018. ABAC allows for high flexibility in access control over a system through the definition of policies based on attribute values. In the context of an IoT-based system, these data can be supplied through its sensors connected to the real world, allowing for context-awareness. However, the ABAC model alone does not include proposals for implementing security policies based on verified and/or meaningful values rather than on raw data flowing from the sensors. Nor does it allow to implement immediate action on the system when some security flaw is detected, while this possibility technically exists if the system is equipped with actuators next to its sensors. We show how to circumvent these limitations by adding a proactive engine to the ABAC components, that runs rule-based scenarios devoted to sensor data pre-processing, to higher-level information storage in the PIP, and to real-time, automatic reaction on the system through its actuators when required.



5.15 Security and Networking Lab (SECAN-Lab)

Head of research 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.

Summary of the group's achievements in 2018

Beside its 20 externally funded projects running currently, SECAN-Lab had five new projects starting that focused on the group's core areas, including security and privacy in data communication and vehicular communication for traffic management. Moreover, the group head together with senior researchers are involved in the supervision of seven ongoing PhD projects. In 2018, SECAN-Lab continued its collaboration with the car manufacturer Honda within the framework of Honda HIGE Grant and focussed on a research in the area of in-car communication. Most notably, team members provide expertise in the buliding of a real automotive testbed for in-car communications based on APU PC Engines and a real testbed for V2X communications based on ALIX PC Engines. In 2018, SECAN-Lab was involved in various international scientific conferences and organized a workshop on advanced tools to access and mitigate the criticality of ICT components and their dependencies over critical infrastructures bringing together different partners 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 (Thierry Derrmann) successfully defended his thesis and graduated.

Three most interesting publications (or other achievements) in 2018

1. Rod McCall, Fintan McGee, Alexander Mirnig, Alexander Meschtscherjakov, Nicolas Louveton, **Thomas Engel**, Manfred Tscheligi, A taxonomy of autonomous vehicle handover situations, Transportation Research Part A: Policy and Practice. The paper provides a taxonomy of different forms of autonomous vehicle handover situations. It covers scheduled, emergency and non-emergency handovers and it differentiates between system and driver initiated handovers. The purpose is to examine how the system and driver are responsible for different stages in the transition timeline, i.e., first alert, handover phase, and return to automated control (handback). This is examined from the perspective of SAE levels in comparison to aspects drawn from situational awareness. The work is complemented by analysis drawn from current practice within the insurance industry and interviews with insurers. The result is a closer examination of system and driver responsibility which is independent of but includes SAE levels with respect to specific handover situations. It also identifies gaps between the current legal liability for accidents when compared to aspects such as the situational awareness requirements placed on driver under different driving conditions.

2. Rocio Lopez Perez, **Florian Adamsky**, **Ridha Soua**, **Thomas Engel**, Machine Learning for Reliable Network Attack Detection in SCADA Systems, 7th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom), July 31th - August 3rd, 2018, New York, USA. Traditional Intrusion Detection Systems (IDSs) cannot detect attacks that are not already present in their databases. Therefore, we assessed Machine Learning techniques for intrusion detection in SCADA systems using a real data set collected from a gas pipeline system and provided by the Mississippi State University. We have used SVM, RF and LSTM to implement diverse IDS classifiers. A complete comparison between these algorithms was provided along with the random hyper-parameters search results. Contrary to the state of the art studies, the use of the test set accuracy, precision, recall and F1 score allowed us to assess correctly and comprehensively their performances.

3. **Asya Mitseva**, **Andriy Panchenko**, **Thomas Engel**, The state of affairs in BGP security: A survey of attacks and defenses, Computer Communications Volume 124, June 2018, Pages 45-60. The Border Gateway Protocol (BGP) is the de facto standard interdomain routing protocol. Despite its critical role on the Internet, it does not provide any security guarantees. In response to this, a large amount of research has proposed a wide variety BGP security extensions and detection-recovery systems in recent decades. Nevertheless, BGP remains vulnerable to many types of attack.

In this journal paper, an up-to-date review of fundamental BGP threats is conducted and then a methodology for evaluation of existing BGP security proposals is presented. Based on this, we introduce a comprehensive and up-to-date survey of proposals intended to make BGP secure and methods for detection and mitigation of routing instabilities. Last but not least, we identify gaps in research, and pinpoint open issues and unsolved challenges.

5.16 Security and Trust of Software Systems (SaToSS)

Head of research group: Prof. Sjouke Mauw

Since its establishment in 2007, the SaToSS group focuses on formalizing and applying formal reasoning to real-world security problems. The SaToSS group carries out research 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 systems security,
- security of cyber-physical socio-technical systems,
- trust management,
- software security (e.g., vulnerability detection).

SaToSS is part of the LACS and ComSys laboratories and has a strong connection to SnT. For more information, please visit our webpage at http://satoss.uni.lu/

Summary of the group's achievements in 2018

In 2018, the SaToSS group counted 16 researchers (1 professor, 1 senior researcher, 7 postdocs, 6 PhD students and 1 technical assistant). The group runs two Junior CORE projects (COMMA on malware analysis and PrivDA on privacy in social networks), two FNR-INTER projects (AlgoReCell on models of biological networks and SURCVS on secure voting systems), one UL-funded project (SEC-PBN on modeling with probabilistic Boolean networks), and one FNR-PRIDE project (SPSquared on security and privacy in information systems). The group also continues to be active in the large Singaporean project Securify. In 2018 the group has secured funding for a PhD position within the FNR-PRIDE project DRIVEN, which will start in 2019. In 2018 SaToSS has successfully completed the FNR-funded Junior CORE project DIST on distance bounding protocols. The Junior PI of DIST, Dr. Rolando Trujillo-Rasua has joined Deakin University, Melbourne, Australia, as Lecturer. The group has contributed to the organization of scientific events (VTSA 2018). Our regular research seminar SRM co-organized jointly with the APSIA group has featured 29 international speakers. SaToSS has been involved in teaching and student supervision for the Bachelor and Master programs in Computer Science (BINFO, BICS, MICS, MSSI).

Three most interesting publications in 2018

1. Distance-Bounding Protocols: Verification without Time and Location. **Sjouke Mauw**, **Zach Smith**, **Jorge Toro-Pozo**, **Rolando Trujillo-Rasua**, in Proceedings of IEEE Symposium on Security and Privacy 2018: 549-566 Distance-bounding protocols are cryptographic protocols that securely establish an upper bound on the physical distance between the participants. Existing symbolic verification frameworks for distance-bounding protocols consider timestamps and the location of agents. In this work we introduce a causality-based characterization of secure distance-bounding that discards the notions of time and location. This allows us to verify the correctness of distance-bounding protocols with standard protocol verification tools. That is to say, we provide the first fully automated verification framework for distance-bounding protocols. By using our framework, we confirmed known vulnerabilities in a number of protocols and discovered unreported attacks against two recently published protocols.

2. Tagvisor: A Privacy Advisor for Sharing Hashtags. Yang Zhang, Mathias Humbert, Tahleen Rahman, Cheng-Te Li, **Jun Pang**, Michael Backes, in Proceedings of WWW 2018: 187-296 Hashtag has emerged as a widely used concept of popular culture and campaigns, but its implications on people's privacy have not been investigated so far. In this paper, we present the first systematic analysis of privacy issues induced by hashtags. We concentrate in particular on location, which is recognized as one of the

key privacy concerns in the Internet era. By relying on a random forest model, we show that we can infer a user's precise location from hashtags with accuracy of 70% to 76%, depending on the city. To remedy this situation, we introduce a system called Tagvisor that systematically suggests alternative hashtags if the user-selected ones constitute a threat to location privacy. Tagvisor realizes this by means of three conceptually different obfuscation techniques and a semantics-based metric for measuring the consequent utility loss. Our findings show that obfuscating as little as two hashtags already provides a near-optimal trade-off between privacy and utility in our dataset. This in particular renders Tagvisor highly time-efficient, and thus, practical in real-world settings.

3. ASSA-PBN: A Toolbox for Probabilistic Boolean Networks. **Andrzej Mizera**, **Jun Pang**, Cui Su, Qixia Yuan, In IEEE/ACM Transactions on Computational Biology and Bioinformatics, Volume 15 Issue 4 (1203-1216), 2018 As a well-established computational framework, probabilistic Boolean networks PBNs are widely used for modelling, simulation, and analysis of biological systems. To analyze the steady-state dynamics of PBNs is of crucial importance to explore the characteristics of biological systems. However, the analysis of large PBNs, which often arise in systems biology, is prone to the infamous state-space explosion problem. Therefore, the employment of statistical methods often remains the only feasible solution. We present ASSA-PBN, a software toolbox for modelling, simulation, and analysis of PBNs. ASSA-PBN provides efficient statistical methods with three parallel techniques to speed up the computation of steady-state probabilities. Moreover, particle swarm optimisation PSO and differential evolution DE are implemented for the estimation of PBN parameters. Additionally, we implement in-depth analyses of PBNs, including long-run influence analysis, long-run sensitivity analysis, computation of one-parameter profile likelihoods, and the visualization of one-parameter profile likelihoods. A PBN model of apoptosis is used as a case study to illustrate the main functionalities of ASSA-PBN and to demonstrate the capabilities of ASSA-PBN to effectively analyse biological systems modelled as PBNs.

5.17 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 2018

2018 was a very fruitful year for Serval. The number of members increased to about 35 researchers. They published about 40 papers in top venues such as FSE, ICSE, Empirical Software Engineering, ISSTA, IST, IEEE TSE etc. They acquired two projects with Paypal, and extended the current industrial projects with BGL, and got several FNR Projects funded (CORE, Junior, Bridges and Pathfinder). Prof. Le Traon was in a mobility grant at UC Berkeley (8 months): he collaborated 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. Contacts have been taken with Apple and Netflix, and two projects with Paypal (Two PhD students and a postdoc) should start in 2019. Prof. Le Traon is also the recipient of the Chaire Francqui Award for University of Namur, Belgium, where he gave inaugural lectures on "Preventive debugging".

Main publications and achievements in 2018

- Mining fix patterns for findbugs violations: Kui Liu, Dongsun Kim, Tegawendé F Bissyandé, Shin Yoo, Yves Le Traon
  IEEE Transactions on Software Engineering
  In this paper, we first collect and track a large number of fixed and unfixed violations across revisions of software. The empirical analyses reveal that there are discrepancies in the distributions of violations that are detected and those that are fixed, in terms of occurrences, spread and categories, which can provide insights into prioritizing violations. To automatically identify patterns in violations and their fixes, we propose an approach that utilizes convolutional neural networks to learn features and clustering to regroup similar instances. We then evaluate the usefulness of the identified fix patterns by applying them to unfixed violations. The results show that developers will accept and merge a majority (69/116) of fixes generated from the inferred fix patterns. It is also noteworthy that the yielded patterns are applicable to four real bugs in the Defects4J major benchmark for software testing and automated repair.
- Feature location benchmark for extractive software product line adoption research using realistic and synthetic Eclipse variants: J Martinez, T Ziadi, M Papadakis, TF Bissyandé, J Klein, Y Le Traon
  Information and Software Technology 104, 46-59
  It is common belief that high impact research in software reuse requires assessment in non-trivial, comparable, and reproducible settings. However,

software artefacts and common representations are usually unavailable. Also, establishing a representative ground truth is a challenging and debatable subject. Feature location in the context of software families is a research field that is becoming more mature with a high proliferation of techniques. We present EFLBench, a benchmark and a framework to provide a common ground for this field.

- Predicting the Fault Revelation Utility of Mutants: Thierry Titcheu Chekam, Mike Papadakis, Tegawendé Francois D Assise Bissyande, Yves Le Traon
40th International Conference on Software Engineering, Gothenburg, Sweden, May 27-3 June 2018 (ICSE 2018)
Mutation testing is one of the strongest code-based test criteria. However, it is expensive as it involves a large number of mutants. To deal with this issue we propose a machine learning approach that learns to select fault revealing mutants. Fault revealing mutants are valuable to testers as their killing results in (collateral) fault revelation. We thus, formulate mutant reduction as the problem of selecting the mutants that are most likely to lead to test cases that uncover unknown program faults. We tackle this problem using a set of static program features and machine learning. Experimental results involving 1,629 real faults show that our approach reveals 14% to 18% more faults than a random mutant selection baseline.
- FaCoY: a code-to-code search engine: Kisub Kim, Dongsun Kim, Tegawendé F Bissyandé, Eunjong Choi, Li Li, Jacques Klein, Yves Le Traon
Proceedings of the 40th International Conference on Software Engineering (ICSE 2018)
Code search is an unavoidable activity in software development. Various approaches and techniques have been explored in the literature to support code search tasks. Most of these approaches focus on serving user queries provided as natural language free-form input. However, there exists a wide range of use-case scenarios where a code-to-code approach would be most beneficial. For example, research directions in code transplantation, code diversity, patch recommendation can leverage a code-to-code search engine to find essential ingredients for their techniques. In this paper, we propose F a C o Y, a novel approach for statically finding code fragments which may be semantically similar to user input code.

5.18 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, including conversion and storage and open for solar-fed structures for transport and thermal energy use. Further Information is available at http://sce.uni.lu/.

Summary of the group's achievements in 2018

In 2018, the PhD of D. Norta for development of the hydrokinetic turbine with RWTH Aachen was finalized , and cooperation with FZ Jülich and the Der-Lab association of European laboratories continued including the set of three custom-built digital power actuators for parallel grid support inverter with dedicated FPGA hardware control. The method for measurable curtailment of Photovoltaic-power inverters has been verified. Furthermore energy economic analysis for the northpool market dynamics and supply curve decomposition were further pursued with DNV-GL in view of future cooperations. The PhD works of K. Torchyan were focused towards research on distributed grid support and curtailment. Both overcurrent and overvoltage constraints are being investigated for the complete subsets of MV-grid configurations, laying the ground for the cooperative control methods including droops and fair curtailment references, being able to guarantee supply security within the tolerances required, while maintaining reconfiguration freedom of the grid operator. The external PhD works of A.Piskun, Norway on modeling of price bids in day-ahead markets was continued towards decomposition of aggregated supply curves as published by commercial operators, with constraints for locational marginal pricing. In a case study, the accuracy of the decomposition mode has been verified with reconstructed bids for simulation of day-ahead market. This approach for model based investigation of the day-ahead markets is also extendable to nodal pricing. Cooperation with the Eurosolar and the Swiss Solar Agency have been continued with Prof. Sachau as member of the Norman Foster committee and the European Solarprize committee. He also followed invitations to the IRENA Congress, Bonn and the Benelux Tanaloa exercise, Brussels .

Three most interesting achievements in 2018

Powertech paper submission : Determination of PV-Plant Integration Capacity of Medium Voltage Networks in Relation to Grid Reconfiguration **K. Torchyan, J. Sachau**

With the increasing number of photovoltaic (PV) distributed generations (DG) being installed on the medium-voltage (MV) level and the fluctuations of the generation and loads, the supply security of the grid requires closer attention. Gridwide voltage profile, overloading of substation transformers and overloading of lines may become bottlenecks for large-scale integration of PV plants. Here, measures to avoid cost-intensive network reinforcement are of interest. In this paper, analysis of grid reconfiguration and it's impact on hosting capacity (HC) and grid operation is studied. Additionally, a method to determine the maximum permissible integration capacity of PV, taking into account the limitations of the transformers, lines, voltages and voltage angles is presented. The proposed method is tested on a 43-bus 20 kV MV network model representative for Luxembourg's grid situations. The modeling, reconfiguration, HC calculation and analysis are done using Pandapower software. The results indicate that by proper reconfiguration of the network the HC can be increased by up to 36% and the number of overloaded lines can be decreased, thus decreasing the expenses on cost-intensive network reinforcement.

Book Contribution : H de Faria, **K. Torchyan**, H. Margossian, **J. Sachau** "Distributed generation with photovoltaic grid connected systems: connection, drivers, and obstacles," in Photovoltaic Systems: Design, Performance and Application; Nova Science Publishers

Integration of photovoltaic generation in distribution networks can cause operational issues such as over-voltages and unnecessary tripping. To overcome these technical obstacles, voltage and frequency control strategies are of interest, 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

J. Sachau : "Advanced Electricity Balancing and Storage for Long term Sustainable Energy Security" EC-JRC cooperation 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 coordinates and supports works on energy market design, supply security and system reliability. In order to achieve the energy- and climate targets for 2020 and beyond, for Luxemburg the works cope with the longterm energyeconomical needs : accommodation of large-scale fluctuating electricity feedin transition to solarelectrical mobility & transport - corresponding integration of storage portfolios under technoeconomical and supply-security conditions. The works aim at reinforcing techno-scientific know-how in energy-security, complementing recent progress financed by the university, Luxembourg's network operator CREOS and the FNR, for sustainable integration of distributed electricity generation in Luxembourg.

5.19 Team Leprévost

Prof. Dr. Franck Leprévost & Dr. Nicolas Bernard

Summary of the achievements in 2018

During 2018 Research has been conducted in three directions. On the one hand, computations were conducted to identify and interpret coefficients of some p-adic expansions coming up in the context of ECDLP in an innovative way. On the other hand, a series of experimentation using the HPC cluster of the university were performed to study how evolutionary algorithms can be used for understanding and attacking convolutional neural networks. An additional 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 published as a chapter of a book. 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 2018, 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 in the past two years, 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 2019 at the earliest. Finally, F. Leprévost gave two keynote talks at the Mathematical Society of South-Eastern Europe International Conference in Mathematics (MICOM-2018, 18-23 September 2018, Cyprus) and at the 3rd International Conference on Applications in Information Technology (ICAIT-2018, November 1-3, 2018, Aizu-Wakamatsu, Japan). He also gave two regular talks, the first one at ICAIT-2018, and the second one at the Latin American High Performance Computing Conference (CARLA-2018, 26-28 September 2018, Bucaramanga, Colombia) in the context of a paper to appear in 2019.

The main publications or work in progress of 2018

- "The University of Luxembourg: A National Excellence Initiative", **F. Leprévost**. Chapter 9 (p. 152-173) in "Accelerated Universities: Ideas and Money Combine to Build Academic Excellence". Editors: Ph. G. Altbach, L. Reisberg, J. Salmi and I. Froumin. Vol 40 of the series Global Perspective on Higher Education. Publisher: Brill (The Netherlands) 2018.
- "James Bond's Most Secret Weapon", **F. Leprévost**. Proceedings of the 3rd International Conference on Applications in Information Technology (ICAIT-2018), hosted by the University of Aizu (November 1-3, 2018, Aizu-Wakamatsu, Japan). Publisher ACM, New York, NY USA (ISBN 978-1-4503-6516-1); p. 1-2.
- "Elliptic Curves Discrete Logarithm Problem over a Finite Prime Field Fp and p-adic Approximations", **F. Leprévost**, **N. Bernard** and **P. Bouvry**. Proceedings of the 3rd International Conference on Applications in Information Technology (ICAIT-2018), hosted by the University of Aizu (November 1-3, 2018, Aizu-Wakamatsu, Japan). Publisher ACM, New York, NY USA (ISBN 978-1-4503-6516-1); p. 9-15.
- "Evolutionary Algorithms for Convolutional Neural Network Visualisation", **N. Bernard**, **F. Leprévost**. To appear in the Proceedings of the Latin American High Performance Computing Conference (CARLA) 2018, hosted by the University of Bucaramanga (26-28 September 2018, Bucaramanga, Colombia)
- "The clash of universities", **F. Leprévost**. Book in progress.
- "How Evolutionary Algorithms and Information Hiding deceive machines and humans for image recognition? A research program", **N. Bernard**, **F. Leprévost**. To appear in the Proceedings of the International Workshop on Optimization and Learning (OLA-2018), Bangkok, Thailand, Jan 29-31, 2019.

5.20 Team Müller

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

Volker Müller and his small research team are interested in algorithmic aspects of common number-theoretic problems. Together with his assistant, an assumed property of integral binary quadratic forms used in several published proofs could be proven as incorrect; necessary corrections for known algorithms relying on that incorrect fact are currently investigated. In addition, new ideas for factoring integers are actively researched, and some preliminary (not yet completely satisfying) results have already been achieved. As study director of the "Bachelor en informatique" and the "Bachelor en informatique en formation continue", Volker Müller was strongly involved in the re-definition of programme regulations and the preparation of the programme specific parts of the "Règlement des études", to make both programmes consistent with the framework defined in the new 2018 University law. In addition, a first re-definition of the BINFO programme with a transition to a few new courses was implemented in September 2018. Further programme adaptions for a better reflection of the professional needs in Luxembourg are planned for the current academic year.

CHAPTER 6

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.

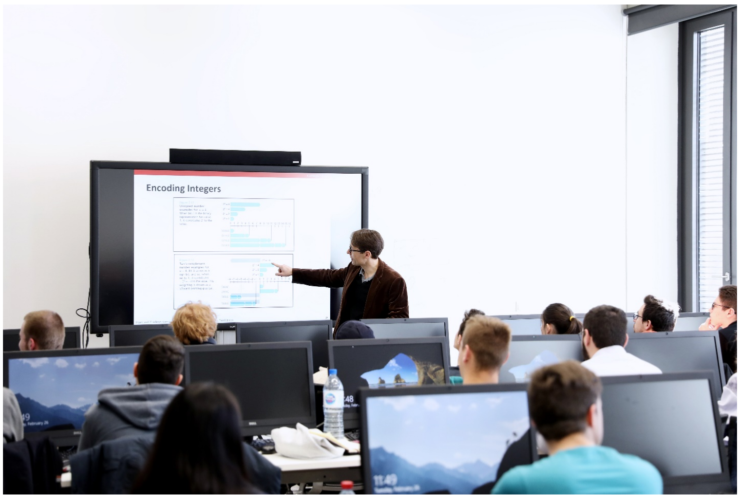
The internal communication within CSC is based on an effective communication infrastructure, based e.g. on ULI or Sharepoint. Short summaries of the CSC professors meeting and the meetings of the education management committee and research management committee is made available. Agenda points for the 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 7

Education



7.1 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.

7.2 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 2018 there were around 60 students from more than 20 countries in the MICS.

7.3 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 2018, the MSSI organised the Information Security Education Day (ISED). It is a yearly one-day event co-organised by University of Luxembourg and Luxembourg Institute of Science and Technology (LIST) and sponsored by CLUSIL, CSC and LIST. 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. The theme of ISED 2018 was “Internet of Things: security challenges and opportunities”.

7.4 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 labor 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. Until today the BiCS has the following global figures:
  - 128 total applicants (17% female, 83% male)

- admission rate: 65%
- high school degrees: 90% classic, 10% vocational
- high school country: 70% Luxembourg, 30% other
- 51 currently registered to the program (34 first year, 17 second year)

7.5 Bachelor of Engineering in Computer Science (BINFO)

The "Bachelor en informatique" (BINFO) offers a practice-oriented study programme that provides the students with highly-demanded professional skills to enter the job market after graduation, be it in the public or the private sector. The BINFO trains students with a combination of theoretical lectures and many practical projects such that the students master basic professional skills and applied IT know-how 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 (English, French) with classmates and instructors from diverse 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 methods required to develop computer systems;
- Acquire a specialization in one application domain of computer science such as banking information technology or distributed applications, especially deepening applied knowledge on the latest trends in the IT industry;
- Be able to efficiently communicate orally and in writing, in English and French, in cross cultural professional environments;
- Understand how companies operate and be well prepared for professional life, through the end-of-study internship done in professional partner institutions 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 2018-2019, a total of 140 students are registered within the BINFO program (55 in the first year, 43 in the second, and 42 students in the third year).

The number of BINFO graduates in 2018 is 31. More information on the programme can be found at https://binfo.uni.lu.

7.6 Bachelor en informatique en formation continue (Binfo-LLL)

The "Bachelor en informatique en formation continue" (BINFO-LLL) offers a practice-oriented part-time study programme that corresponds to the needs of the Luxembourgish labor market for continued professional development. Students require a minimum of 6 years of professional experience in the IT domain, which is honored in the programme with the acknowledgement of a certain number of ECTS credits. The BINFO-LLL trains its students with a combination of theoretical lectures and many practical projects, especially focusing on certain practically important areas like programming, web applications, or big data applications. A special objective of the programme is the empowerment of its students for continued training and further professional development during their future professional career. Beyond technical training in practically relevant IT-related technologies, BINFO-LLL is humanly rich and offers a bilingual study programme (English, French) with classmates and instructors from diverse cultural and professional background.

The main learning objectives of the BINFO-LLL are the following:

- Be competent in software programming and, more widely, in methods required to develop computer systems;
- Acquire a broad basis knowledge in several application domains of computer science such as programming, web applications, algorithms and data structures, banking information technology, distributed applications, data-centered applications, and others, especially deepening already existing practical expertise on latest trends in the IT industry;
- Be able to efficiently communicate orally and in writing, in English and French, in cross cultural professional environments;
- Be able to work autonomously, analyze and anticipate issues, propose solutions in various professional situations.

In the Winter semester 2018-2019, a total of 33 students are registered within the BINFO-LLL program (13 in the first, 20 students in the second/third year).

The number of BINFO-LLL graduates in 2018 is 3 (this is the first promotion since the BINFO-LLL programme started only 2 years ago). More information on the programme can be found at https://binfo-fc.uni.lu.

7.7 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 digital 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**
Books	7	A.1 (p.58)
Book Chapters	6	A.2 (p.59)
Journal	67	A.3 (p.59)
Conference Papers	156	A.4 (p.66)
Theses	17	A.5 (p.83)
Tech Reports	9	A.6 (p.84)
Miscellaneous	52	A.7 (p.85)
Total	*314*	

Table A.1: Overview of publications per category

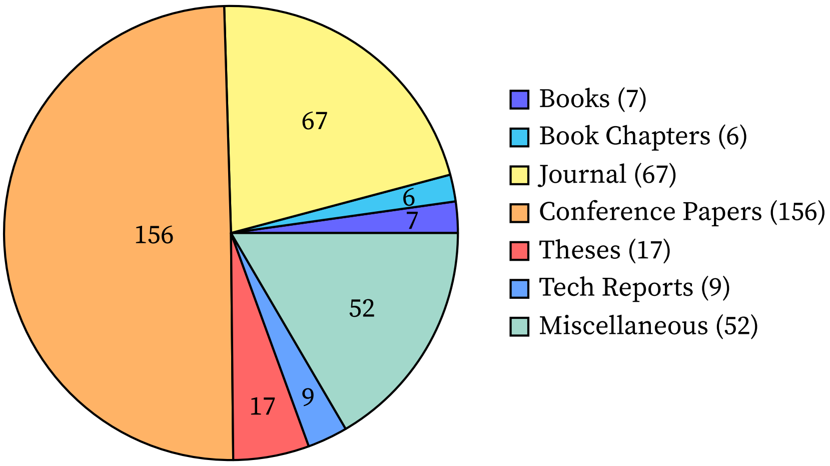


Figure A.1: Distribution of Types of Publications

A.1 Books

[1] Christoph Benzmüller, Francesco Ricca, Xavier Parent, and Dumitru Roman, eds. *Rules and Reasoning, Second International Joint Conference, RuleML+RR 2018, Luxembourg, Luxembourg, September 18-21, 2018, Proceedings*. Springer, 2018. ISBN: 978-3-319-99906-7. DOI: 10.1007/978-3-319-99906-7. URL: http://hdl.handle.net/10993/37448.

[2] Claudia d'Amato and Martin Theobald, eds. *Reasoning Web. Learning, Uncertainty, Streaming, and Scalability - 14th International Summer School 2018, Esch-sur-Alzette, Luxembourg, September 22-26, 2018, Tutorial Lectures*. Springer, 2018. ISBN: 978-3-030-00337-1. URL: http://hdl.handle.net/10993/37836.

[3] J.-G. Dumas, P. Lafourcade, A. Tichit, and Sébastien Varrette. *Les blockchains en 50 questions: comprendre le fonctionnement et les enjeux de cette technologie innovante*. Dunod, 2018. ISBN: 978-2-1007-7924-6. URL: http://hdl.handle.net/10993/36114.

[4] J.-G. Dumas, J.-L. Roch, E. Tannier, and Sébastien Varrette. *Théorie des Codes : Compression, Cryptage et Correction*. Dunod, 2018. ISBN: 978-2-10-078109-6. URL: http://hdl.handle.net/10993/36112.

[5] Daniel Lee, Alexander Steen, and Toby Walsh, eds. *GCAI-2018. 4th Global Conference on Artificial Intelligence*. EasyChair, 2018. URL: http://hdl.handle.net/10993/37246.

[6] Peng Liu, Sjouke Mauw, and Ketil Stolen, eds. *Proceedings of the Fourth International Workshop on Graphical Models for Security (GraMSec 2017)*. Springer, 2018. ISBN: 978-3-319-74860-3. DOI: 10.1007/978-3-319-74860-3. URL: http://hdl.handle.net/10993/37275.

[7] Jun Pang, Chenyi Zhang, Jifeng He, and Jian Weng, eds. *Proceedings of the 12th International Symposium on Theoretical Aspects of Software Engineering*. IEEE Computer Society, 2018. URL: http://hdl.handle.net/10993/37235.

A.2 Book Chapters

[8] Pascal Bouvry, Sébastien Varrette, Muhammad Umer Wasim, Abdallah Ali Zainelabden Abdallah Ibrahim, Xavier Besseron, and T. A. Trinh. "Security, reliability and regulation compliance in Ultrascale Computing System". In: *Ultrascale Computing Systems*. Ed. by J. Carretero and E. Jeannot. IET, 2018. URL: http://hdl.handle.net/10993/36371.

[9] Patrick Glauner and Philipp Plugmann. "Kunstliche Intelligenz - die nächste Revolution (The Artificial Intelligence Revolution)". In: *Innovationsumgebungen gestalten: Impulse für Start-ups und etablierte Unternehmen im globalen Wettbewerb*. Springer, 2018. ISBN: 978-3-658-22126-3. URL: http://hdl.handle.net/10993/36239.

[10] Franck Leprévost. "The University of Luxembourg: A National Excellence Initiative". In: *Accelerated Universities: A ideas and Money Combine to Build Academic Excellence*. Ed. by Phil Altbach, Liz Reisberg, Jamil Salmi, and Isaak Froumin. Brill, 2018, pp. 152–173. URL: http://hdl.handle.net/10993/37315.

[11] Anne-Cecile Orgerie and Sébastien Varrette. "A Full-Cost Model for Estimating the Energy Consumption of Computing Infrastructures". In: *Ultrascale Computing Systems*. Ed. by J. Carretero and E. Jeannot. IET, 2018. URL: http://hdl.handle.net/10993/36377.

[12] Arianna Rossi and Monica Palmirani. "From Words to Images Through Legal Visualization". In: *AI Approaches to the Complexity of Legal Systems: AICOL International Workshops 2015–2017: AICOL-VI@ JURIX 2015, AICOL-VII@ EKAW 2016, AICOL-VIII@ JURIX 2016, AICOL-IX@ ICAIL 2017, and AICOL-X@ JURIX 2017, Revised Selected Papers*. Ed. by Ugo Pagallo, Monica Palmirani, Pompeu Casanovas, Giovanni Sartor, and Serena Villata. Springer Cham, 2018, pp. 72–85. ISBN: 978-3-030-00177-3. URL: http://hdl.handle.net/10993/37300.

[13] Leon van der Torre, Tjitze Rienstra, and Dov Gabbay. "Argumentation as Exogenous Coordination". In: *It's All About Coordination*. Springer, 2018, pp. 208–223. URL: http://hdl.handle.net/10993/36355.

A.3 Journal

[14] Florian Adamsky, Matthieu Aubigny, Federica Battisti, Marco Carli, F. Cimorelli, Tiago Cruz, et al. "Integrated Protection of Industrial Control Systems from Cyber-attacks: the ATENA Approach". In: *Elsevier International Journal of Critical Infrastructure Protection* (2018). DOI: 10.1016/j.ijcip.2018.04.004. URL: http://hdl.handle.net/10993/35720.

[15] Claudia Álvarez-Aparicio, Ángel Manuel Guerrero-Higueras, Maria Carmen Calvo Olivera, Francisco Javier Rodriguez Lera, Francisco Martín, and Vicente Matellán. “Benchmark Dataset for Evaluation of Range-Based People Tracker Classifiers in Mobile Robots”. In: *Frontiers in Neurorobotics* 11 (2018), p. 72. DOI: 10.3389/fnbot.2017.00072. URL: http://hdl.handle.net/10993/37248.

[16] Nicholas Asher and Soumya Paul. “Strategic conversations under imperfect information: Epistemic Message Exchange games”. In: *Journal of Logic, Language and Information* 27 (2018), pp. 343–385. DOI: 10.1007/s10849-018-9271-9. URL: http://hdl.handle.net/10993/38549.

[17] Gabriel A Barragán-Ramírez, Alejandro Estrada-Moreno, Yunior Ramirez Cruz, and Juan A Rodríguez-Velázquez. “The Local Metric Dimension of the Lexicographic Product of Graphs”. In: *Bulletin of the Malaysian Mathematical Sciences Society* (2018). DOI: 10.1007/s40840-018-0611-3. URL: http://hdl.handle.net/10993/37475.

[18] Christof Beierle, Anne Canteaut, and Gregor Leander. “Nonlinear Approximations in Cryptanalysis Revisited”. In: *IACR Transactions on Symmetric Cryptology* 2018 (2018), pp. 80–101. DOI: 10.13154/tosc.v2018.i4.80-101. URL: http://hdl.handle.net/10993/37947.

[19] Christoph Benzmüller. “Universal (Meta-)Logical Reasoning: Recent Successes”. In: *Science of Computer Programming* (2018). DOI: 10.1016/j.scico.2018.10.008. URL: http://hdl.handle.net/10993/37443.

[20] Christoph Benzmüller and Jens Otten. “ARQNL 2018 Automated Reasoning in Quantified Non-Classical Logics”. In: *CEUR Workshop Proceedings* 2095 (2018). URL: http://hdl.handle.net/10993/37465.

[21] Christoph Benzmüller and Dana S. Scott. “Axiom Systems for Category Theory in Free Logic”. In: *Archive of Formal Proofs* (2018). URL: http://hdl.handle.net/10993/37446.

[22] Guillaume Brau, Nicolas Navet, and Jérôme Hugues. “Towards the Systematic Analysis of Non-Functional Properties in Model-Based Engineering for Real-Time Embedded Systems”. In: *Science of Computer Programming* 156 (2018), pp. 1–20. DOI: 10.1016/j.scico.2017.12.007. URL: http://hdl.handle.net/10993/34015.

[23] Jérémy Henri J. Charlier, Eric Falk, Radu State, and Jean Hilger. “User-Device Authentication in Mobile Banking using APHEN for Paratuck2 Tensor Decomposition”. In: *2018 IEEE International Conference on Data Mining Workshops (ICDMW)* (2018). DOI: 10.1109/ICDMW.2018.00130. URL: http://hdl.handle.net/10993/37381.

[24] Jérémy Henri J. Charlier and Radu State. “Non-Negative Paratuck2 Tensor Decomposition Combined to LSTM Network for Smart Contracts Profiling”. In: *International Journal of Computer & Software Engineering* 3 (2018). DOI: 10.15344/2456-4451/2018/132. URL: http://hdl.handle.net/10993/35508.

[25] Benoît-Michel Cogliati. “Tweaking a block cipher: multi-user beyond-birthday-bound security in the standard model”. In: *Designs, Codes and Cryptography* (2018). DOI: 10.1007/s10623-018-0471-8. URL: http://hdl.handle.net/10993/35375.

[26] Stanislav Dashevskyi, Achim D. Brucker, and Fabio Massacci. “A Screening Test for Disclosed Vulnerabilities in FOSS Components”. In: *IEEE Transactions on Software Engineering* (2018), pp. 1–1. DOI: 10.1109/TSE.2018.2816033. URL: http://hdl.handle.net/10993/37252.

[27] Jérémie Decouchant, Maria Fernandes, Marcus Volp, Francisco M. Couto, and Paulo Verissimo. “Accurate filtering of privacy-sensitive information in raw genomic data”. In: *Journal of Biomedical Informatics* (2018). DOI: 10.1016/j.jbi.2018.04.006. URL: http://hdl.handle.net/10993/35870.

[28] Jan Eric Dentler, Martin Rosalie, Grégoire Danoy, Pascal Bouvry, Somasundar Kannan, Miguel Angel Olivares Mendez, et al. “Collision Avoidance Effects on the Mobility of a UAV Swarm Using Chaotic Ant Colony with Model Predictive Control”. In: *Journal of Intelligent \& Robotic Systems* (2018), pp. 1–17. DOI: 10.1007/s10846-018-0822-8. URL: http://hdl.handle.net/10993/35582.

[29] Xavier Devroey, Gilles Perrouin, Mike Papadakis, Axel Legay, Pierre-Yves Schobbens, and Pattrick Heymans. “Model-based mutant equivalence detection using automata language equivalence and simulations”. In: *Journal of Systems and Software* (2018). URL: http://hdl.handle.net/10993/37416.

[30] Dumitru-Daniel Dinu, Yann Le Corre, Dmitry Khovratovich, Léo Paul Perrin, Johann Groszschädl, and Alex Biryukov. “Triathlon of Lightweight Block Ciphers for the Internet of Things”. In: *Journal of Cryptographic Engineering* (2018). DOI: 10.1007/s13389-018-0193-x. URL: http://hdl.handle.net/10993/37760.

[31] Georgios Fotiadis and Elisavet Konstantinou. “Generating Pairing-Friendly Elliptic Curve Parameters Using Sparse Families”. In: *Journal of Mathematical Cryptology* 12 (2018), pp. 83–99. URL: http://hdl.handle.net/10993/39267.

[32] Antônio Augusto Fröhlich, M.Roberto Scheffel, David Kozhaya, and Paulo Verissimo. “Byzantine Resilient Protocol for the IoT”. In: *IEEE Internet of Things Journal* (2018). DOI: 10.1109/JIOT.2018.2871157. URL: http://hdl.handle.net/10993/38282.

[33] David Fuenmayor and Christoph Benzmüller. “A Case Study On Computational Hermeneutics: E. J. Lowe’s Modal Ontological Argument”. In: *IfCoLog Journal of Logics and Their Applications* 5 (2018), pp. 1567–1603. URL: http://hdl.handle.net/10993/37444.

[34] David Fuenmayor and Christoph Benzmüller. “Formalisation and Evaluation of Alan Gewirth’s Proof for the Principle of Generic Consistency in Isabelle/HOL”. In: *Archive of Formal Proofs* (2018). URL: http://hdl.handle.net/10993/37449.

[35] Dov Gabbay, Massimiliano Giacomin, Beishui Liao, and Leon van der Torre. “Present and Future of Formal Argumentation (Dagstuhl Perspectives Workshop 15362)”. In: *Dagstuhl Manifestos* 7 (2018), pp. 69–95. DOI: 10.4230/DagMan.7.1.69. URL: http://hdl.handle.net/10993/37881.

[36] Abdallah Ali Zainelabden Abdallah Ibrahim, Muhammad Umer Wasim, Sébastien Varrette, and Pascal Bouvry. “PRESENCE: Monitoring and Modelling the Performance Metrics of Mobile Cloud SaaS Web Services”. In: *Mobile Information Systems* 2018 (2018). DOI: 10.1155/2018/1351386/. URL: http://hdl.handle.net/10993/36944.

[37] Anastasiia Karpenko, Tuomas Kinnunen, Manik Madhikermi, Jérémy Robert, Kary Främling, Bhargav Dave, et al. “Data Exchange Interoperability in IoT Ecosystem for Smart Parking and EV Charging”. In: *Sensors* (2018). DOI: 10.3390/s18124404. URL: http://hdl.handle.net/10993/38246.

[38] Yasir Imtiaz Khan, Alexandros Konios, and Nicolas Guelfi. “A Survey of Petri Nets Slicing”. In: *ACM Computing Surveys* 51 (2018), p. 109. DOI: 10.1145/3241736. URL: http://hdl.handle.net/10993/37647.

[39] Marinos Kintis, Mike Papadakis, Andreas Papadopoulos, Evangelos Valvis, Nicos Malevris, and Yves Le Traon. “How effective are mutation testing tools? An empirical analysis of Java mutation testing tools with manual analysis and real faults”. In: *Empirical Software Engineering* (2018). URL: http://hdl.handle.net/10993/35336.

[40] Pingfan Kong, Li Li, Jun Gao, Kui Liu, Tegawendé François D Assise Bissyande, and Jacques Klein. “Automated Testing of Android Apps: A Systematic Literature Review”. In: *IEEE Transactions on Reliability* (2018), pp. 1–22. URL: http://hdl.handle.net/10993/36765.

[41] David Kozhaya, Jérémie Decouchant, and Paulo Verissimo. “RT-ByzCast: Byzantine-Resilient Real-Time Reliable Broadcast”. In: *IEEE Transactions on Computers* (2018). DOI: 10.1109/TC.2018.2871443. URL: http://hdl.handle.net/10993/37812.

[42] Diego Kreutz, Jiangshan Yu, Paulo Verissimo, Fernando Ramos, and Catia Magalhaes. “The KISS principle in Software-Defined Networking: a framework for secure communications”. In: *IEEE Security & Privacy Magazine* 16 (2018), pp. 60–70. DOI: 10.1109/MSP.2018.3761717. URL: http://hdl.handle.net/10993/33915.

[43] Kristin Krüger, Marcus Volp, and Gerhard Fohler. “Vulnerability Analysis and Mitigation of Directed Timing Inference Based Attacks on Time-Triggered Systems”. In: *LIPIcs-Leibniz International Proceedings in Informatics* 106 (2018), 22:1–22:17. DOI: 10.4230/LIPIcs.ECRTS.2018.22. URL: http://hdl.handle.net/10993/37810.

[44] Sylvain Kubler, William Derigent, Alexandre Voisin, Jérémy Robert, Yves Le Traon, and Enrique Herrera Viedma. “Measuring inconsistency and deriving priorities from fuzzy pairwise comparison matrices using the knowledge-based consistency index”. In: *Knowledge-Based Systems* (2018). URL: http://hdl.handle.net/10993/36976.

[45] sylvain Kubler, Jérémy Robert, Sebastian Neumaier, Jürgen Umbrich, and Yves Le Traon. “Comparison of metadata quality in open data portals using the Analytic Hierarchy Process”. In: *Government Information Quarterly* (2018). URL: http://hdl.handle.net/10993/36977.

[46] Yongjian Li, Kaiqiang Duan, David Jansen, Jun Pang, Lijun Zhang, Yi Lv, et al. "An Automatic Proving Approach to Parameterized Verification". In: *ACM Transactions on Computational Logic* 19 (2018), pp. 1–27. URL: http://hdl.handle.net/10993/37865.

[47] Beishui Liao, Nir Oren, Leon van der Torre, and Serena Villata. "Prioritized norms in formal argumentation". In: *Journal of Logic and Computation* (2018). DOI: 10.1093/logcom/exy009. URL: http://hdl.handle.net/10993/36538.

[48] Kui Liu, Dongsun Kim, Tegawendé François D Assise Bissyande, Shin Yoo, and Yves Le Traon. "Mining Fix Patterns for FindBugs Violations". In: *IEEE Transactions on Software Engineering* (2018). URL: http://hdl.handle.net/10993/39351.

[49] Zhe Liu, Kim-Kwang Raymond Choo, and Johann Groszschädl. "Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography". In: *IEEE Communications Magazine* 56 (2018), pp. 158–162. DOI: 10.1109/MCOM.2018.1700330. URL: http://hdl.handle.net/10993/37496.

[50] Jabier Martinez, Tewfik Ziadi, Mike Papadakis, Tegawendé François D Assise Bissyande, Jacques Klein, and Yves Le Traon. "Feature location benchmark for extractive software product line adoption research using realistic and synthetic Eclipse variants". In: *Information and Software Technology* (2018). URL: http://hdl.handle.net/10993/37452.

[51] Sjouke Mauw, Yunior Ramirez Cruz, and Rolando Trujillo Rasua. "Anonymising social graphs in the presence of active attackers". In: *Transactions on Data Privacy* 11 (2018), pp. 169–198. URL: http://hdl.handle.net/10993/37227.

[52] Sjouke Mauw, Yunior Ramirez Cruz, and Rolando Trujillo Rasua. "Conditional adjacency anonymity in social graphs under active attacks". In: *Knowledge and Information Systems* (2018). DOI: 10.1007/s10115-018-1283-x. URL: http://hdl.handle.net/10993/38112.

[53] Asya Mitseva, Andriy Panchenko, and Thomas Engel. "The State of Affairs in BGP Security: A Survey of Attacks and Defenses". In: *Computer Communications* (2018). URL: http://hdl.handle.net/10993/35583.

[54] Andrzej Mizera, Jun Pang, Cui Su, and Qixia Yuan. "ASSA-PBN: A Toolbox for Probabilistic Boolean Networks". In: *IEEE/ACM Transactions on Computational Biology and Bioinformatics* 15 (2018), pp. 1203–1216. URL: http://hdl.handle.net/10993/36589.

[55] Andrzej Mizera, Jun Pang, and Qixia Yuan. "Reviving the two-state Markov chain approach". In: *IEEE/ACM Transactions on Computational Biology and Bioinformatics* (2018). URL: http://hdl.handle.net/10993/34366.

[56] Ludovic Mouline, Amine Benelallam, Thomas Hartmann, François Fouquet, Johann Bourcier, Brice Morin, et al. "Enabling Temporal-Aware Contexts for Adaptative Distributed Systems". In: *SAC 2018: SAC 2018: Symposium on Applied Computing , April 9–13, 2018, Pau, France* (2018). DOI: 10.1145/3167132.3167286. URL: http://hdl.handle.net/10993/35423.

[57] Steve Muller, Jean Lancrenon, Carlo Harpes, Yves Le Traon, Sylvain Gombault, and Jean-Marie Bonnin. “A training-resistant anomaly detection system”. In: *Computers & Security* 76 (2018), pp. 1–11. DOI: 10.1016/j.cose.2018.02.015. URL: http://hdl.handle.net/10993/36142.

[58] Nicolas Navet, Jörn Migge, Josetxo Villanueva, and Marc Boyer. “Preshaping Bursty Transmissions under IEEE802.1Q as a Simple and Efficient QoS Mechanism”. In: *SAE International Journal of Passenger Cars—Electronic and Electrical Systems* 11 (2018). URL: http://hdl.handle.net/10993/38606.

[59] Emilie Neveu, Petr Popov, Alexandre Hoffmann, Angelo Migliosi, Xavier Besseron, Grégoire Danoy, et al. “RapidRMSD: Rapid determination of RMSDs corresponding to motions of flexible molecules”. In: *Bioinformatics* (2018). DOI: 10.1093/bioinformatics/bty160. URL: http://hdl.handle.net/10993/35253.

[60] Marek Ostaszewski, Emmanuel Kieffer, Gregoire Danoy, Reinhard Schneider, and Pascal Bouvry. “Clustering approaches for visual knowledge exploration in molecular interaction networks.” In: *BMC bioinformatics* 19 (2018), p. 308. DOI: 10.1186/s12859-018-2314-z. URL: http://hdl.handle.net/10993/37040.

[61] Dimiter Ostrev and Thomas Vidick. “Entanglement of Approximate Quantum Strategies in XOR Games”. In: *Quantum Information and Computation* 18 (2018), pp. 0617–0631. URL: http://hdl.handle.net/10993/37441.

[62] Monica Palmirani, Cesare Bartolini, Michele Martoni, Livio Robaldo, and Arianna Rossi. “Legal Ontology for Modelling GDPR Concepts and Norms”. In: *JURIX 2018 proceedings* (2018). URL: http://hdl.handle.net/10993/37451.

[63] Gabriella Pigozzi and Leon van der Torre. “Arguing about constitutive and regulative norms”. In: *Journal of Applied Non-Classical Logics* 28 (2018), pp. 189–217. DOI: 10.1080/11663081.2018.1487242. URL: http://hdl.handle.net/10993/37879.

[64] Francisco Javier Rodriguez Lera, Vicente Matellán-Olivera, Jesús Balsa-Comerón, Ángel Manuel Guerrero-Higueras, and Camino Fernández-Llamas. “Message Encryption in Robot Operating System: Collateral Effects of Hardening Mobile Robots”. In: *Frontiers in ICT* 5 (2018), p. 2. DOI: 10.3389/fict.2018.00002. URL: http://hdl.handle.net/10993/37249.

[65] Francisco Javier Rodriguez Lera, Vicente Matellán-Olivera, Miguel Á. Conde-González, and Francisco Martı́n-Rico. “HiMoP: A three-component architecture to create more human-acceptable social-assistive robots”. In: *Cognitive Processing* 19 (2018), pp. 233–244. DOI: 10.1007/s10339-017-0850-5. URL: http://hdl.handle.net/10993/37250.

[66] Francisco Javier Rodriguez Lera, Francisco Mart In Rico, and Vicente Matellán Olivera. “Neural networks for recognizing human activities in home-like environments”. In: *Integrated Computer-Aided Engineering* (2018), pp. 1–10. DOI: 10.3233/ica-180587. URL: http://hdl.handle.net/10993/37247.

[67] Martin Rosalie, Grégoire Danoy, Serge Chaumette, and Pascal Bouvry. “Chaos-enhanced mobility models for multilevel swarms of UAVs”. In: *Swarm and Evolutionary Computation* (2018). DOI: 10.1016/j.swevo.2018.01.002. URL: http://hdl.handle.net/10993/34390.

[68] Mingkang Ruan, Thierry Titcheu Chekam, Ennan Zhai, Zhenhua Li, Yao Liu, Jinlong E, et al. “On the Synchronization Bottleneck of OpenStack Swift-like Cloud Storage Systems”. In: *IEEE Transactions on Parallel and Distributed Systems* PP (2018), pp. 1–1. DOI: 10.1109/TPDS.2018.2810179. URL: http://hdl.handle.net/10993/35422.

[69] Bustan S, Gonzalez-Roldan AM, Christoph Schommer, Kamping S, Löffler M, Brunner M, et al. “Psychological, cognitive factors and contextual influences in pain and pain-related suffering as revealed by a combined qualitative and quantitative assessment approach”. In: *PLoS ONE* (2018). DOI: journal.pone.0199814. URL: http://hdl.handle.net/10993/36275.

[70] Morteza Saberi, Martin Theobald, Omar Khadeer Hussain, Elizabeth Chang, and Farookh Khadeer Hussain. “Interactive feature selection for efficient customer recognition in contact centers: Dealing with common names.” In: *Expert Systems with Applications* 113 (2018), pp. 356–376. URL: http://hdl.handle.net/10993/37387.

[71] Mathew Schwartz, Gabriele Lenzini, Yong Geng, Peter Roenne, Peter Ryan, and Jan Lagerwall. “Cholesteric Liquid Crystal Shells as Enabling Material for Information-Rich Design and Architecture.” In: *Advanced Materials* (2018), e1707382. DOI: 10.1002/adma.201707382. URL: http://hdl.handle.net/10993/36053.

[72] 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”. In: *Empirical Software Engineering* 90 (2018), pp. 27–39. URL: http://hdl.handle.net/10993/37599.

[73] Alexander Steen and Christoph Benzmüller. “System Demonstration: The Higher-Order Prover Leo-III”. In: *CEUR Workshop Proceedings* 2095 (2018). URL: http://hdl.handle.net/10993/37463.

[74] Sakthivel Manikandan Sundharam, Nicolas Navet, Sebastian Altmeyer, and Lionel Havet. “A Model-Driven Co-Design Framework for Fusing Control and Scheduling Viewpoints”. In: *Sensors* 18 (2018), p. 628. DOI: 10.3390/s18020628. URL: http://hdl.handle.net/10993/34987.

[75] Iraklis Symeonidis, Gergely Biczók, Fatemeh Shirazi, Cristina Pérez-Solà, Jessica Schroers, and Bart Preneel. “Collateral damage of Facebook third-party applications: a comprehensive study”. In: *Computers & Security* 77 (2018), pp. 179–208. DOI: 10.1016/j.cose.2018.03.015. URL: http://hdl.handle.net/10993/37601.

[76] Mattia Tomasoni, Andrea Capponi, Claudio Fiandrino, Dzmitry Kliazovich, Fabrizio Granelli, and Pascal Bouvry. “Why Energy Matters? Profiling Energy Consumption of Mobile Crowdsensing Data Collection Frameworks”. In: *Pervasive and Mobile Computing* (2018). URL: http://hdl.handle.net/10993/36942.

[77] Maarten Van den Heuvel, Floris Geerts, Martin Theobald, and Wolfgang Getterbauer. “A General Framework for Anytime Approximation in Probabilistic Databases”. In: *CoRR* abs/1806.10078 (2018). URL: http://hdl.handle.net/10993/37488.

[78] Jingyi Wang, Jun Sun, Qixia Yuan, and Jun Pang. “Learning probabilistic models for model checking: an evolutionary approach and an empirical study”. In: *International Journal on Software Tools for Technology Transfer* 20 (2018), pp. 689–704. URL: http://hdl.handle.net/10993/36876.

[79] Jiangshan Yu, Mark Ryan, and Cas Cremers. “DECIM: Detecting Endpoint Compromise In Messaging”. In: *IEEE Transactions on Information Forensics & Security* (2018). URL: http://hdl.handle.net/10993/32515.

A.4 Conference Papers

[80] Florian Adamsky, Tatiana Retunskaia, Stefan Schiffner, and Thomas Engel. “POSTER: WLAN Device Fingerprinting using Channel State Information (CSI)”. In: *11th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec)*. 2018. URL: http://hdl.handle.net/10993/35718.

[81] Grigoris Antoniou, George Baryannis, Sotiris Batsakis, Guido Governatori, Livio Robaldo, Giovanni Siragusa, et al. “Legal Reasoning and Big Data: Opportunities and Challenges”. In: *Legal Reasoning and Big Data: Opportunities and Challenges*. 2018. URL: http://hdl.handle.net/10993/38959.

[82] Arash Atashpendar, Guru Vamsi Policharla, Peter Roenne, and Peter Ryan. “Revisiting Deniability in Quantum Key Exchange via Covert Communication and Entanglement Distillation”. In: *Secure IT Systems, 23rd Nordic Conference, NordSec 2018. Lecture Notes in Computer Science, vol 11252. Springer, Cham.* Springer, 2018, pp. 104–120. DOI: 10.1007/978-3-030-03638-6_7. URL: http://hdl.handle.net/10993/36653.

[83] Gergely Bana, Rohit Chadha, and Ajay Eeralla. “Formal Analysis of Vote Privacy Using Computationally Complete Symbolic Attacker”. In: *Computer Security*. 2018, pp. 350–372. URL: http://hdl.handle.net/10993/36635.

[84] Zohreh Baniasadi, Xavier Parent, Charles Max, and Marcos Creamer. “A Model for Regulating of Ethical Preferences in Machine Ethics”. In: *Proceedings of International Conference on Human-Computer Interaction*. Springer, 2018, pp. 481–506. URL: http://hdl.handle.net/10993/36533.

[85] Kirstie Bellman, Jean Botev, Ada Diaconescu, Lukas Esterle, Christian Gruhl, Chris Landauer, et al. “Self-Improving System Integration – Status and Challenges After Five Years of SISSY”. In: *Proceedings of the 12th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO)*. 2018, pp. 160–167. URL: http://hdl.handle.net/10993/36811.

[86] Paul-Lou Benedick, Jérémy Robert, Yves Le Traon, and Sylvain Kubler. “O-MI/O-DF vs. MQTT: a performance analysis”. In: *O-MI/O-DF vs. MQTT: a performance analysis*. 2018. URL: http://hdl.handle.net/10993/35824.

[87] Christoph Benzmüller, Ali Farjami, and Xavier Parent. “A Dyadic Deontic Logic in HOL”. In: *Deontic Logic and Normative Systems — 14th International Conference, DEON 2018, Utrecht, The Netherlands, 3-6 July, 2018*. Ed. by Jan Broersen, Cleo Condoravdi, Shyam Nair, and Gabriella Pigozzi. College Publications, 2018, pp. 33–50. ISBN: 978-1-84890-278-7. URL: http://hdl.handle.net/10993/36395.

[88] Christoph Benzmüller and David Fuenmayor. “Can Computers Help to Sharpen our Understanding of Ontological Arguments?” In: *Mathematics and Reality, Proceedings of the 11th All India Students’ Conference on Science Spiritual Quest, 6-7 October, 2018, IIT Bhubaneswar, Bhubaneswar, India*. The Bhaktivedanta Institute, Kolkata, www.binstitute.org, 2018, pp. 195–226. ISBN: 81-89635-31-X. DOI: 10.13140/RG.2.2.31921.84323. URL: http://hdl.handle.net/10993/37462.

[89] Christoph Benzmüller, Xavier Parent, and Leon van der Torre. “A Deontic Logic Reasoning Infrastructure”. In: *Sailing Routes in the World of Computation, 14th Conference on Computability in Europe, CiE 2018, Kiel, Germany, July 30 – August 3, 2018, Proceedings*. Springer, 2018, pp. 60–69. ISBN: 978-3-319-67189-5. DOI: 10.1007/978-3-319-94418-0_6. URL: http://hdl.handle.net/10993/37867.

[90] Christoph Benzmüller and Dana S. Scott. “Some Reflections on a Computer-aided Theory Exploration Study in Category Theory (Extended Abstract)”. In: *3rd Conference on Artificial Intelligence and Theorem Proving (AITP 2018), Book of Abstracts*. 2018. URL: http://hdl.handle.net/10993/37445.

[91] Mark Bickford, Liron Cohen, Robert Constable, and Vincent Rahli. “Computability Beyond Church-Turing via Choice Sequences”. In: *LICS 2018*. 2018. URL: http://hdl.handle.net/10993/37405.

[92] Alex Biryukov, Dumitru-Daniel Dinu, Yann Le Corre, and Aleksei Udovenko. “Optimal First-Order Boolean Masking for Embedded IoT Devices”. In: *CARDIS 2017: Smart Card Research and Advanced Applications*. Springer, Cham, 2018, pp. 22–41. ISBN: 978-3-319-75207-5. DOI: 10.1007/978-3-319-75208-2_2. URL: http://hdl.handle.net/10993/37740.

[93] Alex Biryukov and Aleksei Udovenko. “Attacks and Countermeasures for White-box Designs”. In: *Advances in Cryptology – ASIACRYPT 2018*. Ed. by Thomas Peyrin and Steven Galbraith. Springer International Publishing, 2018, pp. 373–402. ISBN: 978-3-030-03328-6. DOI: 10.1007/978-3-030-03329-3. URL: http://hdl.handle.net/10993/33912.

[94] Raphaël Bleuse, Konstantinos Dogeas, Giorgio Lucarelli, Grégory Mounié, and Denis Trystram. “Interference-Aware Scheduling Using Geometric Constraints”. In: *Euro-Par 2018: Parallel Processing*. Springer, 2018, pp. 205–217. ISBN: 978-3-319-96983-1. DOI: 10.1007/978-3-319-96983-1_15. URL: http://hdl.handle.net/10993/37829.

[95] Alessia Calafiore, Guido Boella, and Leon van der Torre. “From Georeferenced Data to Socio-Spatial Knowledge. Ontology Design Patterns to Discover Domain-Specific Knowledge from Crowdsourced Data”. In: *21st International Conference on Knowledge Engineering and Knowledge Management*. 2018. URL: http://hdl.handle.net/10993/38984.

[96] Jialun Cao, Yongjian Li, and Jun Pang. "L-CMP: an automatic learning-based parameterized verification tool". In: *Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering*. ACM, 2018, pp. 892–895. URL: http://hdl.handle.net/10993/36594.

[97] Alfredo Capozucca, Nicolas Guelfi, and Benoît Ries. "Design of a (yet another?) DevOps course". In: *Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment*. Ed. by Jean-Michel Bruel, Manuel Mazzara, and Bertrand Meyer. Springer, 2018. ISBN: 978-3-030-06018-3. DOI: 10.1007/978-3-030-06019-0. URL: http://hdl.handle.net/10993/37224.

[98] Andrea Capponi. "Energy-Efficient Data Acquisition in Mobile Crowdsensing Systems". In: *19th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Chania, Greece, 2018*. 2018. URL: http://hdl.handle.net/10993/35981.

[99] Giovanni Casini, Eduardo Ferme, Thomas Meyer, and Ivan Varzinczak. "A Semantic Perspective on Belief Change in a Preferential Non-Monotonic Framework". In: *Proceedings of the Sixteenth International Conference on Principles of Knowledge Representation and Reasoning (KR 2018)*. AAAI Press, 2018, pp. 220–229. ISBN: 978-1-57735-803-9. URL: http://hdl.handle.net/10993/37394.

[100] Giovanni Casini, Thomas Meyer, and Ivan Varzinczak. "Defeasible Entailment: from Rational Closure to Lexicographic Closure and Beyond". In: *Proceeding of the 17th International Workshop on Non-Monotonic Reasoning (NMR 2018)*. 2018, pp. 109–118. URL: http://hdl.handle.net/10993/37393.

[101] Gianluca Cena, Ivan Cibrario Bertolotti, Tingting Hu, and Adriano Valenzano. "Error detection and management in CAN XR". In: *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*. 2018, pp. 1–9. DOI: 10.1109/WFCS.2018.8402348. URL: http://hdl.handle.net/10993/37369.

[102] Jérémy Henri J. Charlier, Radu State, Jean Hilger, and Jeremy Charlier. "Non-Negative Paratuck2 Tensor Decomposition Combined to LSTM Network For Smart Contracts Profiling". In: *2018 IEEE International Conference on Big Data and Smart Computing Proceedings*. IEEE Computer Society Conference Publishing Services (CPS), 2018, pp. 74–81. ISBN: 978-1-5386-3649-7. URL: http://hdl.handle.net/10993/34803.

[103] Jundong Chen, Md Shafaeat Hossain, Matthias R. Brust, and Naomi Johnson. "A Game Theoretic Analysis of the Twitter Follow-Unfollow Mechanism". In: *International Conference on Decision and Game Theory for Security*. 2018. DOI: 10.1007/978-3-030-01554-1_15. URL: http://hdl.handle.net/10993/38696.

[104] Hao Cheng, Daniel Dinu, and Johann Groszschädl. "Efficient Implementation of the SHA-512 Hash Function for 8-bit AVR Microcontrollers". In: *Innovative Security Solutions for Information Technology and Communications, 11th International Conference, SecITC 2018, Bucharest, Romania, November 8-9, 2018, Revised Selected Papers*. Ed. by Jean-Louis Lanet and Cristian Toma. Springer Verlag, 2018, pp. 273–287. ISBN:

978-3-030-12941-5. DOI: 10.1007/978-3-030-12942-2_21. URL: http://hdl.handle.net/10993/38644.

[105] Marcos Cramer and Mathieu Guillaume. "Directionality of Attacks in Natural Language Argumentation". In: *CEUR Workshop Proceedings*. RWTH Aachen University, 2018. URL: http://hdl.handle.net/10993/37027.

[106] Marcos Cramer and Mathieu Guillaume. "Empirical Cognitive Study on Abstract Argumentation Semantics". In: *Frontiers in Artificial Intelligence and Applications*. 2018. DOI: 10.3233/978-1-61499-906-5-413. URL: http://hdl.handle.net/10993/37025.

[107] María Eugenia Curi, Lucía Carozzi, Renzo Massobrio, Sergio Nesmachnow, Grégoire Danoy, Marek Ostaszewski, et al. "Single and Multiobjective Evolutionary Algorithms for Clustering Biomedical Information with Unknown Number of Clusters". In: *Bioinspired Optimization Methods and Their Applications*. Springer International Publishing, 2018. ISBN: 978-3-319-91641-5. URL: http://hdl.handle.net/10993/35740.

[108] Grégoire Danoy, Didier El Baz, Vincent Boyer, and Bernabé Dorronsoro. "Introduction to PDCO 2018". In: *2018 IEEE International Parallel and Distributed Processing Symposium Workshops, IPDPS Workshops 2018, Vancouver, BC, Canada, May 21-25 2018*. IEEE Computer Society, 2018. DOI: 10.1109/IPDPSW.2018.00099. URL: http://hdl.handle.net/10993/37272.

[109] Jérémie Dauphin and Marcos Cramer. "ASPIC-END: Structured Argumentation with Explanations and Natural Deduction". In: *Theory and Applications of Formal Argumentation*. 2018. URL: http://hdl.handle.net/10993/32409.

[110] Jérémie Dauphin and Marcos Cramer. "Extended Explanatory Argumentation Frameworks". In: *Theory and Applications of Formal Argumentation*. 2018. URL: http://hdl.handle.net/10993/32410.

[111] Jérémie Dauphin, Marcos Cramer, and Leon van der Torre. "Abstract and Concrete Decision Graphs for Choosing Extensions of Argumentation Frameworks". In: *Computational Models of Argument*. 2018. URL: http://hdl.handle.net/10993/36362.

[112] Jérémie Dauphin and Ken Satoh. "Dialogue Games for Enforcement of Argument Acceptance and Rejection via Attack Removal". In: *International Conference on Principles and Practice of Multi-Agent Systems*. 2018. URL: http://hdl.handle.net/10993/37260.

[113] Florian Delavernhe, Takfarinas Saber, Mike Papadakis, and Anthony Ventresque. "A Hybrid Algorithm for Multi-objective Test Case Selection in Regression Testing". In: *IEEE CONGRESS ON EVOLUTIONARY COMPUTATION*. 2018. URL: http://hdl.handle.net/10993/37417.

[114] Antonio Di Maio, Ridha Soua, Maria Rita Palattella, and Thomas Engel. "ROADNET: Fairness- and Throughput-Enhanced Scheduling for Content Dissemination in VANETs". In: *ROADNET: Fairness- and Throughput-Enhanced Scheduling for Content Dissemination in VANETs*. 2018. DOI: 10.1109/ICCW.2018.8403777. URL: http://hdl.handle.net/10993/36278.

[115] Virginia Dignum, Matteo Baldoni, Cristina Baroglio, Maurizio Caon, Raja Chatila, Louise A. Dennis, et al. “Ethics by Design: Necessity or Curse?” In: *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society AIES 2018, New Orleans, LA, USA, February 02-03, 2018*. 2018. DOI: 10.1145/3278721.3278745. URL: http://hdl.handle.net/10993/38926.

[116] Feng Dong, Haoyu Wang, Li Li, Yao Guo, Tegawendé François D Assise Bissyande, Tianming Liu, et al. “FraudDroid: Automated Ad Fraud Detection for Android Apps”. In: *ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2018)*. 2018, pp. 257–268. URL: http://hdl.handle.net/10993/37891.

[117] Loïc Fejoz, Bruno Regnier, Philippe Miramont, and Nicolas Navet. “Simulation-Based Fault Injection as a Verification Oracle for the Engineering of Time-Triggered Ethernet networks”. In: *Proc. Embedded Real-Time Software and Systems (ERTS 2018)*. 2018. URL: http://hdl.handle.net/10993/34054.

[118] Christof Ferreira Torres and Hugo Jonker. “Investigating Fingerprinters and Fingerprinting-Alike Behaviour of Android Applications”. In: *23rd European Symposium on Research in Computer Security, Barcelona, Spain, September 3-7, 2018*. 2018. URL: http://hdl.handle.net/10993/36368.

[119] Christof Ferreira Torres, Julian Schütte, and Radu State. “Osiris: Hunting for Integer Bugs in Ethereum Smart Contracts”. In: *34th Annual Computer Security Applications Conference (ACSAC ’18), San Juan, Puerto Rico, USA, December 3-7, 2018*. 2018. ISBN: 978-1-4503-6569-7. DOI: 10.1145/3274694.3274737. URL: http://hdl.handle.net/10993/36757.

[120] Antonio Maria Fiscarelli, Aleksandr Beliakov, Stanislav Konchenko, Pascal Bouvry, Ngoc Thanh Nguyen, Duong Hung Hoang, et al. “A Degenerate Agglomerative Hierarchical Clustering Algorithm for Community Detection”. In: *Intelligent Information and Database Systems*. Springer, 2018, pp. 234–242. ISBN: 978-3-319-75416-1. URL: http://hdl.handle.net/10993/38403.

[121] Antonio Maria Fiscarelli, Matthias R. Brust, Grégoire Danoy, Pascal Bouvry, Luca Maria Aiello, Chantal Cherifi, et al. “A Memory-Based Label Propagation Algorithm for Community Detection”. In: *Complex Networks and Their Applications VII*. Springer, 2018, pp. 171–182. ISBN: 978-3-030-05410-6. URL: http://hdl.handle.net/10993/38402.

[122] Beltran Fiz Pontiveros, Robert Norvill, and Radu State. “Monitoring the transaction selection policy of Bitcoin mining pools”. In: *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2018. DOI: 10.1109/NOMS.2018.8406328. URL: http://hdl.handle.net/10993/36752.

[123] Beltran Fiz Pontiveros, Robert Norvill, and Radu State. “Recycling Smart Contracts: Compression of the Ethereum Blockchain.” In: *Proceedings of 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) 2018*. IEEE, 2018. DOI: 10.1109/NTMS.2018.8328742. URL: http://hdl.handle.net/10993/36642.

[124] Francois Fouquet, Thomas Hartmann, Sébastien Mosser, and Maxime Cordy. "Enabling lock-free concurrent workers over temporal graphs composed of multiple time-series". In: *33rd Annual ACM Symposium on Applied Computing (SAC'18)*. 2018. DOI: 10.1145/3167132.3167255. URL: http://hdl.handle.net/10993/35993.

[125] Christian Franck, Johann Groszschädl, Yann Le Corre, Cyrille Lenou Tago, Irfan Awan, Muhammad Younas, et al. "Energy-Scalable Montgomery-Curve ECDH Key Exchange for ARM Cortex-M3 Microcontrollers". In: *Proceedings of the 6th International Conference on Future Internet of Things and Cloud Workshops (W-FICLOUD 2018)*. IEEE Computer Society, 2018, pp. 231–236. ISBN: 978-1-5386-7810-7. DOI: 10.1109/W-FiCloud.2018.00044. URL: http://hdl.handle.net/10993/37497.

[126] David Fuenmayor and Christoph Benzmüller. "Computational Hermeneutics: Using Computers to Interpret Philosophical Arguments (Abstract)". In: *Logical Correctness, Workshop at UNILOG'2018, UNILOG'2018 Book of Abstracts*. Universit ́e Clermont Auvergne, 2018, pp. 250–251. ISBN: 978-2-9544948-1-4. URL: http://hdl.handle.net/10993/37464.

[127] Olga Gadyatskaya, Rolando Trujillo Rasua, and Sjouke Mauw. "New Directions in Attack Tree Research: Catching up with Industrial Needs". In: *Proceedings of the 4th International Workshop on Graphical Models for Security*. Springer, 2018. DOI: 10.1007/978-3-319-74860-3_9. URL: http://hdl.handle.net/10993/33731.

[128] Ziya Alper Genç, Gabriele Lenzini, and Peter Ryan. "Next Generation Cryptographic Ransomware". In: *Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings*. Springer International Publishing, 2018, pp. 385–401. ISBN: 978-3-030-03637-9. DOI: 10.1007/978-3-030-03638-6_24. URL: http://hdl.handle.net/10993/37569.

[129] Ziya Alper Genç, Gabriele Lenzini, and Peter Ryan. "No Random, No Ransom: A Key to Stop Cryptographic Ransomware". In: *Proceedings of the 15th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2018)*. Ed. by Cristiano Giuffrida, Sébastien Bardin, and Gregory Blanc. Springer International Publishing, 2018, pp. 234–255. ISBN: 978-3-319-93410-5. DOI: 10.1007/978-3-319-93411-2_11. URL: http://hdl.handle.net/10993/35679.

[130] Ziya Alper Genç, Gabriele Lenzini, and Peter Ryan. "Security Analysis of Key Acquiring Strategies Used by Cryptographic Ransomware". In: *Advances in Cybersecurity 2018*. 2018. URL: http://hdl.handle.net/10993/36627.

[131] Ziya Alper Genç, Gabriele Lenzini, Peter Ryan, and Itzel Vazquez Sandoval. "A Security Analysis, and a Fix, of a Code-Corrupted Honeywords System". In: *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. 2018. URL: http://hdl.handle.net/10993/32789.

[132] Sankalp Ghatpande, Johann Groszschädl, and Zhe Liu. "A Family of Lightweight Twisted Edwards Curves for the Internet of Things". In: *Information Security Theory and Practice, 12th IFIP WG 11.2 International Conference, WISTP 2018, Brussels, Belgium, December 10-11, 2018, Proceedings*. Ed. by Olivier Blazy and Chan Y. Yeun. Springer Verlag, 2018, ??–?? URL: http://hdl.handle.net/10993/39121.

[133] Domenico Giotti, Luca Lamorte, Ridha Soua, Maria Rita Palattella, and Thomas Engel. "Performance Analysis of CoAP under Satellite Link Disruption". In: *Performance Analysis of CoAP under Satellite Link Disruption*. 2018. URL: http://hdl.handle.net/10993/35976.

[134] Patrick Glauner, Radu State, Petko Valtchev, and Diogo Duarte. "On the Reduction of Biases in Big Data Sets for the Detection of Irregular Power Usage". In: *Proceedings 13th International FLINS Conference on Data Science and Knowledge Engineering for Sensing Decision Support (FLINS 2018)*. 2018. URL: http://hdl.handle.net/10993/35427.

[135] Patrick Glauner, Petko Valtchev, and Radu State. "Impact of Biases in Big Data". In: *Proceedings of the 26th European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN 2018)*. 2018. URL: http://hdl.handle.net/10993/35141.

[136] Christian Grevisse, Rubén Manrique, Olga Mariño, and Steffen Rothkugel. "Knowledge Graph-based Teacher Support for Learning Material Authoring". In: *Advances in Computing - CCC 2018*. Springer, 2018. DOI: 10.1007/978-3-319-98998-3_14. URL: http://hdl.handle.net/10993/36645.

[137] Christian Grevisse, Rubén Manrique, Olga Mariño, and Steffen Rothkugel. "SoLeMiO: Semantic Integration of Learning Material in Office". In: *Proceedings of E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2018*. 2018. URL: http://hdl.handle.net/10993/36971.

[138] Christian Grevisse, Jeff Alphonse Antoine Meder, Jean Botev, and Steffen Rothkugel. "Ontology Coverage Tool and Document Browser for Learning Material Exploration". In: *2018 Thirteenth International Conference on Digital Information Management (ICDIM)*. IEEE, 2018. URL: http://hdl.handle.net/10993/36790.

[139] Siwen Guo, Sviatlana Höhn, Feiyu Xu, and Christoph Schommer. "PERSEUS: A Personalization Framework for Sentiment Categorization with Recurrent Neural Network". In: *International Conference on Agents and Artificial Intelligence , Funchal 16-18 January 2018*. 2018, p. 9. URL: http://hdl.handle.net/10993/34177.

[140] Helena Haapio, Margaret Hagan, Monica Palmirani, and Arianna Rossi. "Legal Design Patterns for Privacy". In: *Data Protection / LegalTech Proceedings of the 21st International Legal Informatics Symposium IRIS 2018*. 2018. URL: http://hdl.handle.net/10993/37453.

[141] Shohreh Haddadan, Elena Cabrio, and Serena Villata. "Annotation of Argument Components in Political Debates Data". In: *Proceedings of the Workshop on Annotation in Digital Humanities*. 2018. URL: http://hdl.handle.net/10993/37877.

[142] Sytze van Herck, Antonio Maria Fiscarelli, David Kreps, Charles Ess, Louise Leenen, and Kai Kimppa. “Mind the Gap: Gender and Computer Science Conferences”. In: *This Changes Everything - ICT and Climate Change: What Can We Do? 13th IFIP TC 9 International Conference on Human Choice and Computers, HCC13 2018. Held at the 24th IFIP World Computer Congress, WCC2018, Poznan, Poland, September 19-21, 2018, Proceedings*. Springer, 2018, pp. 232–249. ISBN: 978-3-319-99604-2. DOI: 10.1007/978-3-319-99605-9_17. URL: http://hdl.handle.net/10993/39090.

[143] Ross James Horne, Ki Yung Ahn, Shang-wei Lin, and Alwen Tiu. “Quasi-Open Bisimilarity with Mismatch is Intuitionistic”. In: *Proceedings of LICS ’18: 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, Oxford, United Kingdom, July 9-12, 2018 (LICS ’18)*. ACM, 2018, pp. 26–35. DOI: 10.1145/3209108.3209125. URL: http://hdl.handle.net/10993/37429.

[144] Abdallah Ali Zainelabden Abdallah Ibrahim. “PRESEnCE: A Framework for Monitoring, Modelling and Evaluating the Performance of Cloud SaaS Web Services”. In: *48th Annual IEEE/IFIP Intl. Conf. on Dependable Systems and Networks Workshops (DNS’18)*. IEEE Computer Society, 2018, pp. 83–86. DOI: 10.1109/DSN-W.2018.00041. URL: http://hdl.handle.net/10993/36547.

[145] Abdallah Ali Zainelabden Abdallah Ibrahim, Sébastien Varrette, and Pascal Bouvry. “On Verifying and Assuring the Cloud SLA by Evaluating the Performance of SaaS Web Services Across Multi-cloud Providers”. In: *48th Annual IEEE/IFIP Intl. Conf. on Dependable Systems and Networks Workshops (DNS’18)*. IEEE Computer Society, 2018, pp. 69–70. DOI: 10.1109/DSN-W.2018.00034. URL: http://hdl.handle.net/10993/36373.

[146] Abdallah Ali Zainelabden Abdallah Ibrahim, Sébastien Varrette, and Pascal Bouvry. “PRESENCE: Toward a Novel Approach for Performance Evaluation of Mobile Cloud SaaS Web Services”. In: *Proc. of the 32nd IEEE Intl. Conf. on Information Networking (ICOIN 2018)*. IEEE Computer Society, 2018, pp. 50–55. ISBN: 978-1-5386-2290-2. DOI: 10.1109/ICOIN.2018.8343082. URL: http://hdl.handle.net/10993/36115.

[147] Abdallah Ali Zainelabden Abdallah Ibrahim, Umer Wasim, Sébastien Varrette, and Pascal Bouvry. “PRESENCE: Performance Metrics Models for Cloud SaaS Web Services”. In: *Proc. of the 11th IEEE Intl. Conf. on Cloud Computing (CLOUD 2018)*. IEEE Computer Society, 2018. URL: http://hdl.handle.net/10993/36375.

[148] Sasan Jafarnejad, German Castignani, and Thomas Engel. “Non-intrusive Distracted Driving Detection Based on Driving Sensing Data”. In: *4th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2018)*. 2018. URL: http://hdl.handle.net/10993/34786.

[149] Sasan Jafarnejad, German Castignani, and Thomas Engel. “Revisiting Gaussian Mixture Models for Driver Identification”. In: *Proceedings of IEEE International Conference on Vehicular Electronics and Safety (ICVES) (ICVES 2018)*. 2018. URL: http://hdl.handle.net/10993/36588.

[150] Ravi Jhawar, Karim Lounis, Sjouke Mauw, and Yunior Ramirez Cruz. "Semi-automatically Augmenting Attack Trees using an Annotated Attack Tree Library". In: *Security and Trust Management. STM 2018.* Ed. by Sokratis Katsikas and Cristina Alcaraz. Springer, 2018, pp. 85–101. ISBN: 978-3-030-01141-3. DOI: 10.1007/978-3-030-01141-3_6. URL: http://hdl.handle.net/10993/37229.

[151] Matthieu Jimenez, Maxime Cordy, Yves Le Traon, and Mike Papadakis. "TUNA: TUning Naturalness-based Analysis". In: *34th IEEE International Conference on Software Maintenance and Evolution, Madrid, Spain, 26-28 September 2018*. 2018. URL: http://hdl.handle.net/10993/36136.

[152] Matthieu Jimenez, Yves Le Traon, and Mike Papadakis. "Enabling the Continous Analysis of Security Vulnerabilities with VulData7". In: *IEEE International Working Conference on Source Code Analysis and Manipulation*. 2018. URL: http://hdl.handle.net/10993/36157.

[153] Matthieu Jimenez, Thierry Titcheu Chekam, Maxime Cordy, Mike Papadakis, Marinos Kintis, Yves Le Traon, et al. "Are mutants really natural? A study on how "naturalness" helps mutant selection". In: *12th International Symposium on Empirical Software Engineering and Measurement (ESEM'18)*. 2018. URL: http://hdl.handle.net/10993/36854.

[154] Souhila Kaci, Leon van der Torre, and Serena Villata. "Preference in Abstract Argumentation". In: *Computational Models of Argument*. 2018. URL: http://hdl.handle.net/10993/36357.

[155] Monika Kaczmarek-Heß, Sybren de Kinderen, Qin Ma, and Iván Razo-Zapata. "Modeling in Support of Multi-Perspective Valuation of Smart Grid Initiatives". In: *IEEE 12th International Conference on Research Challenges in Information Science*. 2018. URL: http://hdl.handle.net/10993/37341.

[156] Georgios Kaiafas, Georgios Varisteas, Sofiane Lagraa, and Radu State. "Detecting Malicious Authentication Events Trustfully". In: *IEEE/IFIP Network Operations and Management Symposium, 23-27 April 2018, Taipei, Taiwan Cognitive Management in a Cyber World*. 2018. URL: http://hdl.handle.net/10993/35702.

[157] Ekaterina Kamlovskaya, Christoph Schommer, and Joshgun Sirajzade. "A Dynamic Associative Memory for Distant Reading". In: *International Conference on Artificial Intelligence Humanities, Book of Abstracts*. Chung-Ang University, 2018. URL: http://hdl.handle.net/10993/36612.

[158] Nida Khan, Abdelkader Lahmadi, Jerome Francois, and Radu State. "Towards a Management Plane for Smart Contracts: Ethereum Case Study". In: *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2018. DOI: 10.1109/NOMS.2018.8406326. URL: http://hdl.handle.net/10993/36826.

[159] Kisub Kim, Dongsun Kim, Tegawendé François D Assise Bissyande, Eunjong Choi, Li Li, Jacques Klein, et al. "FaCoY - A Code-to-Code Search Engine". In: *International Conference on Software Engineering (ICSE 2018)*. 2018. URL: http://hdl.handle.net/10993/36389.

[160] Sybren de Kinderen and Qin Ma. “Towards Purposeful Enterprise Modeling for Enterprise Analysis”. In: *2018 International Conference on Information Management & Management Science*. 2018. URL: http://hdl.handle.net/10993/37343.

[161] Daniel Kirchner, Christoph Benzmüller, and Edward N. Zalta. “Mechanizing Principia Logico-Metaphysica in Functional Type Theory (Extended Abstract)”. In: *3rd Conference on Artificial Intelligence and Theorem Proving (AITP 2018), Book of Abstracts*. 2018. URL: http://hdl.handle.net/10993/37447.

[162] Yann Le Corre, Johann Groszschädl, Dumitru-Daniel Dinu, Junfeng Fan, and Benedikt Gierlichs. “Micro-Architectural Power Simulator for Leakage Assessment of Cryptographic Software on ARM Cortex-M3 Processors”. In: *Constructive Side-Channel Analysis and Secure Design - 9th International Workshop, COSADE 2018, Singapore, April 23-24, 2018, Proceedings*. Springer Verlag, 2018, pp. 82–98. ISBN: 978-3-319-89640-3. DOI: 10.1007/978-3-319-89641-0. URL: http://hdl.handle.net/10993/37498.

[163] Yann Le Corre, Johann Groszschädl, Dumitru-Daniel Dinu, Junfeng Fan, and Benedikt Gierlichs. “Micro-architectural Power Simulator for Leakage Assessment of Cryptographic Software on ARM Cortex-M3 Processors”. In: *Constructive Side-Channel Analysis and Secure Design - 9th International Workshop, COSADE 2018, Singapore, April 23-24, 2018, Proceedings*. Springer, 2018, pp. 82–98. ISBN: 978-3-319-89640-3. DOI: 10.1007/978-3-319-89641-0_5. URL: http://hdl.handle.net/10993/37783.

[164] Franck Leprévost. “James Bond’s Most Secret Weapon”. In: *Proceedings of the 3rd International Conference on Applications in Information Technology*. ACM, 2018, pp. 1–2. URL: http://hdl.handle.net/10993/37313.

[165] Franck Leprévost, Nicolas Bernard, and Pascal Bouvry. “Elliptic Curves Discrete Logarithm Problem over a Finite Field Fp and p-adic Approximations”. In: *Proceedings of the 3rd International Conference on Applications in Information Technology (ICAIT-2018)*. ACM, 2018, pp. 9–15. URL: http://hdl.handle.net/10993/37314.

[166] Daoyuan Li, Jessica Lin, Tegawendé François D Assise Bissyande, Jacques Klein, and Yves Le Traon. “Extracting Statistical Graph Features for Accurate and Efficient Time Series Classification”. In: *21st International Conference on Extending Database Technology*. 2018. URL: http://hdl.handle.net/10993/35125.

[167] Li Li, Tegawendé François D Assise Bissyande, and Jacques Klein. “MoonlightBox: Mining Android API Histories for Uncovering Release-time Inconsistencies”. In: *29th IEEE International Symposium on Software Reliability Engineering (ISSRE)*. 2018, pp. 212–223. URL: http://hdl.handle.net/10993/37563.

[168] Li Li, Tegawendé François D Assise Bissyande, Haoyu Wang, and Jacques Klein. “CiD: Automating the Detection of API-related Compatibility Issues in Android Apps”. In: *International Symposium on Software Testing and Analysis (ISSTA)*. ACM, 2018, pp. 153–163. URL: http://hdl.handle.net/10993/37890.

[169] Li Li, Jun Gao, Tegawendé François D Assise Bissyande, Lei Ma, Xin Xia, and Jacques Klein. “Characterising Deprecated Android APIs”. In: *15th International Conference on Mining Software Repositories (MSR 2018)*. ACM, 2018, pp. 254–264. URL: http://hdl.handle.net/10993/37602.

[170] Beishui Liao, Marija Slavkovik, and Leon van der Torre. “Building Jiminy Cricket: An Architecture for Moral Agreements Among Stakeholders”. In: *AAAI/ACM Artificial Intelligence, Ethics and Society*. 2018. URL: http://hdl.handle.net/10993/38925.

[171] Beishui Liao and Leon van der Torre. “Representation Equivalences among Argumentation Frameworks”. In: *Computational Models of Argument*. IOS Press, 2018. URL: http://hdl.handle.net/10993/36359.

[172] Kui Liu, Dongsun Kim, Anil Koyuncu, Li Li, Tegawendé François D Assise Bissyande, and Yves Le Traon. “A Closer Look at Real-World Patches”. In: *34th IEEE International Conference on Software Maintenance and Evolution (ICSME)*. 2018. URL: http://hdl.handle.net/10993/36571.

[173] Kui Liu, Anil Koyuncu, Kisub Kim, Dongsun Kim, and Tegawendé François D Assise Bissyande. “LSRepair: Live Search of Fix Ingredients for Automated Program Repair”. In: *25th Asia-Pacific Software Engineering Conference (APSEC)*. 2018. URL: http://hdl.handle.net/10993/37414.

[174] José Miguel Lopez Becerra, Dimiter Ostrev, and Marjan Skrobot. “Forward Secrecy for SPAKE2”. In: *Provable Security*. Ed. by Joonsang Baek and Susilo Willy. Springer International Publishing, 2018, pp. 366–384. ISBN: 978-3-030-01446-9. URL: http://hdl.handle.net/10993/37390.

[175] José Miguel Lopez Becerra, Peter Roenne, Peter Ryan, and Petra Sala. “HoneyPAKEs”. In: *Security Protocols XXVI: Lecture Notes in Computer Science*. Springer International Publishing, 2018, pp. 63–77. ISBN: 978-3-030-03251-7. URL: http://hdl.handle.net/10993/37937.

[176] Rocio Lopez Perez, Florian Adamsky, Ridha Soua, and Thomas Engel. “Machine Learning for Reliable Network Attack Detection in SCADA Systems”. In: *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (IEEE TrustCom-18)*. 2018. URL: http://hdl.handle.net/10993/35719.

[177] Qin Ma and Pierre Kelsen. “Decomposing Models through Dependency Graphs”. In: *12th International Symposium on Theoretical Aspects of Software Engineering*. 2018. URL: http://hdl.handle.net/10993/37342.

[178] Abdoul Wahid Mainassara Chekaraou, Alban Rousset, Xavier Besseron, Sébastien Varrette, and Bernhard Peters. “Hybrid MPI+OpenMP Implementation of eXtended Discrete Element Method”. In: *Proc. of the 9th Workshop on Applications for Multi-Core Architectures (WAMCA’18), part of 30th Intl. Symp. on Computer Architecture and High Performance Computing (SBAC-PAD 2018)*. IEEE Computer Society, 2018. URL: http://hdl.handle.net/10993/36374.

[179] Rubén Manrique, Christian Grevisse, Olga Mariño, and Steffen Rothkugel. “Knowledge Graph-based Core Concept Identification in Learning Resources”. In: *8th Joint International Conference, JIST 2018, Awaji, Japan, November 26–28, 2018, Proceedings*. Springer, 2018. DOI: 10.1007/978-3-030-04284-4_3. URL: http://hdl.handle.net/10993/37231.

[180] Michaël Marcozzi, Sébastien Bardin, Nikolai Kosmatov, Mike Papadakis, Virgile Prevosto, and Loïc Correnson. “Time to Clean Your Test Objectives”. In: *40th International Conference on Software Engineering, May 27 - 3 June 2018, Gothenburg, Sweden*. 2018. URL: http://hdl.handle.net/10993/34949.

[181] Jabier Martinez, Jean-Sebastien Sottet, Alfonso Garcia-Frey, Tegawendé François D Assise Bissyande, Tewfik Ziadi, Jacques Klein, et al. “Towards Estimating and Predicting User Perception on Software Product Variants”. In: *17th International Conference on Software Reuse (ICSR)*. Springer, LNCS, 2018, pp. 23–40. URL: http://hdl.handle.net/10993/37597.

[182] Sjouke Mauw, Zachary Daniel Smith, Jorge Luis Toro Pozo, and Rolando Trujillo Rasua. “Automated Identification of Desynchronisation Attacks on Shared Secrets”. In: *Automated Identification of Desynchronisation Attacks on Shared Secrets*. Springer, 2018. URL: http://hdl.handle.net/10993/37278.

[183] Sjouke Mauw, Zachary Daniel Smith, Jorge Luis Toro Pozo, and Rolando Trujillo Rasua. “Distance-Bounding Protocols: Verification without Time and Location”. In: *Proceedings of IEEE Symposium on Security and Privacy (SP), San Francisco 21-23 May 2018*. IEEE Computer Society, 2018. URL: http://hdl.handle.net/10993/37277.

[184] Jaruwan Mesit, Matthias R. Brust, and Pascal Bouvry. “Lightweight Key Agreement for Wireless Sensor Networks”. In: *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. 2018. DOI: 10.1109/QRS-C.2018.00080. URL: http://hdl.handle.net/10993/38693.

[185] Jörn Migge, Josetxo Villanueva, Nicolas Navet, and Marc Boyer. “Insights on the Performance and Configuration of AVB and TSN in Automotive Ethernet Networks”. In: *Proc. Embedded Real-Time Software and Systems (ERTS 2018)*. 2018. URL: http://hdl.handle.net/10993/34055.

[186] Andrzej Mizera, Jun Pang, Hongyang Qu, and Qixia Yuan. “ASSA-PBN 3.0: Analysing Context-Sensitive Probabilistic Boolean Networks”. In: *Proceedings of the 16th International Conference on Computational Methods in Systems Biology*. Springer Science & Business Media B.V., 2018, pp. 277–284. URL: http://hdl.handle.net/10993/36591.

[187] monica palmirani monica, Michele Martoni, Arianna Rossi, Cesare Bartolini, and Livio Robaldo. “PrOnto: Privacy Ontology for Legal Reasoning”. In: *International Conference on Electronic Government and the Information Systems Perspective*. 2018. URL: http://hdl.handle.net/10993/37454.

[188] Ludovic Mouline, Amine Benelallam, François Fouquet, Johann Bourcier, and Olivier Barais. “A Temporal Model for Interactive Diagnosis of Adaptive Systems”. In: *2018 IEEE International Conference on Autonomic Computing (ICAC)*. 2018. URL: http://hdl.handle.net/10993/36721.

[189] Mohamed Nizar Msadek, Ridha Soua, Latif Ladid, and Thomas Engel. “Advancing the Security of Trustworthy Self-IoT (Position Paper)”. In: *International Conference on Smart Applications, Communications and Networking (SmartNets)*. 2018. URL: http://hdl.handle.net/10993/37042.

[190] Sandro Mund, Raphaël Frank, Georgios Varisteas, and Radu State. "Visualizing the Learning Progress of Self-Driving Cars". In: *21st International Conference on Intelligent Transportation Systems*. IEEE, 2018, pp. 2358–2363. ISBN: 978-1-7281-0322-8. URL: http://hdl.handle.net/10993/37215.

[191] Nicolas Navet, Jörn Migge, Josetxo Villanueva, and Marc Boyer. "Pre-shaping Bursty Transmissions under IEEE802.1Q as a Simple and Efficient QoS Mechanism". In: *Proc. WCX World Congress Experience*. SAE, 2018. DOI: 10.4271/2018-01-0756. URL: http://hdl.handle.net/10993/37457.

[192] Gilles Neyens and Denis Zampunieris. "A rule-based approach for self-optimisation in autonomic eHealth systems". In: *Workshop Proceedings ot the 6th International Workshop on "Self-Optimisation in Autonomic & Organic Computing Systems" in ARCS 2018 - 31st International Conference on Architecture of Computing Systems, Braunschweig, Germany, 09 - 12 April, 2018*. 2018, pp. 151–154. ISBN: 978-3-8007-4559-3. URL: http://hdl.handle.net/10993/35484.

[193] Robert Norvill, Beltran Fiz Pontiveros, Radu State, and Andrea Cullen. "Visual emulation for Ethereum's virtual machine". In: *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2018. DOI: 10.1109/NOMS.2018.8406332. URL: http://hdl.handle.net/10993/36756.

[194] Tiago Oliveira, Jérémie Dauphin, Ken Satoh, Shusaku Tsumoto, and Paulo Novais. "Argumentation with Goals for Clinical Decision Support in Multimorbidity". In: *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*. 2018. URL: http://hdl.handle.net/10993/36364.

[195] Maya Alexandra Olszewski, Jeff Alphonse Antoine Meder, Emmanuel Kieffer, Raphaël Bleuse, Martin Rosalie, Grégoire Danoy, et al. "Visualizing the Template of a Chaotic Attractor". In: *26th International Symposium on Graph Drawing and Network Visualization (GD 2018)*. 2018. URL: http://hdl.handle.net/10993/37764.

[196] Monica Palmirani, Arianna Rossi, Michele Martoni, and Hagan Margaret. "A Methodological Framework to Design a Machine-Readable Privacy Icon Set". In: *Data Protection / LegalTech Proceedings of the 21st International Legal Informatics Symposium IRIS 2018*. 2018. URL: http://hdl.handle.net/10993/37299.

[197] Mike Papadakis, Donghwan Shin, Shin Yoo, and Doo-Hwan Bae. "Are Mutation Scores Correlated with Real Fault Detection? A Large Scale Empirical study on the Relationship Between Mutants and Real Faults". In: *40th International Conference on Software Engineering, May 27 - 3 June 2018, Gothenburg, Sweden*. 2018. URL: http://hdl.handle.net/10993/34950.

[198] Mike Papadakis, Thierry Titcheu Chekam, and Yves Le Traon. "Mutant Quality Indicators". In: *13th International Workshop on Mutation Analysis (MUTATION'18)*. 2018. URL: http://hdl.handle.net/10993/34352.

[199] Katerina Papaioannou, Martin Theobald, and Michael Böhlen. "Supporting Set Operations in Temporal-Probabilistic Databases". In: *Proceedings of the 34th IEEE International Conference on Data Engineering, ICDE 2018, Paris, France, April 16-19, 2018*. IEEE Computer Society, 2018, pp. 1180–1191. ISBN: 978-1-5386-5520-7. URL: http://hdl.handle.net/10993/37837.

[200] Xavier Parent, Leon van der Torre, and Gabriella Pigozzi. "Input/output logics with a consistency check". In: *Deontic Logic and Normative Systems (DEON 2018)*. Ed. by Jan Broersen, Cleo Condoravdi, and Shyam Nair. College Publications, 2018. ISBN: 978-1-84890-278-7. URL: http://hdl.handle.net/10993/37887.

[201] Soumya Paul, Jun Pang, and Cui Su. "On the Full Control of Boolean Networks". In: *Proceedings of the 16th International Conference on Computational Methods in Systems Biology*. Springer Science & Business Media B.V., 2018, pp. 313–317. URL: http://hdl.handle.net/10993/36592.

[202] Soumya Paul, Jun Pang, and Cui Su. "Towards the Existential Control of Boolean Networks: A Preliminary Report". In: *Proceedings of the 4th International Symposium on Dependable Software Engineering. Theories, Tools, and Applications*. Springer Science & Business Media B.V., 2018, pp. 142–149. URL: http://hdl.handle.net/10993/36596.

[203] Soumya Paul, Cui Su, Jun Pang, and Andrzej Mizera. "A Decomposition-based Approach towards the Control of Boolean Networks". In: *Proceedings of the 2018 ACM International Conference on Bioinformatics, Computational Biology, and Health Informatics*. ACM, 2018. URL: http://hdl.handle.net/10993/36590.

[204] Noé Picard, Jean-Noël Colin, and Denis Zampunieris. "Context-aware and Attribute-based Access Control Applying Proactive Computing to IoT System". In: *Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018)*. SCITEPRESS, 2018, pp. 333–339. ISBN: 978-989-758-296-7. DOI: 10.5220/0006815803330339. URL: http://hdl.handle.net/10993/35604.

[205] Andreia Pinto Costa, Louise Charpiot, Francisco Javier Rodriguez Lera, Pouyan Ziafati, Aida Nazarikhorram, Leon van der Torre, et al. "More Attention and Less Repetitive and Stereotyped Behaviors using a Robot with Children with Autism". In: *27th IEEE International Symposium on Robot and Human Interactive Communication, RO-MAN 2018, Nanjing, China, August 27-31, 2018*. 2018. DOI: 10.1109/ROMAN.2018.8525747. URL: http://hdl.handle.net/10993/37880.

[206] Vincent Rahli, Liron Cohen, and Mark Bickford. "A Verified Theorem Prover Backend Supported by a Monotonic Library". In: *LPAR 2018*. 2018. URL: http://hdl.handle.net/10993/37406.

[207] Vincent Rahli, Ivana Vukotic, Marcus Volp, and Paulo Verissimo. "Velisarios: Byzantine Fault-Tolerant Protocols Powered by Coq". In: *ESOP 2018*. 2018. URL: http://hdl.handle.net/10993/35304.

[208] Iván Razo-Zapata, Eng Chew, Qin Ma, Loïc Gammaitoni, and Henderik Proper. “Enabling Value Co-Creation in Customer Journeys with VIVA”. In: *Joint International Conference of Service Science and Innovation and Serviceology*. 2018. URL: http://hdl.handle.net/10993/37344.

[209] Mostafa Rezazad, Matthias R. Brust, Mohammad Akbari, Pascal Bouvry, and Ngai-Man Cheung. “Detecting Target-Area Link-Flooding DDoS Attacks using Traffic Analysis and Supervised Learning”. In: *Advances in Intelligent Systems and Computing*. 2018. DOI: 10.1007/978-3-030-03405-4_12. URL: http://hdl.handle.net/10993/38713.

[210] Tjitze Rienstra, Matthias Thimm, Beishui Liao, and Leon van der Torre. “Probabilistic Abstract Argumentation Based on SCC Decomposability”. In: *Principles of Knowledge Representation and Reasoning: Proceedings of the Sixteenth International Conference, KR 2018, Tempe, Arizona 30 October - 2 November 2018*. 2018. URL: http://hdl.handle.net/10993/37873.

[211] Benoît Ries, Alfredo Capozucca, and Nicolas Guelfi. “Messir: A Text-First DSL-Based Approach for UML Requirements Engineering (Tool Demo)”. In: *Proceedings of the 11th ACM SIGPLAN International Conference on Software Language Engineering SLE’18*. 2018. DOI: 10.1145/3276604.3276614. URL: http://hdl.handle.net/10993/37375.

[212] Francisco Javier Rodriguez Lera, F. Martín-Rico, and V. Matelián-Olivera. “Generating symbolic representation from sensor data: Inferring knowledge in robotics competitions”. In: *2018 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC)*. 2018. DOI: 10.1109/ICARSC.2018.8374193. URL: http://hdl.handle.net/10993/37251.

[213] Stefan Schiffner, Bettina Berendt, Triin Siil, Martin Degeling, Robert Riemann, Florian Schaub, et al. “Towards a Roadmap for Privacy Technologies and the General Data Protection Regulation : A transatlantic initiative”. In: *proceedings of the Annual Privacy Forum 2018*. Ed. by Manel Medina. 2018. URL: http://hdl.handle.net/10993/35869.

[214] Wazen Shbair, Mathis Steichen, Jérôme François, and Radu State. “Blockchain Orchestration and Experimentation Framework: A Case Study of KYC”. In: *The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018*. 2018. URL: http://hdl.handle.net/10993/35467.

[215] Joshgun Sirajzade and Christoph Schommer. “Mind and Language. AI in an Example of Similar Patterns of Luxembourgish Language”. In: *International Conference on Artificial Intelligence Humanities, Book of Abstracts*. Chung-Ang University, 2018, p. 2. URL: http://hdl.handle.net/10993/36609.

[216] Ridha Soua, Maria Rita Palattella, and Thomas Engel. “IoT Application Protocols Optimisation for Future Integrated M2M-Satellite Networks”. In: *IoT Application Protocols Optimisation for Future Integrated M2M-Satellite Networks*. 2018. URL: http://hdl.handle.net/10993/37041.

[217] Ridha Soua, Ion Turcanu, Florian Adamsky, Detlef Führer, and Thomas Engel. "Multi-Access Edge Computing for Vehicular Networks: a Position Paper". In: *2018 IEEE Global Communications Conference: Workshops: Vehicular Networking and Intelligent Transportation Systems*. 2018. DOI: 10.1109/GLOCOMW.2018.8644392. URL: http://hdl.handle.net/10993/36464.

[218] Alexander Steen and Christoph Benzmüller. "The Higher-Order Prover Leo-III". In: *Automated Reasoning 9th International Joint Conference, IJCAR 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 14-17, 2018, Proceedings*. Springer, Cham, 2018, pp. 108–116. ISBN: 978-3-319-94204-9. DOI: 10.1007/978-3-319-94205-6_8. URL: http://hdl.handle.net/10993/37461.

[219] Mathis Steichen, Beltran Fiz Pontiveros, Robert Norvill, Wazen Shbair, and Radu State. "Blockchain-Based, Decentralized Access Control for IPFS". In: *The 2018 IEEE International Conference on Blockchain (Blockchain-2018)*. IEEE, 2018, pp. 1499–1506. URL: http://hdl.handle.net/10993/36641.

[220] Thierry Titcheu Chekam, Mike Papadakis, Tegawendé François D Assise Bissyande, and Yves Le Traon. "Predicting the Fault Revelation Utility of Mutants". In: *40th International Conference on Software Engineering, Gothenburg, Sweden, May 27 - 3 June 2018*. 2018. URL: http://hdl.handle.net/10993/35329.

[221] 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". In: *A New Modelling Framework over Temporal Graphs for Collaborative Mobility Recommendation Systems*. 2018. URL: http://hdl.handle.net/10993/32959.

[222] Mattia Tomasoni, Andrea Capponi, Claudio Fiandrino, Dzmitry Kliazovich, Fabrizio Granelli, and Pascal Bouvry. "Profiling Energy Efficiency of Mobile Crowdsensing Data Collection Frameworks for Smart City Applications". In: *The 6th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (IEEE Mobile Cloud 2018)*. 2018. URL: http://hdl.handle.net/10993/34424.

[223] Georgios Varisteas, Tigran Avanesov, and Radu State. "Distributed C++-Python embedding for fast predictions and fast prototyping". In: *Proceedings of the Second Workshop on Distributed Infrastructures for Deep Learning*. 2018. ISBN: 978-1-4503-6119-4. URL: http://hdl.handle.net/10993/37854.

[224] Itzel Vazquez Sandoval and Gabriele Lenzini. "Experience report: How to extract security protocols' specifications from C libraries". In: *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*. IEEE, 2018. ISBN: 978-1-5386-2666-5. URL: http://hdl.handle.net/10993/36266.

[225] Itzel Vazquez Sandoval, Gabriele Lenzini, and Borce Stojkovski. "A Protocol to Strengthen Password-Based Authentication". In: *Emerging Technologies for Authorization and Authentication - ESORICS 2018 International Workshops*. 2018. URL: http://hdl.handle.net/10993/36650.

[226] Bharathi Vijayakumar, Sviatlana Höhn, and Christoph Schommer. “Quizbot: Exploring Formative Feedback with Conversational Interfaces”. In: *Proceedings of the*. Springer, 2018. URL: http://hdl.handle.net/10993/37859.

[227] Piergiorgio Vitello, Andrea Capponi, Claudio Fiandrino, Paolo Giaccone, Dzmitry Kliazovich, and Pascal Bouvry. “High-Precision Design of Pedestrian Mobility for Smart City Simulators”. In: *IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018*. 2018. URL: http://hdl.handle.net/10993/34432.

[228] Piergiorgio Vitello, Andrea Capponi, Claudio Fiandrino, Paolo Giaccone, Dzmitry Kliazovich, Ulrich Sorger, et al. “Collaborative Data Delivery for Smart City-oriented Mobile Crowdsensing Systems”. In: *IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, UAE, 2018*. 2018. URL: http://hdl.handle.net/10993/36943.

[229] Marcus Volp and Paulo Verissimo. “Intrusion-Tolerant Autonomous Driving”. In: *2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC)*. 2018. DOI: 10.1109/ISORC.2018.00026. URL: http://hdl.handle.net/10993/37811.

[230] Qingju Wang, Lorenzo Grassi, and Christian Rechberger. “Zero-Sum Partitions of PHOTON Permutations”. In: *Topics in Cryptology - CT-RSA 2018 - The Cryptographers’ Track at the RSA Conference 2018, San Francisco, CA, USA, April 16-20, 2018 Proceedings*. Ed. by Nigel P. Smart. Springer, 2018, pp. 279–299. URL: http://hdl.handle.net/10993/37218.

[231] Qingju Wang, Yonglin Hao, Yosuke Todo, Chaoyun Li, Takanori Isobe, and Willi Meier. “Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly”. In: *38th Annual International Cryptology Conference, Santa Barbara 19-23 Aug 2018*. Springer, 2018, pp. 275–305. DOI: https://link.springer.com/chapter/10.1007%2F978-3-319-96884-1_10. URL: http://hdl.handle.net/10993/37220.

[232] Alexander Yakubov, Wazen Shbair, and Radu State. “BlockPGP: A Blockchain-based Framework for PGP Key Servers”. In: *The Sixth International Symposium on Computing and Networking*. IEEE Xplore, 2018. URL: http://hdl.handle.net/10993/37533.

[233] Alexander Yakubov, Wazen Shbair, Anders Wallbom, David Sanda, and Radu State. “A Blockchain-Based PKI Management Framework”. In: *The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23-27 April 2018*. 2018. URL: http://hdl.handle.net/10993/35468.

[234] Yang Zhang, Mathias Humbert, Tahleen Rahman, Cheng-Te Li, Jun Pang, and Michael Backes. “Tagvisor: A privacy advisor for sharing hashtags”. In: *Proceedings of The Web Conference 2018 (WWW’18)*. ACM Press, 2018, pp. 287–296. URL: http://hdl.handle.net/10993/35884.

[235] Yaqiong Zheng, Siwen Guo, and Christoph Schommer. “An Approach to Incorporate Emotions in a Chatbot with Seq2Seq Model”. In: *Benelux Conference on Artificial Intelligence, ‘s-Hertogenbosch 8-9 November 2018*. 2018. URL: http://hdl.handle.net/10993/37210.

A.5 Theses

[236] Kolawole John Adebayo. “MULTIMODAL LEGAL INFORMATION RETRIEVAL”. PhD thesis. University of Luxembourg, Luxembourg and Kolawole Adebayo, Bologna, Italy, 2018. URL: http://hdl.handle.net/10993/36614.

[237] Alessia Calafiore. “REPRESENTING THE SOCIAL CHARACTER OF PLACES: ONTOLOGY MODELS OF THE URBAN ENVIRONMENT”. PhD thesis. University of Luxembourg, Luxembourg, 2018. URL: http://hdl.handle.net/10993/37680.

[238] Thierry Derrmann. “Mobile Network Data Analytics for Intelligent Transportation Systems”. PhD thesis. University of Luxembourg, Luxembourg, 2018. URL: http://hdl.handle.net/10993/37029.

[239] Winfried Höhn. “Semiautomatische Annotation von Orten in digitalisierten Altkarten”. PhD thesis. University of Luxembourg, Luxembourg, 2018. URL: http://hdl.handle.net/10993/37233.

[240] Matthieu Jimenez. “Evaluating Vulnerability Prediction Models”. PhD thesis. University of Luxembourg, Luxembourg, 2018. URL: http://hdl.handle.net/10993/36869.

[241] Johannes Klein. “Integrating User- and System-Centric Perspectives into Collaborative Compound Document Authoring”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2018. URL: http://hdl.handle.net/10993/34542.

[242] Patrick Kobou Ngani. “Active Harmonics Compensation in Smart Grids”. PhD thesis. University of Luxembourg, Luxembourg, 2018. URL: http://hdl.handle.net/10993/34280.

[243] Daoyuan Li. “Transforming Time Series for Efficient and Accurate Classification”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2018. URL: http://hdl.handle.net/10993/34046.

[244] Steve Muller. “Risk Monitoring and Intrusion Detection for Industrial Control Systems”. PhD thesis. University of Luxembourg, Luxembourg, 2018. URL: http://hdl.handle.net/10993/36171.

[245] Dayana Pierina Brustolin Spagnuelo. “Defining, Measuring, and Enabling Transparency for Electronic Medical Systems”. PhD thesis. University of Luxembourg, Luxembourg, 2018. URL: http://hdl.handle.net/10993/38915.

[246] Gabriele Pozzetti. “A Dual-Grid Multiscale Approach to CFD-DEM Couplings for Multiphase Flow”. PhD thesis. University of Luxembourg, Luxembourg, 2018. URL: http://hdl.handle.net/10993/36897.

[247] Alejandro Sanchez Guinea. “Engineering Smart Software Services for Intelligent Pervasive Systems”. PhD thesis. University of Luxembourg, Luxembourg city, Luxembourg, 2018. URL: http://hdl.handle.net/10993/36613.

[248] Salvatore Signorello. “A multifold approach to address the security issues of stateful forwarding mechanisms in Information-Centric Networks.” PhD thesis. University of Luxembourg University of Lorraine, Luxembourg Nancy, Luxembourg France, 2018. URL: http://hdl.handle.net/10993/36478.

[249] Danilo Spano. “Advanced Symbol-level Precoding Schemes for Interference Exploitation in Multi-antenna Multi-user Wireless Communications”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2018. URL: http://hdl.handle.net/10993/36227.

[250] Iraklis Symeonidis. “Analysis and Design of Privacy-Enhancing Information Sharing Systems”. PhD thesis. KU Leuven, Leuven, Belgium, 2018. URL: http://hdl.handle.net/10993/37607.

[251] Jun Wang. “Privacy-preserving Recommender Systems Facilitated By The Machine Learning Approach”. PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2018. URL: http://hdl.handle.net/10993/37026.

[252] Muhammad Umer Wasim. “Design and Implementation of Legal Protection for Trade Secrets in Cloud Brokerage Architectures relying on Blockchains”. PhD thesis. University of Luxembourg, Belval, Luxembourg, 2018. URL: http://hdl.handle.net/10993/36660.

A.6 Tech Reports

[253] Alexandre Bartel, Jacques Klein, and Yves Le Traon. *MUSTI: Dynamic Prevention of Invalid Object Initialization Attacks*. Tech. rep. Université du Luxembourg, 2018. URL: http://hdl.handle.net/10993/36085.

[254] Christoph Benzmüller, Ali Farjami, and Xavier Parent. *Faithful Semantical Embedding of a Dyadic Deontic Logic in HOL*. Tech. rep. 2018. URL: http://hdl.handle.net/10993/36397.

[255] Pascal Bouvry, Raymond Bisdorff, Christoph Schommer, Ulrich Sorger, Martin Theobald, and Leon van der Torre. *Proceedings - 2017 ILILAS Distinguished Lectures*. Tech. rep. University of Luxembourg, 2018. URL: http://hdl.handle.net/10993/33848.

[256] Giovanni Casini, Thomas Meyer, Ivan Varzinczak, and Richard Booth. *On Rational Entailment for Propositional Typicality Logic*. Tech. rep. ArXiv, 2018. URL: http://hdl.handle.net/10993/37863.

[257] Marcos Cramer and Jérémie Dauphin. *Technical online appendix to ”A Structured Argumentation Framework for Modeling Debates in the Formal Sciences”*. Tech. rep. University of Luxembourg, 2018. URL: http://hdl.handle.net/10993/35722.

[258] Jérémie Dauphin, Marcos Cramer, and Leon van der Torre. *A Dynamic Approach for Combining Abstract Argumentation Semantics – Technical Report*. Tech. rep. University of Luxembourg, 2018. URL: http://hdl.handle.net/10993/36754.

[259] Jérémie Dauphin, Marcos Cramer, and Leon van der Torre. *Abstract and Concrete Decision Graphs for Choosing Extensions of Argumentation Frameworks - Technical Report*. Tech. rep. University of Luxembourg, 2018. URL: http://hdl.handle.net/10993/36335.

[260] Nader Samir Labib, Chao Liu, Saharnaz Dilmaghani, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. *White Paper: Data Protection and Privacy in Smart ICT - Scientific Research and Technical Standardization*. Tech. rep. ILNAS, 2018. DOI: 10.13140/RG.2.2.32160.23045. URL: http://hdl.handle.net/10993/37276.

[261] Sébastien Varrette. *Tutorial Big Data Analytics: Overview and Practical Examples*. Tech. rep. EU COST NESUS, 3rd NESUS Winter School, PhD Symposium on Data Science, and Heterogeneous Computing, 2018. URL: http://hdl.handle.net/10993/36376.

A.7 Miscellaneous

[262] Arash Atashpendar, Marc Beunardeau, Aisling Connolly, Rémi Géraud, David Mestel, A.W. (Bill) Roscoe, et al. *From Clustering Supersequences to Entropy Minimizing Subsequences for Single and Double Deletions*. 2018. URL: http://hdl.handle.net/10993/36636.

[263] Arash Atashpendar, David Mestel, A.W. (Bill) Roscoe, and Peter Ryan. *A Proof of Entropy Minimization for Outputs in Deletion Channels via Hidden Word Statistics*. 2018. URL: http://hdl.handle.net/10993/36637.

[264] Alexandre Bartel. *Exploitation du CVE-2015-4843*. 2018. URL: http://hdl.handle.net/10993/38065.

[265] Alexandre Bartel and John Doe. *Twenty years of Escaping the Java Sandbox*. 2018. URL: http://hdl.handle.net/10993/38190.

[266] Alexandre Bartel, Jacques Klein, and Yves Le Traon. *Désérialisation Java : Une brève introduction*. 2018. URL: http://hdl.handle.net/10993/38067.

[267] Alexandre Bartel, Jacques Klein, and Yves Le Traon. *Fini le Bac à Sable. Avec le CVE-2017-3272, devenez un grand!* 2018. URL: http://hdl.handle.net/10993/38066.

[268] Christoph Benzmüller, Ali Farjami, and Xavier Parent. *A Faithful Semantic Embedding of the Dyadic Deontic Logic E in HOL*. 2018. URL: http://hdl.handle.net/10993/36394.

[269] Christoph Benzmüller and Xavier Parent. *First Experiments with a Flexible Infrastructure for Normative Reasoning*. 2018. URL: http://hdl.handle.net/10993/37466.

[270] Christoph Benzmüller and Xavier Parent. *I/O Logic in HOL — First Steps*. 2018. URL: http://hdl.handle.net/10993/37467.

[271] Xavier Besseron and Sébastien Varrette. *High Performance Computing and Big Data analytics in Luxembourg: Overview and Challenges in the EuroHPC horizon*. 2018. URL: http://hdl.handle.net/10993/36398.

[272] Raymond Bisdorff. *Computational Statistics: Lecture notes and presentation slides*. 2018. URL: http://hdl.handle.net/10993/37870.

[273] Raymond Bisdorff. *Tutorials for using the Digraph3 Python software collection*. 2018. URL: http://hdl.handle.net/10993/37886.

[274] Raymond Bisdorff. *UL HPC users'session: Mastering big data*. 2018. URL: http://hdl.handle.net/10993/36270.

[275] Pascal Bouvry, Sébastien Varrette, Valentin Plugaru, Sarah Peter, Hyacinthe Cartiaux, and Clément Parisot. *Large-scale research data management: Road to GDPR compliance*. 2018. URL: http://hdl.handle.net/10993/36113.

[276] Hyacinthe Cartiaux, Sébastien Varrette, Valentin Plugaru, Sarah Diehl, Clément Parisot, and Pascal Bouvry. *UL HPC Tutorial: HPC workflow with sequential jobs*. 2018. URL: http://hdl.handle.net/10993/36446.

[277] Stanislav Dashevskyi, Olga Gadyatskaya, Aleksandr Pilgun, and Zhauniarovich Yury. *The Influence of Code Coverage Metrics on Automated Testing Efficiency in Android*. 2018. DOI: 10.1145/3243734.3278524. URL: http://hdl.handle.net/10993/37077.

[278] Sarah Diehl, Sébastien Varrette, Valentin Plugaru, Clément Parisot, Hyacinthe Cartiaux, and Pascal Bouvry. *UL HPC Tutorial: Building [custom] software with EasyBuild on the UL HPC platform*. 2018. URL: http://hdl.handle.net/10993/36448.

[279] Georgios Fotiadis and Elisavet Konstantinou. *TNFS Resistant Families of Pairing-Friendly Elliptic Curves*. 2018. URL: http://hdl.handle.net/10993/39265.

[280] Georgios Fotiadis and Chloe Martindale. *Optimal TNFS-secure pairings on elliptic curves with even embedding degree*. 2018. URL: http://hdl.handle.net/10993/39266.

[281] Christian Franck. *A Trellis-Based SAT Problem*. 2018. URL: http://hdl.handle.net/10993/39383.

[282] Jun Gao, Li Li, Kong Pingfan, Bissyandé Tegawendé F., and Klein Jacques. *On Vulnerability Evolution in Android Apps*. 2018. URL: http://hdl.handle.net/10993/38919.

[283] Ziya Alper Genç. *Crypren Decryptor*. 2018. URL: http://hdl.handle.net/10993/37570.

[284] Aurélien Ginolhac, Joseph Emeras, Sébastien Varrette, Valentin Plugaru, Sarah Diehl, Clément Parisot, et al. *UL HPC Tutorial: Statistical Computing with R*. 2018. URL: http://hdl.handle.net/10993/36456.

[285] Sofiane Lagraa, Jérémy Henri J. Charlier, and Radu State. *Knowledge Discovery Approach from Blockchain, Crypto-currencies, and Financial Stock Exchanges*. 2018. URL: http://hdl.handle.net/10993/36518.

[286] Pierre Leyers. *Maschinen nach menschlichem Vorbild*. 2018. URL: http://hdl.handle.net/10993/37234.

[287] Chao Liu, Sébastien Varrette, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. *A Standardized Broker Model in Smart Cities*. 2018. URL: http://hdl.handle.net/10993/37479.

[288] José Miguel Lopez Becerra, Peter Ryan, Petra Sala, and Marjan Skrobot. *An Offline Dictionary Attack Against zkPAKE Protocol*. 2018. DOI: 10.1145/1235. URL: http://hdl.handle.net/10993/37403.

[289] Nicolas Navet. *A journey into time-triggered communication protocols with a focus on Ethernet TSN*. 2018. URL: http://hdl.handle.net/10993/37456.

[290] Dimiter Ostrev. *Composable, Unconditionally Secure Message Authentication without any Secret Key*. 2018. URL: http://hdl.handle.net/10993/37480.

[291] Clément Parisot, Hyacinthe Cartiaux, Sébastien Varrette, Valentin Plugaru, Sarah Diehl, and Pascal Bouvry. *UL HPC Tutorial: Getting Started on the Uni.lu HPC platform*. 2018. URL: http://hdl.handle.net/10993/36445.

[292] Clément Parisot, Sarah Diehl, Sébastien Varrette, Valentin Plugaru, Hyacinthe Cartiaux, and Pascal Bouvry. *UL HPC Tutorial: (Advanced) Prototyping with Python*. 2018. URL: http://hdl.handle.net/10993/36453.

[293] Balazs Pejo, Qiang Tang, and Biczok Gergely. *The Price of Privacy in Collaborative Learning*. 2018. DOI: 10.1145/3243734.3278525. URL: http://hdl.handle.net/10993/36651.

[294] Aleksandr Pilgun, Olga Gadyatskaya, Stanislav Dashevskyi, Yury Zhauniarovich, and Artsiom Kushniarou. *DEMO: An Effective Android Code Coverage Tool*. 2018. DOI: 10.1145/3243734.3278484. URL: http://hdl.handle.net/10993/37050.

[295] Valentin Plugaru, Xavier Besseron, Sébastien Varrette, Sarah Diehl, Clément Parisot, Hyacinthe Cartiaux, et al. *UL HPC Tutorial: Performance engineering - HPC debugging and profilling*. 2018. URL: http://hdl.handle.net/10993/36449.

[296] Valentin Plugaru, Sarah Diehl, Sébastien Varrette, Clément Parisot, Hyacinthe Cartiaux, and Pascal Bouvry. *UL HPC Tutorial: Bio-informatics workflows and applications*. 2018. URL: http://hdl.handle.net/10993/36452.

[297] Valentin Plugaru, Sébastien Varrette, Sarah Diehl, Clément Parisot, Hyacinthe Cartiaux, and Pascal Bouvry. *UL HPC Tutorial: Advanced Job scheduling with SLURM and OAR*. 2018. URL: http://hdl.handle.net/10993/36447.

[298] Valentin Plugaru, Sébastien Varrette, Sarah Diehl, Clément Parisot, Hyacinthe Cartiaux, and Pascal Bouvry. *UL HPC Tutorial: Basic and Advanced scientific computing using MATLAB*. 2018. URL: http://hdl.handle.net/10993/36454.

[299] Valentin Plugaru, Sébastien Varrette, Sarah Diehl, Clément Parisot, Hyacinthe Cartiaux, and Pascal Bouvry. *UL HPC Tutorial: HPC Containers with Singularity*. 2018. URL: http://hdl.handle.net/10993/36458.

[300] Valentin Plugaru, Sébastien Varrette, Sarah Diehl, Clément Parisot, Hyacinthe Cartiaux, and Pascal Bouvry. *UL HPC Tutorial: Multi-Physics workflows: test cases on CFD / MD / Chemistry applications*. 2018. URL: http://hdl.handle.net/10993/36451.

[301] Benoît Ries, Alfredo Capozucca, and Nicolas Guelfi. *Messir: A Text-First DSL-Based Approach for UML Requirements Engineering (Artifact Evaluation) accepted at the 11th ACM SIGPLAN International Conference on Software Language Engineering (SLE)*. 2018. DOI: 10.5281/zenodo.1458158. URL: http://hdl.handle.net/10993/37370.

[302] Benoît Ries, Alfredo Capozucca, and Nicolas Guelfi. *Messir: A Text-First DSL-Based Approach for UML Requirements Engineering (Tool Demo), in ACM SIGPLAN conference on Systems, Programming, Languages and Applications: Software for Humanity (SPLASH)*. 2018. URL: http://hdl.handle.net/10993/37374.

[303] Peter Roenne, Peter Ryan, and Marie-Laure Zollinger. *Electryo, In-person Voting with Transparent Voter Verifiability and Eligibility Verifiability*. 2018. URL: http://hdl.handle.net/10993/37857.

[304] Nader Samir Labib, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. *On Standardised UAV Localisation and Tracking Systems in Smart Cities*. 2018. URL: http://hdl.handle.net/10993/37265.

[305] Sébastien Varrette. *Luxembourg Proposals for Large Scale Architectures for Data Science*. 2018. URL: http://hdl.handle.net/10993/36372.

[306] Sébastien Varrette. *Next Generation Computing and Storage at Scale: Overview and Implementation within the European HPC strategy*. 2018. URL: http://hdl.handle.net/10993/36116.

[307] Sébastien Varrette, Pascal Bouvry, Valentin Plugaru, Sarah Diehl, Clément Parisot, and Hyacinthe Cartiaux. *Overview and Challenges of the UL HPC Facility at the EuroHPC Horizon*. 2018. URL: http://hdl.handle.net/10993/36687.

[308] Sébastien Varrette, Valentin Plugaru, Sarah Diehl, Clément Parisot, Hyacinthe Cartiaux, and Pascal Bouvry. *UL HPC Tutorial: Big Data Applications (batch, stream, hybrid) with Hadoop and Spark*. 2018. URL: http://hdl.handle.net/10993/36455.

[309] Sébastien Varrette, Valentin Plugaru, Sarah Diehl, Clément Parisot, Hyacinthe Cartiaux, and Pascal Bouvry. *UL HPC Tutorial: Machine and Deep Learning on the UL HPC Platform*. 2018. URL: http://hdl.handle.net/10993/36457.

[310] Sébastien Varrette, Valentin Plugaru, Sarah Diehl, Clément Parisot, Hyacinthe Cartiaux, and Pascal Bouvry. *UL HPC Tutorial: Parallel computations with OpenMP/MPI*. 2018. URL: http://hdl.handle.net/10993/36450.

[311] Jun Wang, Afonso Arriaga, Qiang Tang, and Peter Ryan. *Facilitating Privacy-preserving Recommendation-as-a-Service with Machine Learning*. 2018. DOI: 10.1145/3243734.3278504. URL: http://hdl.handle.net/10993/37324.

[312] Teng Andrea Xu, Florian Adamsky, Ion Turcanu, Ridha Soua, Christian Köbel, Thomas Engel, et al. *Poster: Performance Evaluation of an Open-Source Audio-Video Bridging/Time-Sensitive Networking Testbed for Automotive Ethernet*. 2018. DOI: 10.1109/VNC.2018.8628414. URL: http://hdl.handle.net/10993/37006.

[313] Marie-Laure Zollinger. *Selene User Interface*. 2018. URL: http://hdl.handle.net/10993/38534.

Appendix B

Research Projects

This chapter lists research projects that were ongoing during 2018, and whose principal investigator is a CSC member. It is structured to summarize the projects by funding source.

- EC - Erasmus+ - KA2
- EC - H2020
- EU - COST Action
- ESA
- FNR
- FNR and UL
- FNR - AFR
- FNR - AFR PhD
- FNR - AFR PhD and ILNAS
- FNR - CORE
- FNR - CORE and NCBR
- FNR - CORE - Core Junior
- FNR - Industrial Fellowships
- FNR - INTER
- FNR - JUMP
- FNR - PRIDE
- UL
- UL and External Organisation Funding
- SnT partnership with pEp security
- ONRG - NICOP
- External Organisation Funding

B.1 EC - Erasmus+ - KA2 Projects

Modernisation of Higher Education in central Asia through new technologies

Acronym:	HiedTec
Reference:	R-AGR-3536-10
PI:	Thomas ENGEL
Funding:	European Commission - Erasmus+ - Key Action 2: Cooperation for innovation and the exchange of good practices
Budget:	988,773.00 €
Duration:	15 Nov 2018 – 14 Nov 2021
Members:	• Thomas ENGEL (Principal Investigator) • Aurel MACHALEK (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Latif LADID (Program Coordinator)
Area:	Communicative Systems
Partners:	• Ala-Too Intenational University • Almaty Technological University • Andijan Machine-Building Institute • Innovativa University of Euroasia • International University for the Humanities and Development • Issykkul State University named after K. Tynystanov • Khorog State University • Kyrgyz State Technical University • L.N.Gumilyov Euroasian National University • Ministry of Education and Science of the Kyrgyz Republic • Ministry of Education and Science of the Rep. of Kazakhstan • Ministry of Education and Science of the Rep. of Tajikistan • Ministry of Education of Turkmenistan Turkmenistan • Ministry of Higher and Secondary specialized education • Oguz Han Engineering and Technology University • State Power Engineering Institute of Turkmenistan • Tajik Technical University • Tashkent State University of Economics • Tashkent University of Information Technology • Technological University of Tajikistan • University of Coimbra • University of Pavia • University of Russe

Description

REASONS:
In order to respond to:

- the Digital Transformation of Industries (Industry 4.0), which also requires DIGITAL TRANSFORMATION OF EDUCATION with overtaking pace, the consortium will develop Concepts of adapting the educational system to the digital generation, considering the specific conditions of each of the partner countries;
- the requirement of the EU to give the opportunity for EVERYBODY to learn at ANY time and at ANY place with the help of ANY lecturer, using ANY device - computer, laptop, tablet, phablet, smart phone, etc. the consortium will create Centres for innovative education technologies.

MAIN PROJECT OUTCOMES AND PRODUCTS:

- Sustainable academic network for sharing experience and exchange of good practices in the field of innovative educational technologies and didactic models;
- 5 Concepts of adapting the education system to the digital generation - 1 per Partner country (PC);
- 15 Centres for innovative educational technologies - 1 at each PC university;
- 45 active learning classrooms - 3 at each PC university;
- Virtual classrooms - one at each PC university;
- Handbook of implementing innovative educational technologies in PC institutions;
- Courses for trainers for the acquisition of digital skills and learning methods;
- Courses for lecturers for the acquisition of digital skills and learning methods;
- 75 e-Learning courses - 5 at each PC university;
- 75 PowerPoint presentations of lectures, suitable for delivering using interactive electronic white board - 5 at each PC university;
- Cloud-based Virtual Library of the digital educational resources.

IMPACT:

- The project products will be of benefit for all stakeholders in education:
  - National and university policy-makers in the field of education; ”
  - University academics who are trainers / lecturers / learners;
  - Scientific, economic and social partners.
- The project will help to turn partner universities into innovative universities and to improve the quality of the trained specialists, who are necessary to perform the Digital Transformation of Industries (Industry 4.0).

Results

The main aim of the project is to adapt the education system in the PCs to the digital generation through introduction and effective use of ICT-based Innovative Educational Technologies and Didactic Models (IET&DMs) in the teaching process. After the first two project months, the project is collecting feedback for the first project deliverables. A Quality plan is in the making as well as a report on the teaching methods and techniques that exist in Europe. The information is collected by a questionnaire that has been distributed to the European projects partners.

B.2 EC - H2020 Projects

5G HarmoniseD Research and TrIals for serVice Evolution between EU and China

http://5g-drive.eu

Acronym:	5G-DRIVE
Reference:	R-AGR-3451-10
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	5,999,130.00 €
Duration:	1 Sep 2018 – 28 Feb 2021
Members:	• Thomas ENGEL (Principal Investigator) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Latif LADID (Program Coordinator) • Ridha SOUA (Post-Doc)
Area:	Communicative Systems
Partners:	• BMW AG • Dynniq Finland Oy • ERTICO - ITS • EURESCOM • Hellenic Telecommunications Organization S.A. • Joint Research Centre (JRC) • Mandat International • Martel Consulting • Orange Polska Spolka Akcyjna • ORION INNOVATIONS PRIVATE COMPANY • SMARTNET ANONYMI TOURISTIKI KAI KATASKEVASTIKI ETAIREIA PAROCHIS YPIRESION • Spi • University of Kent • University of Surrey • Vediafi Oy

- VTT, Finland

Description

5G-DRIVE will trial and validate the interoperability between EU & China 5G networks operating at 3.5 GHz bands for enhanced Mobile Broadband (eMBB) and 3.5 & 5.9 GHz bands for V2X scenarios. The key objectives are to boost 5G harmonisation & R&I cooperation between EU & China through strong connected trials & research activities, with a committed mutual support from the China "5G Product R&D Large-scale Trial" project led by China Mobile. To achieve these objectives and to deliver the impact for early 5G adoption, 5G-DRIVE structures its main activities into three pillars. The first one will test and demonstrate the latest 5G key technologies in eMBB and V2X scenarios in pre-commercial 5G networks. 5G-DRIVE will run three extensive trials in Finland, Italy and UK. The Chinese project will run large-scale trials in five cities. These twinned trials aim to evaluate synergies and interoperability issues and provide recommendations for technology and spectrum harmonisation. The second one focuses on researching key innovations in network slicing, network virtualisation, 5G transport network, edge computing and New Radio features to fill gaps between standards and real-world deployment. The third one will push EU-China 5G collaboration at all levels thru extensive dissemination and exploitation actions. The project formed a strong team of mobile operators and industry, including a prominent car manufacturer, SMEs, research institutes and universities. This well-balanced consortium has the necessary skills with an established close cooperation with the Chinese consortium will provide first class expertise to achieve full interoperability of the 5G networks and V2X between the EU and China. 5G-DRIVE is ideally set to instill tremendous impact on the validation of standards and trigger the roll-out of real 5G networks and V2X innovative solutions driving new business opportunities and creating thereby new jobs and brand new business models.

Results

The Horizon 2020 project 5G-DRIVE - "5G Harmonised Research and Trials for service Evolution between EU and China" - started in September 2018 and will end in February 2021. It is coordinated by Eurescom (Germany) and includes 16 further European partners from industry and academia: BMW Group (Germany), Dynniq (Finland), ERTICO (Belgium), European Commission's Joint Research Centre (JRC) (Belgium), Martel Innovate (Switzerland), Mandat International (Switzerland), Orange (Poland), Orion Innovations P.C. (Greece), OTE (Greece), SMNET (Greece), SPI (Portugal), University of Kent (UK), University of Luxembourg (Luxembourg), University of Surrey (UK), Vediafi Oy (Finland), and VTT (Finland). The Chinese "5G Large-scale Trial" project is coordinated by China Mobile (Budget 80 M$) and runs from June 2018 to June 2020. Further consortium partners include Huawei, Datang, Ericsson China, Traffic Management Science Research Institute MoPS, Research Institute of Highway MoT, Shanghai International Automobile City, and Beijing University of Posts and Telecommunications.

SECAN-Lab, under the leadership of Prof. Thomas Engel, is responsible for the evaluation and verification of the vulnerabilities of the vehicular communications in the context of automated driving. In order to secure the connected mobility, the SECAN-Lab will conduct also research on the 5G security especially based on the Blockchain technology.

The SECAN-Lab will be also working on the standardisation of 5G and IoT in order to facilitate larger scale of adoption of these new technologies. It will also lead the efforts in terms of recommendations for the cooperation between the EU and China.

5G-MOBIX

Acronym:	5G-MOBIX
Reference:	R-AGR-3457-10
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	21,410,205.65 €
Duration:	1 Nov 2018 – 31 Oct 2021
Members:	• Thomas ENGEL (Principal Investigator) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Latif LADID (Program Coordinator) • Ridha SOUA (Post-Doc) • Ion TURCANU (Post-Doc)
Area:	Communicative Systems
Partners:	• Aalto Korkeakoulusaatio S.R. • AEVAC - Asociación Española del Vehículo Autónomo Conectado • AKKA Informatique et Systemes • Alsa Grupo, S.L.U. • ASELSAN Elektronik Sanayi ve Ticaret A.S. • Associação CCG/ZGDV – Centro de Computação Gráfica • Auto-Estradas Norte Litoral • Ayuntamiento de Vigo • Brisa Inovacao e Tecnologia, S.A. • COSMOTE KINITES TILEPIKOINONIES A.E. • CTAG - Centro Tecnológico de Automoción de Galicia • DAIMLER AG • Dalian Roiland Technology Co.,Ltd • Dalian University of Technology • Datang Telecom Technology • DEKRA Testing and Certification, S.A.U.

- Eindhoven University of Technology
- Electronics and Telecommunications Research Institute (ETRI)
- Ericsson Arastirma Gelistirme ve Bilisim Hizmetleri A.S.
- Ericsson Hellas
- ERTICO - ITS
- FONDATION PARTENARIAL MOV'EOTEC (VeDecoM)
- Ford Otomotiv Sanayi A.S.
- Fraunhofer Gesellschaft
- Gemeente Helmond
- GT-ARC gemeinnützige GmbH
- HERE Global B.V.
- Infraestruturas de Portugal S.A.
- Institute of Automation Shandong Academy of Science
- Institute of Communications and Computer Systems (ICCS)
- Instituto da Mobilidade e dos Transportes, I.P. (IMT)
- Instituto de Telecomunicações
- Intelligent and Connected Vehicles Group, China National Heavy Duty Truck
- Intrasoft International S.A.
- ISEL
- JEFATURA CENTRAL DE TRAFICO
- Korea Automotive Technology Institute (KATECH)
- KPN
- Luxembourg Institute of Science & technology (LIST)
- National Electric Vehicle Sweden (NEVS)
- NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK (TNO)
- NOKIA SIEMENS NETWORKS PORTUGAL S.A.
- NOKIA SPAIN S.A.
- Satellite Applications Catapult Limited
- Sensible 4
- Siemens S.A.
- SNETICT
- TASS International
- Technical University of Berlin
- Telefonica
- TIS
- TURKCELL Teknoloji ARGE A.S.
- Universidad de Murcia
- Valeo Schalter und Sensoren GmbH
- VICOMTECH
- VTT, Finland
- WINGS ICT

Description

5G-MOBIX aims at executing CCAM trials along x-border and urban corridors using 5G core technological innovations to qualify the 5G infrastructure and evaluate its benefits in the CCAM context as well as defining deployment scenarios and identifying and responding to standardisation and spectrum gaps. 5G-MOBIX will first define the critical scenarios needing advanced connectivity provided by 5G, and the required features to enable those advanced CCAM use cases. The matching between the advanced CCAM use cases and the expected benefit of 5G will be tested during trials on 5G corridors in different EU countries as well as China and Korea. Those trials will allow running evaluation and impact assessments and defining also business impacts and cost/benefit analysis. As a result of these evaluations and also internation consultations with the public and industry stakeholders, 5GMOBIX will propose views for new business opportunity for the 5G enabled CCAM and recommendations and options for the deployment. Also the 5G-MOBIX finding in term of technical requirements and operational conditions will allow to actively contribute to the standardisation and spectrum allocation activities. 5G-MOBIX will evaluate several CCAM use cases, advanced thanks to 5G next generation of Mobile Networks. Among the possible scenarios to be evaluated with the 5G technologies, 5G-MOBIX has raised the potential benefit of 5G with low reliable latency communication, enhanced mobile broadband, massive machine type communication and network slicing. Several automated mobility use cases are potential candidates to benefit and even more be enabled by the advanced features and performance of the 5G technologies, as for instance, but limited to: cooperative overtake, highway lane merging, truck platooning, valet parking, urban environment driving, road user detection, vehicle remote control, see through, HD map update, media & entertainment.

Results

SECAN-Lab, under the leadership of Pro. Thomas Engel, is responsible for promoting the research carried out in 5G-MOBIX and foster the cooperation agreements with the international 5G community and similar projects in USA, China, Japan, Korea and comparative analysis of government policies in these selected countries. Moreover, SECAN-Lab is involved in the standardisation activities, by providing recommendations in the 3GPP meetings, as well as contributing to the spectrum allocation discussions about the required frequency bands for the Cooperative And Connected Automated Mobility (CCAM) services. SECAN-Lab is also involved in the assessment of the potential business and societal impact of the project results and of the applications demonstrated in the cross-border corridors and trial sites. Finally, SECAN-Lab is involved in the dissemination activities of the 5G-MOBIX results in order to increase the project reach and impact in EU, China, Korea, and beyond.

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

Acronym:	ATENA
Reference:	R-AGR-3026

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

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) • Aurel MACHALEK (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Latif LADID (Program Coordinator) • Andriy PANCHENKO (Scientific Contact) • Florian ADAMSKY (Post-Doc) • Mohamed Nizar MSADEK (Post-Doc) • Stefan SCHIFFNER (Post-Doc) • Ridha SOUA (Post-Doc)
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

SCADA systems are used to monitor critical infrastructures behaviour and to send commands remotely. However, with the massive spread of connectivity, using open protocols and more connectivity opens new network attacks against critical infrastructures. To cope with this dilemma, sophisticated security measures are needed to address malicious intrusions, which are steadily increasing in number and variety.

ATENA aims at developing SDN-based Intrusion detection architecture. In 2018, to this end SECAN-Lab provided a taxonomy of security agents with a specific focus on statistical, deep packet and honeypots agents. To highlight the novelty, we outline both academic work related to Agents/Probes and available IDS software. Moreover, we provide a detailed description of network signature, statistical, SDN–assisted, distributed statistical SDN agent, multi-antivirus, rule-based agents and honeypots. We show how to integrate these into the ATENA Agent/Probe management API. Moreover, machine learning techniques for anomaly detection were assessed using a real data set collected from a gas pipeline system. We used SVM, RF, and BLSTM to implement diverse IDS classifiers. We provided a complete comparison between these algorithms along with the random hyper-parameter search results. We published our source code on GitHub to help other researchers to verify, compare, and/or extend their studies. Further, our research efforts for ATENA resulted in 2018 in the following publications:

- ”Integrated Protection of Industrial Control Systems from Cyber-attacks: the ATENA Approach”, Adamsky, Florian; Aubigny, Matthieu; Battisti, Federica; Carli, Marco; Cimorelli, F.; Cruz, Tiago; Di Giorgio, A.; Foglietta, C.; Galli, A.; Giuseppi, A.; Liberati, F.; Neri, A.; Panzieri, S.; Pascucci, F.; Proenca, J.; Pucci, P.; Rosa, L.; Soua, Ridha, in Elsevier International Journal of Critical

Infrastructure Protection (2018)

- ”Machine Learning for Reliable Network Attack Detection in SCADA Systems”; Lopez Perez, Rocio; Adamsky, Florian; Soua, Ridha; Engel, Thomas; in 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (IEEE TrustCom-18) (2018)

Last but not least, the SECAN-Lab hosted the 2018 Atena workshop at its premises in the frame of the European cyber security month 2018.

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) • Stefanie OESTLUND (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Latif LADID (Scientific Contact) • Detlef FUEHRER (Research Associate)
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

The SECAN-Lab team has analysed and synthesised the 5G and IoT standardisation efforts in China and the EU in terms of Standardisations bodies recommendations, spectrum allocations, 5G and IoT protocols, regulations and made recommendations for harmonisation and alignment in the benefit of scaling 5G and IoT deployment to the ultimate benefit of end-users. A white paper has been prepared which summarises the 5G and IoT recommendations aligning and harmonising China and the EU and the issues still open for resolutions

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) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Latif LADID (Collaborator) • Andriy PANCHENKO (Scientific Contact) • Marharyta ALEKSANDROVA (Post-Doc)

- Mohamed Nizar MSADEK (Post-Doc)
- Stefan SCHIFFNER (Post-Doc)

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 makers 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

Most citizens have little experience in assessing privacy risks of online services. It is considered as burden by providers and users alike. Privacy Flag developed tools for end-users and business owners to ease this burden. These tools are connected to a shared knowledge database, that combines expert knowledge and user experiences. PrivacyFlag also created a voluntary mechanism for organisations outside the EU to conform to European Data Protection Law. In the scope of this project, SECAN-Lab provided expert knowledge on frequent cyber security threats and developed several tools that can be used by end-users to protect their privacy online.

PrivacyFlag was awarded as a distinguished success story by the European Commission in June 2018 (https://ec.europa.eu/digital-single-market/en/news/privacy-flag-eu-funded-project-success-story). The project ended this summer but lives on with its voluntary certification mechanism which is still maintained by the project partners.

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) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Latif LADID (Program Coordinator) • Mohamed Nizar MSADEK (Post-Doc)

- Ion TURCANU (Post-Doc)

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 2018, SECAN-Lab continued its active contribution to the F-Interop project. In particular, we released the final version of the Privacy Test Tool, one of the testing tools available in the F-Interop platform. To this end, we designed a general framework that detects privacy issues by analysing both *encrypted* and *non-encrypted* data traffic of IoT protocols. The framework is composed of two main modules: the Encrypted Traffic Analysis (ETA) module and the Non-encrypted Traffic Analysis (NTA) module. ETA is able to investigate how an adversary can get sensitive information related to IoT device activities by passively observing patterns of encrypted communication. NTA follows a pattern matching approach in the data payload of IoT protocols in order to detect what is considered personal and/or private. In addition, we presented an analysis of the technology state in SDN and provided insights into how SDN technologies can be applied to the F-Interop platform when ready in the future.

F-Interop project was officially completed on October 31st 2018, and successfully passed the final review on December 19th 2018.

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) • Aurel MACHALEK (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Detlef FUEHRER (Research Associate) • David NAVEH (Research Associate)
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

Project has delivered exceptional results with significant immediate or potential impact.

The project objective was to provide an innovative, end to end, integrated and risk based approach to security at European Airports. The project has achieved this through a number of components and has successfully demonstrated that the technology is available (with some refinements needed before it could be used in a live airport environment).

The key issue is now a regulatory, political and societal decision as to how far aviation security wants to proceed with a risk based approach. A risk based approach can only be implemented if provided for within EU Regulation 300/2008 and 2015/1998. It may be appropriate to propose to the Commission that the regulations be amended to allow an airport to use a risk based approach such as that demonstrated by FlySec or to use the standards set out currently.

Floating Car Data Collection for Intelligent Transportation Systems

Acronym:	FCD4ITS
Reference:	R-AGR-3409-10
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	100,000.00 €
Duration:	1 Mar 2018 – 31 Dec 2018
Members:	• Thomas ENGEL (Principal Investigator) • Aurel MACHALEK (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Florian ADAMSKY (Post-Doc) • Ion TURCANU (Post-Doc)
Area:	Communicative Systems

Description

The FCD4ITS project will deploy and execute a set of experiments using the RAWFIE vehicular testbeds to evaluate the performance of our own (and other state-of-the-art) Floating Car Data collection algorithms, in order to understand their properties in real-world settings. We will deploy automated large-scale real-world procedures using Unmanned Ground Vehicles (UGVs) provided by the RAWFIE testbeds to evaluate the performance and applicability of our novel algorithms and compare them to the state of the art. RAWFIE testbeds will allow validation of the solutions in real-world settings, building on our existing simulation-based evaluations. We will also give feedback to RAWFIE on facilitating the automated execution of such experiments. Our work will help the research community to understand the limitations of simulations in targeted scenarios and adapt them to better reflect the real world. Our solid experience in fundamental and applied vehicular research will allow us to successfully complete these tasks.

Results

The FCD4ITS project aims at deploying and executing a set of experiments using the RAWFIE vehicular testbeds to evaluate the performance of several Floating Car Data collection algorithms, in order to understand their properties in real-world settings. In 2018, we started our work on this project by providing a thorough analysis of the networking and mobility capabilities of the RAWFIE vehicular testbeds. In particular, we provided a brief description of the main

Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication technology, namely Dedicated Short-Range Communication (DSRC), and the protocol stack proposed by the European Telecommunications Standards Institute (ETSI), named ETSI ITS-G5. Then, we described one of the open-source projects implementing this standard, OpenC2X, and its main software and hardware requirements. In addition, we presented the modifications made to the software in order to integrate it with Alix single-board computers. Finally, we created a simple V2X testbed based on OpenC2X and Alix devices, and started the implementation of the FCD collection algorithms.

Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module

Acronym:	FutureTPM
PI:	Peter Y A RYAN
Funding:	European Commission - Horizon 2020
Duration:	1 Jan 2018 – 31 Dec 2020
Member:	Peter Y A RYAN (Principal Investigator)

Description

The goal of FutureTPM is to design a Quantum-Resistant (QR) Trusted Platform Module (TPM) by designing and developing QR algorithms suitable for inclusion in a TPM. The algorithm design will be accompanied with implementation and performance evaluation, as well as formal security analysis in the full range of TPM environments: i.e. hardware, software and virtualization environments. Use cases in online banking, activity tracking and device management will provide environments and applications to validate the FutureTPM framework.

Results

FutureTPM is a Horizon 2020 project whose goal is the design and implementation of trusted platform modules (TPM) that are secure against adversaries equipped with a large quantum computer. The project, which involves 15 partners, started on 01/01/2018 and it will last three years. In 2018, work package 1, whose objective is to gather security and functionality requirements and to create a reference architecture for TPMs, has been completed. In work package 2, the project has reviewed existing quantum-resistant cryptographic primitives and protocols of interest for TPMs and has started research on new quantum-resistant primitives and protocols. In work package 3, the project has analyzed existing security frameworks and has started to define security for a quantum-resistant TPM. In work package 4, work on run-time risk assessment for TPMs has also started.

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) • Giovanni CASINI (Researcher) • 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.

Results

The project is an H2020 project involving 16 international partners and structured into four work packages (WP1-WP4). In 2018, the work done in WP1 focused on investigating temporal properties of policies and the deontic dimension of norms and interpretation. WP2 was devoted to connect legal text to concepts and instances in legal ontologies. The work in WP3 was focused on extending description and defeasible logics for reasoning with ontology-based access to normative information, argumentation systems for legal representation and reasoning in order to improve transparency of the reasoning. Finally, WP4 focused on mining and reasoning on technical documents, and the first global evaluation, which focuses on the significant advancements made in machine learning and deep learning techniques for use on legal texts.

In addition, Dr. Casini has worked in particular with Prof. Thomas Meyer in extending Description Logics with forms of defeasible reasoning, in particular with Deontic Modalities, in order to define a formalism that is appropriate for the development of Ontologies containing normative information, and of the correlated reasoners, aimed at executing relevant reasoning tasks as regulatory compliance.

Related publications:

- Casini G., Straccia U., Meyer T. (in press), ‘A polynomial Time Subsumption Algorithm for Nominal Safe ELO_\bot under Rational Closure’, Information Sciences, in press.
- Casini G., Meyer T., Varzinczack I. (2018) ‘Defeasible Entailment: from Rational Closure to Lexicographic Closure and Beyond’ in Proceedings of the 17th edition of the International Workshop on Non-Monotonic Reasoning (NMR-18), pp. 109-118.
- Casini G., Fermé E., Meyer T., Varzinczack I. (2018) ‘A Semantic Perspective on Belief Change in a Preferential Non-monotonic Framework’ in Proceedings of the 16th International Conference on Knowledge Representation and Reasoning (KR-18), AAAI Press, pp. 220-229.

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) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Latif LADID (Collaborator) • Andriy PANCHENKO (Scientific Contact) • Marharyta ALEKSANDROVA (Post-Doc) • Stefan SCHIFFNER (Post-Doc)
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

SAINT analyses the ecosystems of cybercriminal activity, associated markets and revenues to develop a framework of business models appropriate for fighting with cybercrime. In 2018, SECAN-Lab contributed to this by analysing the impact of encrypted network traffic on privacy. We developed a tool to assess website fingerprintability and analysed the state of the art of privacy technologies in relation with the GDPR. The latter contribution was presented at the annual privacy forum [1]. We also contributed to formalisation of privacy models. These results were accepted as a publication at PETs in 2019 [2].

[1] "Towards a Roadmap for Privacy Technologies and the General Data Protection Regulation : A transatlantic initiative" Schiffner, Stefan et. al in proceedings of the Annual Privacy Forum 2018 (2018)

[2] "On Privacy Notions in Anonymous Communication" Christiane Kuhn*, Martin Beck, Stefan Schiffner, Eduard Jorswieck, and Thorsten Strufe to appear in proceedings on privacy enhancing technologies 2019 (2019)

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)
- Anne OCHSENBEIN (Project Coordinator)
- Stefanie OESTLUND (Project Coordinator)
- Mathieu VIAU-COURVILLE (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

TARGET delivered 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)

Within the TARGET project there have been developed 6 separate and specific training exercises to prepare emergency commanders for 'real' incidents in a challenging, immersive and safe environment and widely present possibilities of virtual / augmented reality together with TARGET platform for training purposes.

Level of usability is different and depends on each Training Content. Some have been identified as almost ready to use. In every case, trainings are not on level of final product and there are requirements for improvements still.

Using of AR / VR have been assessed as possibly effective. In case, that technical identified points can be solved, these training can save financial sources and simplified way of preparation of Security Critical Agents staff with aim of increasing general level of security preparedness. In every case, innovation potential have been identified and confirmed by end-users.

B.3 EU - COST Action 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

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.4 ESA 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) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Domenico GIOTTI (Research assistant) • Ridha SOUA (Post-Doc)
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

Satellites are playing a key role in driving the vision for a truly connected world, providing ubiquitous coverage and reliability in places where no other terrestrial technology could. While the potentials of satellites for Internet of Things (IoT) are well recognised, to allow a smooth integration of Machine-to-Machine (M2M) and satellite networks, a lot of tweaking and optimising is still required. In this vein, the work in 2018 was focused on the optimizations of the two IoT applications protocols Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), identified as IoT Application Protocols suitable for IoT data collection over satellite. The network architecture, highly scalable, includes two MQTT brokers (with bridge functionality) and two CoAP proxies, in Observe mode, respectively. We finally designed optimisation of the two selected protocols aiming to reduce the amount of traffic load over the satellite return channel, to avoid bandwidth waste with transmission of obsolete data, and to support Quality of Service (QoS) for traffic delivery. These optimizations deal with IoT Traffic Aggregation, message delivery priority and obsolete message cancellation. The latter aim to reduce the amount of traffic on the satellite return channel, and delivery of critical data in due time. The evaluation of the achievable performances is ongoing. To this aim, a testbed is set up, using the OpenSAND emulator, MQTT Mosquitto, and CoAPthon.

B.5 FNR Projects

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 offered 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

- A. Pilgun, O. Gadyatskaya, S. Dashevskyi, Y. Zhauniarovich and A. Kushniarou. *An Effective Android Code Coverage Tool.* In Proceedings of ACM CCS Poster session, pp. 2189–2191, 2018.
- S. Dashevskyi, O. Gadyatskaya, A. Pilgun and Y. Zhauniarovich. *The Influence of Code Coverage Metrics on Automated Testing Efficiency in Android.* In Proceedings of ACM CCS Poster session, pp. 2216–2218, 2018.

B.6 FNR and UL Projects

Approaching Indigenous Australian History With Text Mining Methods

https://acc.uni.lu/index.php?page=projects

Acronym:	AIAHTMM
PI:	Christoph SCHOMMER
Funding:	Fonds National de la Recherche, University of Luxembourg
Duration:	1 Jan 2017 – 31 Dec 2030
Members:	• Christoph SCHOMMER (Principal Investigator) • Ekaterina KAMLOVSKAYA (Doctoral Candidate)
Area:	Intelligent and Adaptive Systems

Description

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 Partner: C2DH.

- See more at: https://acc.uni.lu/index.php?page=projects

Results

The collection of data is completed and the experiments started.

B.7 FNR - AFR Projects

Tailoring Automated Software Techniques for Real World and Large Scale Software Applications

Acronym:	TASTRA
PI:	Yves LE TRAON
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche
Duration:	15 Jan 2016 – 14 Jan 2020
Member:	Yves LE TRAON (Principal Investigator)

Description

In recent years, there has been much research in the area of automated software testing, leading to the development of interesting testing techniques such as symbolic execution and mutation testing. These techniques are shown in academic research to be quite effective for finding defects in programs. Despite the undisputed potential of those techniques, the problems of their application cost, scalability, operation of software with environment interaction are obstacles to its practical use in real-world programs and environments. The main problems that require attention and hopefully will be resolved by the present project are the design of effective mutations and symbolic execution that will allow the techniques to scale and deal with environmental defects such as configuration errors, network protocols, file systems and concurrency. The present project will 1) Evaluate the level of test confidence or guarantee that should be provided by mutation testing, 2) Design a technique to effectively detect useful mutants, 3) leverage symbolic execution on program environment.

B.8 FNR - AFR PhD Projects

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 – 31 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 [10993/33616]: 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 pay-

load configuration [↗10993/30386]: 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 [↗10993/32009]: 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.

Clustering approaches for visual knowledge exploration in molecular interaction networks [60]: Biomedical knowledge grows in complexity, and becomes encoded in network-based repositories, which include focused, expert-drawn diagrams, networks of evidence-based associations and established ontologies. Combining these structured information sources is an important computational challenge, as large graphs are difficult to analyze visually. We investigate knowledge discovery in manually curated and annotated molecular interaction diagrams.To evaluate similarity of content we use: i) Euclidean distance in expert-drawn diagrams, ii) shortest path distance using the underlying network and iii) ontology-based distance. We employ clustering with these metrics used separately and in pairwise combinations. We propose a novel bi-level optimization approach together with an evolutionary algorithm for informative combination of distance metrics. We compare the enrichment of the obtained clusters between the solutions and with expert knowledge. We calculate the number of Gene and Disease Ontology terms discovered by different solutions as a measure of cluster quality. Our results show that combining distance metrics can improve clustering accuracy, based on the comparison with expert-provided clusters. Also, the performance of specific combinations of distance functions depends on the clustering depth (number of clusters). By employing bi-level optimization approach we evaluated relative importance of distance functions and we found that indeed the order by which they are combined affects clustering performance. Next, with the enrichment analysis of clustering results we found that both hierarchical and bi-level clustering schemes discovered more Gene and Disease Ontology terms than expert-provided clusters for the same knowledge repository. Moreover, bi-level clustering found more enriched terms than the best hierarchical clustering solution for three distinct distance metric combinations in three different instances of disease maps. Int his work, we examined the impact of different distance functions on clustering of a visual biomedical knowledge repository. We found that combining distance functions may be beneficial for clustering, and improve exploration of such repositories. We proposed bi-level optimization to evaluate the importance of order by which the distance functions are combined. Both combination and order of these functions affected clustering quality and knowledge recognition in the considered benchmarks. We propose that multiple dimensions can be utilized simultaneously for visual knowledge exploration.

A competitive approach for bi-level co-evolution: Real-life problems often involve several decision makers whose decisions impact each other. When two decision makers decides sequentially, these problems are referred to as bi-level optimization problems. Generally modeled as nested optimization problems, they are NP-hard even for two linear and continuous levels. Such problems often occur in situations were only a part of the decision variables is controlled by each decision makers. Their final objective value is thus subject to each other's decision. From the first decision maker point of view, it is necessary to predict the rational reaction of the second decision maker which may have a conflicting objective function. The first decision maker should therefore ensure that this reaction will not have a disastrous effect on its own final objective value. The inherent complexity of bi-level optimization problems led researchers to consider metaheuristics. Among the most promising metaheuristics, co-evolutionary algorithms proved their abilities to tackle large scale problems. Unfortunately, BOPs are naturally strongly epistatic. In this work, we propose an hybrid competitive co-evolutionary algorithm (CARBON) to tackle this pitfall. We compare CARBON against another co-evolutionary approach for bi-level optimization problems, i.e., COBRA. Experimental results demonstrate the abilities of CARBON to break the inherent nested structure that makes bi-level optimization problems so difficult.

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.

Results

In 2018, the Ph.D. candidate (Aleksei Udovanko) focused on white-box cryptography and wrote together with Alex Biryukov a paper describing their follow-up work after the WhibOx 2017 competition, where they reached the first place in the design category. The paper, which was accepted at ASIACRYPT 2018, contains new attacks and provably secure countermeasures for white-box implementations. The Ph.D. candidate also worked (together with Christof Beierle and Alex Biryukov) on the theoretic foundations of nonlinear invariant attacks, a recent method for the cryptanalysis of block ciphers. A paper resulting from this work is currently under submission. Finally, the Ph.D. candidate contributed to the design and analysis of a new lightweight authenticated cipher and hash function, which will be submitted to the NIST in response to their call for lightweight primitives.

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.

B.9 FNR - AFR PhD and ILNAS Projects

ILNAS - UL/SnT Research Programme on Digital Trust in Smart ICT

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 R. BRUST (Post-Doc) • Saharnaz ESMAEILZADEH DILMAGHANI (PhD student) • 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.

Results

Publications:

- White Paper: Data Protection and Privacy in Smart ICT - Scientific Research and Technical Standardization, 2018 [260]
- On Standardised UAV Localisation and Tracking Systems in Smart Cities - N. Labib, M.R. Brust, G. Danoy, P. Bouvry, To appear in book of abstracts of the 17th Annual STS Conference (Graz), 2018 [304]
- A Standardized Broker Model in Smart Cities, C. Liu, S. Varrette, G. Danoy, M.R. Brust, P. Bouvry, To appear in book of abstracts of the 17th Annual STS Conference (Graz), 2018 [287]
- Maya Olszewski, Jeff Meder, Emmanuel Kieffer, Raphaël Bleuse, Martin Rosalie, Grégoire Danoy, and Pascal Bouvry. Template of a Chaotic Attractor . Graph Drawing. 2018 [195]
- J. Mesit, M.R. Brust, P. Bouvry. Lightweight Key Agreement for Wireless Sensor Networks, IEEE QRS, 2018
- Raphaël Bleuse, Giorgio Lucarelli, and Denis Trystram. Data Movements by Anticipation: Position Paper . Euro-Par Workshops 2018 [↗10993/37830]
- A.M. Fiscarelli, M.R. Brust, G. Danoy, P. Bouvry, *A Memory-based Label Propagation Algorithm for Community Detection*, Int. C. on Complex Networks and Their Applications (COMPLEX NETWORKS), 2018 [121]
- C. Liu, P. Bouvry. Optimal Pricing for Socially-aware Usage of Cloud Services. International Conference on Optimization and Learning, OLA 2019 (to appear)
- Transforming Collaboration Data into Network Layers for Enhanced Analytics , S. Dilmaghani, A. Piyatumrong, P. Bouvry, M.R. Brust, International Conference on Optimization and Learning OLA 2019 (to appear)
- M. Rezazad, M.R. Brust, M. Akbari, P. Bouvry, N-M. Cheung*, Detecting Target-Area Link-Flooding DDoS Attacks using Traffic Analysis and Supervised Learning,* Future of Information and Communication Conference (FICC), 2018
- J. Chen, S. Hossain, M.R. Brust, N. Johnson, *A Game Theoretic Analysis of the Twitter Follow-Unfollow Mechanism,* Int. C. on Decision and Game Theory for Security (GameSec), 2018 [103]

Talks:

- On 06.07.2018, Prof. Bouvry presented the SnT-ILNAS research and educational programme at the ETSI Workshop at the Technoport in Belval.
- On 09.07.2018, Dr. Brust delivered a talk entitled Toward an innovative and trustworthy ICT Ecosystem for the Smart City at the Int. Workshop on Urban Data Science (UDS 2018) (http://urban.se.rit.edu/2018/index.html) in

Bangkok (Thailand).

B.10 FNR - CORE Projects

A Distributed Graph Database for Large-Scale Text Analytics

Acronym:	BigText
PI:	Martin THEOBALD
Funding:	Fonds National de la Recherche - CORE
Budget:	230,000.00 €
Duration:	1 Jan 2018 – 31 Dec 2020
Member:	Martin THEOBALD (Principal Investigator)
Area:	Computational Sciences
Partner:	Max Planck Institute for informatics

Description

The World Wide Web (in the following referred to as just "the Web") is the most comprehensive – but likely also the most complex – source of information that we have access to today. More than 95 percent of all information in the so-called surface Web, i.e., the part of the Web that is publically accessible either as static pages or in the form of dynamically created contents, is in fact estimated to consist of text. This textual data just happens to sometimes be interspersed with semi-structured components such as form fields, lists, and tables – or so-called "infoboxes" in Wikipedia. These infoboxes, plus perhaps some more metadata, however still constitute the main source of information for all of the currently available, Web-extracted knowledge bases such as DBpedia, YAGO, Freebase, and Wikidata. This means we in fact only exploit a tiny fraction of the information that is published on the Web for Information Extraction (IE) purposes. By exploiting the syntactic and semantics dependencies of information conveyed in Web documents, BigText aims to build a large-scale, distributed graph database of highly interlinked and semantically enriched documents that serves as a basis for high-accuracy retrieval of information, mining of syntactic and semantic relationships among real-world entities, and – more broadly – a whole line of online analytical tasks that serve as a basis for further text and knowledge mining. In other words, we intended to investigate a radically new approach to information access and retrieval that bridges the three key areas of Information Extraction, Information Retrieval and Big Data Analytics.

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) • Jose 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.

Results

Research under the AToMS project in 2018 has focused on three directions: forward secrecy for password authenticated key exchange protocols, alternative methods for achieving unconditional, composable message authentication, and determining the resource requirements for authentication in the context of quantum key distribution. In the first direction, Jose Becerra, Dimiter Ostrev and Marian Skrobot proved that the SPAKE2 protocol provides weak forward secrecy, proposed a modification of the protocol and proved that the modified protocol provides perfect forward secrecy. In the second direction, Dimiter Ostrev showed that an advantage in channel noise is sufficient to achieve composable, unconditionally secure message authentication, without needing any secret key. The third direction is still ongoing work; Dimiter Ostrev has determined what is known about resource requirements of stand-alone message authentication and what proof techniques are used, and is currently working to adapt these to the context of quantum key distribution.

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 program 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.

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) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Antonio DI MAIO (Doctoral Candidate) • Ridha SOUA (Post-Doc) • Ion TURCANU (Post-Doc)
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 2018 focused on two aspects:

The first aspect tackles the routing protocols in Software defined networking (SDN)-enabled vehicular networks. Vehicular networks have unique peculiarities such as high mobility, intermittent connectivity, etc. which make the routing problem a very challenging task. In this vein, Antonio Di Maio, a PhD student working on CONTACT project, conducted an in deep study of classical mobile ad-hoc network routing protocols (AODV, dymo DSDV, GPSR) available in literature and evaluated their performance in terms of packet delivery ratio (PDR), throughput, and overhead in a simulated environment using sumo and veins, determining their unsuitability for dynamic networks. Antonio currently focuses on new SDN-based algorithms to improve QoS in unicast flows over vehicular networks, taking into consideration delay and congestion of the network, as well as the lifetime of the wireless links.

The second aspect tackles the adoption of Multi-access Edge Computing (MEC) in future vehicular networks. Indeed, with the emergence of self-driving technology and the ever-increasing demand of bandwidth-hungry applications, providing the required latency, security and computational capabilities is becoming a challenging task. In addition, current vehicular architectures are not sufficiently flexible to support the highly heterogeneous landscape of emerging communication technologies, such as mmWave, Cellular Vehicle-to-Everything (C-V2X), and Visible Light Communication (VLC). To this aim, Multi-access Edge Computing (MEC) has been recently proposed to enhance the quality of passengers experience in delay-sensitive applications. Dr. Ridha Soua and Dr. Ion Turcanu have investigated the in-premises features of MEC and the need of supporting technologies, such as Software Defined Networking (SDN) and Network Function Virtualization (NFV), to fulfil the requirements in terms of responsiveness, reliability and resiliency. The latter is of paramount importance for automated services, which are supposed to be always-on and always-available. We have described possible solutions for mobility-aware computation offloading, dynamic spectrum sharing, and interference mitigation.

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.

Results

The project is about building a knowledge base of deontic logic formulae expressing the legal interpretation of article of the GDPR. On that base, it is possible to build a semi-automatic reasoning about GDPR compliance . The DAPRECO Knowledge base has been delivered in its first drafted version.

Distance Bounding: a graph theoretical and formal approach

Acronym:	DIST
Reference:	C15/IS/10428112
PI:	Rolando TRUJILLO RASUA
Funding:	Fonds National de la Recherche - CORE
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 • Computer Science & ICT Security • 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 studying 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

- 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, 2018
- The Junior PI Dr. Rolando Trujillo-Rasua has joined Deakin University (Melbourne, Australia) as Lecturer.

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) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (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 2018, 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 and AIMS). 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.

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) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Ion TURCANU (Post-Doc)
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 2018, SECAN-Lab continued its contribution to the MaDSAV project in collaboration with LIST and the University of Salzburg. In particular, we were involved in a study aiming to find out how different levels of task load affect unscheduled takeovers and subsequent driving performance. We also investigated if retaining situation awareness of the driver in phases of autonomous driving helps to mitigate negative effects. MaDSAV project was officially completed on June 30th 2018.

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) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator)
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 2018, 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. We also extended one of our tools LuST-LTE, presented at IEEE ITSC, 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) 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) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Augusto Wladimir DE LA CADENA RAMOS (Doctoral Candidate)

- Marharyta ALEKSANDROVA (Post-Doc)
- Daniel KAISER (Post-Doc)
- Mohamed Nizar MSADEK (Post-Doc)
- Stefan SCHIFFNER (Post-Doc)

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 main objective of the FNR junior core project PETIT is in designing and evaluating privacy-enhancing techniques for future Internet. Within the scope of the project in 2018, the SECAN-Lab team made advances mainly in three areas. These are website fingerprinting, multipath routing, and analysis of existing privacy-preserving protocols with respect to recently proposed enhancements. In the following, be briefly summarize our achievements.

During the reported period, we continued our investigation of real-world cases of website fingerprinting in order to study its feasibility. To this end, we addressed a scenario, where the user navigates through multiple pages of a website. We analyzed how a potential attacker can benefit from information about webpages belonging to the same website by the use of clustering in combination with supervised learning. It helped us to boost the performance of the fingerprinting techniques and, hence, provide a more realistic feedback about the severity of the attack to the end users of privacy-preserving techniques.

We also worked on the analysis of a recently proposed modification of the guard node selection algorithm for the anonymization network Tor. This modification aims at protection of the users from active BGP routing attacks. These are performed for path hijacking and mounting traffic analysis and traffic confirmation attacks. Our preliminary investigations confirm our hypothesis that selecting guard nodes that are more resistant to the BGP route hijacking attacks imply choosing nodes that are closer to the client with respect to the internet distance. Hence, this leaks information about client's location. Our findings show that this approach leaks further user-related information and may impact the broader efficiency and security of the system.

Using multiple paths in communication has several advantages. These are better reliability, performance, and resistance with respect to several attacks. Proceeding our research in the field of multi-path onion routing for anonymization networks (such as Tor), we evaluated both performance and security implications of the designs that can be adapted to provide multipath. We introduced a taxonomy for designing and classifying onion routing-based approaches and evaluated existing implementations taking into account our taxonomy. Through an exhaustive evaluation at different scales, we were able to reveal the impact of the multipath paradigm on key performance indicators and showed open gaps in system designs to better incorporate parallel paths for the benefit of performance and security.

Quantum Communication with Deniability

Acronym:	Q-CoDe
PI:	Peter Y A RYAN
Funding:	Fonds National de la Recherche - CORE
Duration:	1 Jul 2018 – 30 Jun 2021

Members:	• Peter Y A RYAN (Principal Investigator) • Arash ATASHPENDAR (PhD student) • Dimiter OSTREV (Research Associate)

Description

The goal of this project is to conduct a thorough formal analysis of the promising, but poorly understood field of deniable quantum communication. It will entail a systematic analysis and classification of the quantum primitives that are relevant for deniability, and further give precise definitions of deniability and related concepts in quantum protocols. The results will be both in the form of impossibility, as well as feasibility theorems with corresponding protocols. This will be both in the form of modifying existing QKD protocols to restore deniability, as well as devising new quantum protocols that provide deniability for key exchange and beyond, e.g. for e-voting.

Results

Q-CoDe: Quantum Communication with Deniability: Q-CoDe was started in July 2018. Jeroen van Wier was recruited as a PhD candidate for the project and started in December 2018. A first paper for the project was accepted for NordSec 2018 and presented there in December.

Security in the Shell

Acronym:	SSH
PI:	Jan LAGERWALL, Gabriele LENZINI
Funding:	Fonds National de la Recherche - CORE
Duration:	1 Apr 2018 – 31 Mar 2021
Members:	• Gabriele LENZINI (Principal Investigator) • Peter Y A RYAN (Scientific Advisor)

Description

SSh is a highly interdisciplinary and ambitious research project that poses, to both scientific fields that it connects, intellectual and scientific challenges that are as fascinating as they are unprecedented. The acronyms plays with the name “secure shell”, which in this project is not a virtual computing construct but a real physical object: a shell of cholesteric liquid crystal. Such shell, so far a playground for fundamental soft matter physics experiments, holds great potential for providing a potentially game-changing security tool. Arrays of them, the project hypotheses, represent a new kind of optical Physical Unclonable Function of great potentiality in the authentication of physical objects such as artworks, drugs and foods. The role of computer science in this project is to analyze the security features of arrays of CLC shells and to propose protocols for ensuring a secure and reliable authentication process.

Security, Scalability, and Privacy in Blockchain Applications and Smart Contracts

https://www.cryptolux.org/index.php/Projects

Acronym:	FinCrypt
PI:	Alexei BIRYUKOV
Funding:	Fonds National de la Recherche - CORE
Duration:	1 Aug 2018 – 31 Jul 2021
Members:	• Alexei BIRYUKOV (Principal Investigator) • Ritam BHAUMIK (Post-Doc) • Shange FU (PhD student) • Giuseppe VITTO (PhD student)
Area:	Security, Reliability and Trust in Information Technology

Description

Blockchain technology gathered momentum with the popularity of the Bitcoin cryptocurrency. Being an interesting practical proposal which gained a large community of followers in the last 4 years Bitcoin can be seen as a testbed for ideas in the FinTech area. By now it is clear what Bitcoin ideas can be generalized and are valuable but also what are the shortcomings of the concrete Bitcoin instantiation of a distributed ledger and cryptocurrency. For example, the scalability problem has become vital, as the transaction rate growth made the designers think to increase the block size, which in turn might lead to higher network latency and vulnerability to various network attacks. Also current proof-of-work based blockchains are very energy intensive. Active research is now happening around greener alternatives for consensus protocols, such as fault-tolerant Byzantine agreement or Proof of Stake which tolerate higher transaction rate and were tested on small networks.The security of blockchain applications with an accent on the data confidentiality is an unsolved problem. So far the blockchain ledger is implicitly public, but users demand more confidentiality for their data. On the other hand governments demand access to blockchain information for AML/KYC policies and taxation. The problem of storing and processing encrypted data on the blockchain as well as privacy vs governance tradeoff remain largely unexplored.One of the most interesting blockchain applications are smart contracts. Whereas the Bitcoin ledger consists of transactions only, a smart contract ledger contains programming code of almost arbitrary complexity, so that sophisticated financial instruments, legal contracts, and reputation systems can be encoded and executed automatically. However, the private character of contracts poses a challenge of concealing the exact functionality while, at the same time, still keeping it verifiable to the other protocol participants.Our proposal is to investigate blockchain applications from both the scalability and confidentiality point of view and to suggest new solutions in this area (Work Package 1) as well as to study the privacy and security aspects of smart contracts and to propose new efficient methods to achieve user privacy and contract confidentiality (Work Package 2).

Results

The FinCrypt project officially started on 1st July 2018. Besides the PI, two Ph.D. students and a post-doctoral researcher are involved and contribute to the two work-packages of the project. The two Ph.D. students started to work on (i) privacy in distributed ledgers with a focus on zero-knowledge proofs, and (ii) a classification of consensus protocols. The postdoc's research topic is resource-hard functions and their applications, for example proof of space.

B.11 FNR - CORE and NCBR 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.

Results

1. Gergely Bana published a paper (with co-authors at the University of Missouri) at ESORICS'18 on the computationally sound symbolic verification of the FOO protocol. The paper included some new attacks.
2. Gergely Bana, Wojtek Jamroga (Polish National Academy of Sciences) and Peter Ryan are finishing a paper on choosing a winner for Condorcet voting with a technique motivated by PageRank and based on the theory of Markov processes, and argue about the advantages compared to other methods. They are planning to submit the paper to IJCAI'19
3. Gergely Bana and Wojtek Jamroga (Polish National Academy of Sciences) are working on a paper on game-theoretic definition of coercion-resistance of voting protocols.

B.12 FNR - CORE - Core Junior Projects

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.

Stateful Zero-Knowledge

Acronym:	SZK
PI:	Alfredo RIAL DURAN
Funding:	Fonds National de la Recherche - CORE - Core Junior
Duration:	1 Mar 2018 – 28 Feb 2021
Members:	• Alfredo RIAL DURAN (Principal Investigator) • Peter Y A RYAN (Local Scientific Advisor)

Description

A zero-knowledge (ZK) proof system allows a prover to prove statements to a verifier without revealing secret information. The goal of this project is to define, construct and analyse protocols for stateful zero-knowledge (SZK). SZK is defined as the task of keeping state information between prover and verifier in a ZK proof system. We view the state as a data structure where the prover stores each piece of data at a certain position.
Our definitions must ensure the following: (1) data in the state is hidden from the verifier, (2) the prover can read and write data at positions while hiding both the data and the positions, and (3) a piece of data read from the state at a position equals the last piece of data stored at that position.
Our constructions for SZK will allow the prover to prove statements about the positions read or written. We will use SZK as building block in protocols for data collection and analysis, which are useful to protect privacy while allowing the release of statistics about data. These protocols are of interest in a lot of

settings, e.g. e-commerce, location-based services and smart metering and billing. Thanks to the strong privacy properties offered by SZK, we will be able to design protocols for tasks that before could not be realized while fully protecting user privacy.

Results

SZK is a FNR CORE (junior track) project whose goal is the design of zero-knowledge proof of knowledge protocols with state, i.e., where the prover is able to reuse efficiently statements that have already been proven. The project started on 01/03/2018 and it will last three years. In 2018, we have defined security for SZK protocols and we have provided a construction for a SZK protocol that uses a table as data structure where state information is stored. We have also started work on applying our SZK protocol to practical settings. Concretely, we are applying SZK to construct a priced oblivious transfer protocol that gathers statistics about purchases.

B.13 FNR - Industrial Fellowships Projects

Application of Near Field Technology in Commercial Vehicle Tire Monitoring System

Reference:	R-AGR-3426-10
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - Industrial Fellowships
Budget:	51,000.00 €
Duration:	15 Sep 2018 – 15 Sep 2022
Members:	• Thomas ENGEL (Principal Investigator) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Ahmad RIDA (Doctoral Candidate)
Area:	Communicative Systems
Partner:	Goodyear S.A.

Description

This project addresses the advantages of using near-field based automotive systems in applications where RFID based systems cannot function properly, proposing an automotive tire identification and diagnose system to use on fleet commercial vehicles.

The project will research other capabilities of near-field (NF) technology as a replacement for wire based communication between the tractor and trailer, providing the driver and possibly the control center with crucial information about tire conditions. This is the first study on the use of NF in automotive safety systems as well as the first automotive application using low frequency NF. It will look at the various advantages of the use of NF in such an application, and possibility extend this research to initiate major innovation in the automotive industry using this technology.

Results

The PhD research project has started officially in mid-September 2018. The PhD student Ahmad Tawakuli is investigating the technical background of the project, which is mainly related to Near Field Communications (NFC) for automotive applications. This is crucial to have a better understanding of the research challenges and the different concepts that will be used during the PhD. A literature review of ongoing research projects and studies is being carried out. Moreover, a critical review of solutions proposed so far in the literature is being described. A fruitful meeting with the industry partner supporting the project took place in November 2018.

On the other hand, the PhD student succeeded to established contact with NFC components manufacturers such as Inepro and OPPIOT as well as the RAIN alliance for future cooperation.

B.14 FNR - INTER 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:	• 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.

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 systems 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.

Results

PhD candidate Marie-Laure Zollinger has worked on the UI for the Selene voting system with the UX method. A user-experience test was carried out in Summer 2018 and has resulted in a paper accepted for CHI 2019. A Demo was presented at E-Vote-ID 2018 where a paper on a new paper-based electronic voting system, Electryo, was also presented. A paper in collaboration with UC Louvain has been accepted for Voting'19.

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 protocolS - 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.

Results

This project ended in Summer 2018, however the collaboration with INRIA, Nancy is continuing. Papers were presented at SPW 2018 and E-Vote-ID 2018.

B.15 FNR - JUMP Projects

No more Cryptographic Ransomware

Acronym:	NoCry
PI:	Gabriele LENZINI
Funding:	Fonds National de la Recherche - JUMP (Pathfinder)
Duration:	15 May 2018 – 14 Sep 2018
Members:	• Gabriele LENZINI (Principal Investigator) • Ziya Alper GENÇ (PhD student) • Peter Y A RYAN (Scientific Advisor)

Description

This project is a pathfinder project. It is meant to investigate and assess the commercial viability of the new idea together with its competitive position in the market of an idea that we designed and nighly-build in a prototype. The project is meant to support our activity to understand the requirements coming from potential customers and those necessary for the commercialization of a possible product based on the prototype. We also intend to improve the current nightly-build prototype by improving technology that we have used; we intend also to test and benchmark it carefully in order to be able to propose to potential customers a clear and complete overview of the advantages of the product against the state of the art solutions offered by competitors.That clarified, we disclose that the new idea of this project is an anti-ransomware system.Differently from current anti-ransomware solutions, which are just a few, it does not help recover from a ransomware attack. More specifically, it does not either analyse the behaviour of applications running on a computer in the attempt to find evidence of the presence of a ransomware in the system, like many anti-viruses do, nor it stores information that can be later used to decrypt files when a ransomware has finished its job, a strategy that may fail and has been proved extremely expensive in resources and with no assurance of success.Instead, our solution stops a ransomware before it starts encrypting files. The core idea (invention disclosure #180013) relies on a cryptographic understanding of the way in which ransomware work. Our nighly-build implementation (which we needed to have to provide scientific evidence on the reliability of the idea but which, we need to be stress, is far from being a minimal valuate product) already demonstrates that we can stop 94% of the ransomware from a set of hundreds of real ransomware sample that we collected.This including the currently unstoppable NotPetya, a ransomware used for cyber attacks and currently able to circumvent any existing defense. We believe that our idea has an immense commercial potentiality and with this project, we intend to put this statement to a test. We also intend to come out with a solid plan towards a full commercialization and exploitation of the idea and to define a roadmap to be used in a successive POC proposal.

No more ransomware Proof-of-Concept

Acronym:	NoCry POC
PI:	Gabriele LENZINI
Funding:	Fonds National de la Recherche - JUMP (Pathfinder)
Duration:	2 Nov 2018 – 2 Nov 2020
Members:	• Gabriele LENZINI (Principal Investigator) • Ziya Alper GENÇ (PhD student) • Peter Y A RYAN (Scientific Advisor)

unpredictAble Uav swaRms fOr suRveillAnce

Acronym:	AURORA
PI:	Grégoire DANOY
Funding:	Fonds National de la Recherche - JUMP (Pathfinder)
Budget:	48,000.00 €
Duration:	1 May 2018 – 31 Aug 2018
Members:	• Grégoire DANOY (Principal Investigator) • Pascal BOUVRY (Scientific and Technology Mentoring)

Description

The AURORA (unpredictAble Uav swaRms fOr surveillance) project aims at providing a unique solution through a new generation of aerial surveillance service based on multiple-features autonomous drones evolving simultaneously as a swarm and using unpredictable trajectories.

To this end, AURORA exploits a disruptive artificial intelligence (AI) approach that combines a nature inspired technique (ant colony optimization - ACO) and chaos theory. The developed UAV swarming intelligence is the result of 15 years of expertise in AI and mobile ad hoc networks of the AURORA team.

B.16 FNR - PRIDE Projects

Security and Privacy for System Protection

Acronym:	PRIDE: SPsquared
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - PRIDE

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) • Olga GADYATSKAYA (Research Associate)
Areas:	• Computer Science & ICT Security • Security, Reliability and Trust in Information Technology

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.

Results

The project has hired most of the PhD candidates.

Several publications have been published by the PhD candidates, for example:

- Acceptability and Acceptance of Autonomous Mobility on Demand: The Impact of an Immersive Experience by V. Distler, C. Lallemand, and T. Bellet in Proceedings of the CHI Conference on Human Factors in Computing Systems (2018).
- A Protocol to Strengthen Password-Based Authentication by I. Vasquez Sandoval, B. Stojkovski, and G. Lenzini in Proceedings of International Workshop on Emerging Technologies for Authorization and Authentication (2018).
- On Vulnerability Evolution of Android Apps by J. Gao, L. Li, P. Kong, T. Bissayande, and J. Klein in the 40th International Conference on Software Engineering: Companion Proceeedings (2018).

Security and Privacy for System Protection

Acronym:	SPsquared
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - PRIDE
Budget:	3,037,120.00 €
Duration:	1 Sep 2016 – 31 Aug 2022
Members:	• Sjouke MAUW (Principal Investigator) • Alexei BIRYUKOV (Supervisor / Scientific Advisor) • Jean-Sébastien CORON (Supervisor / Scientific Advisor) • Thomas ENGEL (Supervisor / Scientific Advisor) • Jacques KLEIN (Supervisor / Scientific Advisor) • Gabriele LENZINI (Supervisor / Scientific Advisor) • Volker MÜLLER (Supervisor / Scientific Advisor) • Jun PANG (Supervisor / Scientific Advisor) • Peter Y A RYAN (Supervisor / Scientific Advisor) • Radu STATE (Supervisor / Scientific Advisor)
Area:	Computational Sciences
Partners:	• David Naccache (Université de Paris - II) • University of Luxembourg

Description

The proposed Doctoral Training Unit is set up by the main security researchers of the CSC research unit and the Interdisciplinary Center SnT. The primary goal is to provide a high-quality research environment for PhD students in Security and Privacy and to strengthen research and supervision efforts in this field by fostering cooperation between the applicants through co-supervising PhD students, establishing links between fundamental and applied research and by supporting interdisciplinary research.

B.17 UL Projects

A Personalization Framework for Sentiment Categorization with Recurrent Neural Network

https://acc.uni.lu/index.php?page=projects

Acronym:	PERSEUS
PI:	Christoph SCHOMMER
Funding:	University of Luxembourg
Duration:	15 Jan 2016 – 15 Jan 2020
Members:	• Christoph SCHOMMER (Principal Investigator) • Siwen GUO (Doctoral Candidate) • Sviatlana HOEHN (Scientific Advisor)
Area:	Intelligent and Adaptive Systems
Partner:	DFKI

Description

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 categorisation 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. Aspects of sentiment analysis in chatbots are analysed.

Results

Current progress:

- Evaluating the Effect of Time Gaps in a Personalized Sentiment Model (accepted at ACM SAC 2019)
- Topic-based Historical Information Selection for Personalized Sentiment Analysis (accepted at ESANN 2019)
- Personalized Sentiment Analysis and a Framework with Attention-Based Hawkes Process Model (LNAI 2019)

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.

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.

Future Directions in Symmetric Cryptography

Acronym:	FDISC
PI:	Alexei BIRYUKOV
Funding:	University of Luxembourg
Duration:	1 Oct 2017 – 30 Sep 2019
Members:	• Alexei BIRYUKOV (Principal Investigator) • Qingju WANG (Post-Doc)
Area:	Security, Reliability and Trust in Information Technology

Description

Symmetric cryptographic primitives (e.g. block ciphers, hash functions) form an indispensible part of modern security protocols, most notably TLS and IPSec, where they are used for bulk encryption and the verification of message integrity. The emergence of novel application domains for symmetric cryptosystems, such as the Internet of Things (IoT) or digital currencies, has introduced very specific requirements that were not anticipated in the past. FDISC explores new research directions for the design, analysis and implementation of symmetric primitives with the goal of facilitating their deployment in the afore-mentioned new application domains. The research carried out in the FDISC project consists of two Work Packages (WPs), each involving two tasks. The goal of the first WP is to design and implement a lightweight ARXbased block cipher with provable security guarantees against certain forms of both classical cryptanalysis and side-channel attacks. Thereafter, the second WP aims at designing a provably memory-hard Proof-of-Work (PoW) scheme for digital currencies and developing new approaches for client puzzles suitable for mobile devices.

Results

In the context of WP1 the project team contributed to the cube attack, which is one of the classical statistical cryptanalytic methods in symmetric cryptography. At CRYPTO 2017, the division property based cube attack method was proposed to launch cube attacks with cubes of dimensions far beyond practical reach. The project team introduced several techniques to improve the division property based cube attacks and presented the results from this work at CRYPTO 2018. Related to WP2 is the project team's work to extend the FELICS framework to support the benchmarking of lightweight Authenticated Encryption (AE) algorithms and hash functions. In order to get fine-grained benchmarking results for AE algorithms, a low-level API consisting of seven functions was designed and integrated into the framework. Then, reference implementations of five AE algorithms, namely ACORN, AES-GCM, ASCON, Ketje, and NORX were mapped to the low-level API and a set of preliminary benchmarking results were generated.

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) • Hyacinthe CARTIAUX (Collaborator) • 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

- The paper "ASSA-PBN 3.0: Analysing Context-Sensitive Probabilistic Boolean Networks" has been published in the Proceedings of the 16th International Conference on Computational Methods in Systems Biology (2018).
- The poster "On the Full Control of Boolean Networks" has been published in the Proceedings of the 16th International Conference on Computational Methods in Systems Biology (2018).
- The paper "ASSA-PBN: A Toolbox for Probabilistic Boolean Networks" has been published in IEEE/ACM Transactions on Computational Biology and Bioinformatics (2018).
- The paper "Reviving the two-state Markov chain approach" has been pub-

lished in IEEE/ACM Transactions on Computational Biology and Bioinformatics (2018).
- The paper "A Decomposition-based Approach towards the Control of Boolean Networks" has been published in the Proceedings of the 2018 ACM International Conference on Bioinformatics, Computational Biology, and Health Informatics (2018).
- The paper titled "Towards the Existential Control of Boolean Networks: A Preliminary Report" has been published in the Proceedings of the 4th International Symposium on Dependable Software Engineering. Theories, Tools, and Applications (2018).

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) • 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.

B.18 UL and External Organisation Funding Projects

A Semantic Search Engine for the Retrieve of Similar Patterns in Luxembourgish Texts

http://wiki.uni.lu/mine

Acronym:	STRIPS
PI:	Christoph SCHOMMER
Funding:	University of Luxembourg, External Organisation Funding
Duration:	15 Jan 2018 – 14 Jan 2021
Members:	• Christoph SCHOMMER (Principal Investigator) • Joshgun SIRAJZADE (Researcher)
Area:	Intelligent and Adaptive Systems
Partner:	RTL

Description

The aim of STRIPS is to develop a toolbox of semantic search algorithms for Luxembourgish. We want to implement search algorithms to retrieve and to monitor, e.g., temporal patterns of named entities in Luxembourgish texts. The term 'semantic', hereby, does not only refer to the usage of keywords or Bag-of-Words (for example: names, geographic identifiers), but fosters also on more complex structures like, for example, on concepts (e.g., topics or themes) and a document's sentiment (e.g., a positive or a negative polarity of the document). The main focus of STRIPS lies in the linguistic processing of texts written in Luxembourgish (particularly stemming, use of phonetic dictionaries and tagged word list for Luxembourgish; Part-of-speech-tagged text corpus), in similarity learning aspects to allow fuzziness in search queries, and in the identification of temporal cross-dependencies inside the Luxembourgish text corpus. To validate the project, we have given heterogeneous text sources (official news items and user-contributed comments) by RTL.

B.19 SnT partnership with pEp security Projects

SnT partnership with pEp security

PI:	Gabriele LENZINI
Funding:	SnT partnership with pEp security
Duration:	2 May 2016 – 14 Feb 2019
Members:	• Gabriele LENZINI (Principal Investigator) • Itzel VAZQUEZ SANDOVAL (PhD student) • Iraklis SYMEONIDIS (Research Associate)

Results

The collaboration aiming at analysis the socio-technical security of the pEp application for peer-to-peer encrypted communications continues; the team had a new postdoc Iraklis Symeonidis started in September. The methodology has been enriched with some task on user experience.

B.20 ONRG - NICOP Projects

Heterogeneous multi-swarms of UNmanned auTonomous systEms for mission Deployment

Acronym:	HUNTED
PI:	Pascal BOUVRY
Funding:	Office of Naval Research Global
Budget:	413,000.00 €
Duration:	15 Aug 2018 – 14 Aug 2021
Members:	• Pascal BOUVRY (Principal Investigator) • Grégoire DANOY (Co-Investigator)
Areas:	• Intelligent and Adaptive Systems • Security, Reliability and Trust in Information Technology

Description

The HUNTED project proposes a new generation of mobility models for autonomous and heterogeneous UAS swarms that combines a bio-inspired cooperative approach with the power of chaotic dynamics and adaptive clustering.

These disruptive models will stand out thanks to a first of its kind integration of state-of-the-art solutions that will permit to optimize the missions' objectives and resilience while ensuring unpredictable yet deterministic trajectories in the different swarm levels.

B.21 External Organisation Funding Projects

Building an In-Car Ethernet Testbed System

Reference:	R-AGR-3411-10
PI:	Thomas ENGEL
Funding:	External Organisation Funding
Budget:	30,000.00 €
Duration:	1 May 2018 – 30 Apr 2019
Members:	• Thomas ENGEL (Principal Investigator) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Teng Andrea XU (Research assistant) • Florian ADAMSKY (Post-Doc) • Ridha SOUA (Post-Doc) • Ion TURCANU (Post-Doc)
Area:	Communicative Systems
Partner:	Honda r&d Europe GmbH

Description

Nowadays, cars are becoming increasingly dependant on embedded computers, sensors, cameras, Light Imaging, Detection, And Ranging (LIDAR), etc. to enable safe and comfortable journeys for drivers and passengers. Moreover, self-driving cars will hit our roads in the coming years, which will require an increasing number of advanced sensors and high resolution camera systems. To integrate these features into cars and to ensure the delivery of bandwidth-hungry and delay-sensitive traffic, it is a necessity to have reliable, deterministic and bandwidth-guarantee communication protocols. Current communication technologies adopted by car manufacturers include Controller Area Network (CAN), Local Interconnect Network (LIN), Media Oriented Serial Transport (MOST), and FlexRay. The main limitation of these technologies is that, at the time of their conception, they were not tailored with the sharp rise of high-bandwidth applications.

To support the above mentioned requirements, in-car networks have to undergo significant changes. The inherent features of Ethernet, such as increased bandwidth, low cost and flexibility, makes it a potential candidate to substitute or complement existing in-car communication technologies. Recently, several Ethernet-based protocols have been proposed, such as Audio Video Bridging (AVB)/Time-Sensitive Networking (TSN) and Time-Triggered Ethernet (TTEthernet). It was demonstrated by several simulation studies that AVB/TSN is able to support high volumes of data while fulfilling critical timing constraints. The aim of this project is to build an in-car testbed for testing automotive Ethernet-based solutions and for carrying out realistic traffic load experiments that reflect upcoming in-car communications. To this end, selected open-source Automotive Ethernet protocols will be deployed, while different Ethernet-based topologies will be investigated and evaluated.

Results

The project "Building an In-Car Ethernet Testbed System", officially started in May 2018, has been chosen to receive the 2018 Honda Initiation Grant Europe (HIGE). The main goal of this project is to build an in-car testbed for testing Automotive Ethernet-based solutions and for carrying out realistic traffic load experiments that reflect upcoming in-car communications. To this end, we built a simple testbed using general-purpose single-board computers and conducted experiments to assess the real-time performance of an open-source Audio Video Bridging (AVB)/Time Sensitive Networking (TSN) implementation, namely OpenAvnu. Our preliminary results showed that even under heavy load, AVB/TSN can fulfil the latency requirements of Automotive Ethernet while keeping a constant latency variation. These results have been published in the proceedings of the IEEE Vehicular Networking Conference (VNC) 2018.

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) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Giulia RINALDI (Research assistant) • Florian ADAMSKY (Post-Doc) • Ridha SOUA (Post-Doc)
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

Critical Infrastructures (CIs) use Supervisory Control And Data Acquisition (SCADA) systems for remote control and monitoring. Secan-lab is hosting a SCADA lab provided by CREOS. Secan-Lab team is supporting the CREOS team to set up the VPN connection between Betzdorf and Maison du Nombre. The aim is to collect real data that can be used to form a solid basis for the analysis of network behavior in the presence of e.g., network attacks and other effects we could emulate.

On the other hand, traditional Intrusion Detection Systems (IDSs) cannot detect attacks that are not already present in their databases. Therefore, we assessed Machine Learning techniques for intrusion detection in SCADA systems using a real data set collected from a gas pipeline system and provided by the Mississippi State University. We have used SVM, RF and LSTM to implement diverse IDS classifiers. A complete comparison between these algorithms was provided along with the random hyper-parameters search results. Contrary to the state of the art studies, the use of the test set accuracy, precision, recall and F1 score allowed us to assess correctly and comprehensively their performances.

In addition, IDSs are facing many unprecedented challenges due the specific characteristics of SCADA such as heterogeneity, large-scale deployment and maintenance. Leveraging on the Software-Defined Networking (SDN) paradigm and entropies, we have introduced the softwarization of SCADA by designing distributed SDN-agents that ensure at the same time fast anomaly detection and flexible programmability. Conducted tests using Floodlight and the defacto network protocols of SCADA demonstrate the high potential of using SDN.

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) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Tatiana RETUNSKAIA (Research assistant) • Florian ADAMSKY (Post-Doc)
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 built two prototypes. The first one measures the distance between two wireless devices with the Time Stamp Function (TSF) with ± 1-2 m accuracy. The other prototype captures the Channel State Information (CSI) of a wireless devices and creates a unique fingerprint of it.

Appendix C

Representational Activities

C.1 Conference Committee Memberships

10th International Workshop on Immersive Mixed and Virtual Environment Systems (MMVE 2018)

Location: Amsterdam, Netherlands, 12 Jun 2018.

Participating Members:

- Jean BOTEV (Steering Committee Member)

11th International Conference on Information Technology and Communications Security

Location: Bucharest, Romania, 8 Nov 2018 – 9 Nov 2018.

Participating Members:

- Peter Y A RYAN (Program Committee Member)

11th International Conference on Security for Information Technology and Communications (SecITC 2018)

http://www.secitc.eu

Location: Bucharest, Romania, 8 Nov 2018 – 9 Nov 2018.

Participating Members:

- Johann GROSZSCHÄDL (Paper presentation)

12th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO 2018)

Location: Trento, Italy, 3 Sep 2018 – 7 Sep 2018.

Participating Members:

- Jean BOTEV (Programme Chair)

12th International Conference on Information Security Theory and Practice (WISTP 2018)

http://www.wistp.org/wistp2018

Location: Brussels, Belgium, 10 Dec 2018 – 11 Dec 2018.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member, Paper presentation)

13th International Workshop on the Implementation of Logics

http://www.eprover.org/EVENTS/IWIL-2018.html

Location: Awassa, Ethiopia, 16 Nov 2018.

Description: The **13th International Workshop on the Implementation of Logics** will be held in November 2018 in conjunction with the 22th International Conference on Logic for Programming, Artificial Intelligence and Reasoning, at the Haile Resort in Awassa, Ethiopia.

We are looking for contributions describing implementation techniques for and implementations of automated reasoning programs, theorem provers for various logics, logic programming systems, and related technologies. Topics of interest include, but are not limited to:

- Propositional logic and decision procedures, including SMT
- First-order and higher order logics
- Non-classical logics, including modal, temporal, description, non-monotonic reasoning
- Formal foundations for efficient implementation of logics
- Data structures and algorithms for the efficient representation and processing of logical concepts

- Proof/model search organization and heuristics for logical reasoning systems
- Data analysis and machine learning approaches to search control
- Techniques for proof/model search visualization and analysis
- Practical constraint handling
- Reasoning with ontologies and other large theories
- Implementation of efficient theorem provers and model finders for different logics
- System descriptions of logical reasoning systems
- Issues of reliability, witness generation, and witness verification
- Evaluation and benchmarking of provers and other logic-based systems
- I/O standards and communication between reasoning systems

We are particularly interested in contributions that help the community to understand how to build useful and powerful reasoning systems, and how to apply them in practice.

Participating Members:

- Alexander STEEN (Program Committee Member)

14th IEEE International Workshop on Factory Communication Systems (WFCS'2018)

http://wfcs2018.ieiit.cnr.it/

Location: Imperia, Italy, 13 Jun 2018 – 15 Jun 2018.

Description: WFCS is the largest IEEE conference especially dedicated to industrial communication systems and technologies. The aim of the WFCS series is to provide a forum for researchers, developers and practitioners to review and discuss most recent trends in the area and share innovative research directions.

Participating Members:

- Qin MA (Program Committee Member)
- Tingting HU (Short Papers, Posters, and Demo Co-Chair)

16th IEEE International Conference on Pervasive Intelligence and Computing (PICom)

http://cyber-science.org/2018/picom/

Location: Athens, Greece, 12 Aug 2018 – 15 Aug 2018.

Participating Members:

- Grégoire DANOY (Program Committee Member)

17th INTERNATIONAL WORKSHOP ON NON-MONOTONIC REASONING (NMR 2018)

http://www4.uma.pt/nmr2018/

Location: Tempe, United States of America, 27 Oct 2018 – 29 Oct 2018.

Description: NMR is the premier forum for results in the area of Non-Monotonic Reasoning. Its aim is to bring together active researchers in this broad field within knowledge representation and reasoning (KR), including belief revision, uncertain reasoning, reasoning about actions, planning, logic programming, preferences, argumentation, causality, and many other related topics including systems and applications.

NMR has a long history — it started in 1984, and is held every two years. Recent previous NMR workshops were held in Cape Town (2016) Vienna (2014) Rome (2012), Toronto (2010), Sydney (2008), and Lake District (UK) (2006).

Participating Members:

- Emil WEYDERT (Program Committee Member)

1st International Conference on Applied Informatics (ICAI 2018

http://icai.itiud.org/

Location: Bogota, Colombia, 1 Nov 2018 – 3 Nov 2018.

Participating Members:

- Grégoire DANOY (Program Committee Member)

21st Information Security Conference

Location: London, United Kingdom, 9 Sep 2018 – 12 Sep 2018.

Participating Members:

- Peter Y A RYAN (Program Committee Member)

23rd European Symposium on Research in Computer Security

Location: Barcelona, Spain, 3 Sep 2018 – 7 Sep 2018.

Participating Members:

- Peter Y A RYAN (Program Committee Member)

24th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2018)

http://asiacrypt.iacr.org/2018

Location: Brisbane, Australia, 2 Dec 2018 – 6 Dec 2018.

Participating Members:

- Aleksei UDOVENKO (Paper presentation)

25th International Conference on Fast Software Encryption (FSE 2018)

http://fse.iacr.org/2018

Location: Brussels, Belgium, 5 Mar 2018 – 7 Mar 2018.

Participating Members:

- Aleksei UDOVENKO (Attendant)

26th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2018)

https://conf.researchr.org/home/fse-2018

Location: Lake Buena Vista (FL), United States of America, 4 Nov 2018 – 9 Nov 2018.

Description: The ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE) is an internationally renowned forum for researchers, practitioners, and educators to present and discuss the most recent innovations, trends, experiences, and challenges in the field of software engineering. Formerly the FSE conference in alternating years and ESEC/FSE in other years, ESEC/FSE is now the new name of this annual conference series. The ESEC/FSE conference brings together experts from academia and industry to exchange the latest research results and trends, as well as their practical application in all areas of software engineering.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

30th Benelux Conference on Artificial Intelligence (BNAIC 2018)

https://bnaic2018.nl/

Location: ‘s-Hertogenbosch, Netherlands, 8 Nov 2018 – 9 Nov 2018.

Participating Members:

- Grégoire DANOY (Program Committee Member)

33rd IFIP TC-11 SEC 2018 International Conference on Information Security and Privacy Protection

Location: Poznan, Poland, 18 Sep 2018 – 20 Sep 2018.

Participating Members:

- Gergely BANA (PC Member)

38th International Cryptology Conference (CRYPTO 2018)

http://crypto.iacr.org/2018

Location: Santa Barbara (CA), United States of America, 19 Aug 2018 – 23 Aug 2018.

Participating Members:

- Qingju WANG (Paper presentation)

3rd International Conference on Applications in Information Technology

http://icait-aizu.org/

Location: Aizu-Wakamatsu, Japan, 1 Nov 2018 – 3 Nov 2018.

Description: The 3rd International Conference on Applications in Information Technology is the meeting point for young researchers, scholars and IT-industry professionals interested in advancing computer science and technology towards serving society and expectations of the day in the digitally transforming world.

Participating Members:

- Alfredo CAPOZUCCA (Program Committee Member)
- Nicolas GUELFI (Program Committee Member)
- Benoit RIES (Program Committee Member)

3rd MIning and REasoning with Legal texts Workshop (MIREL2018)

https://sites.google.com/view/mirelworkshop2018/

Location: Esch-sur-Alzette, Luxembourg, 17 Sep 2018.

Description: The aim of MIREL-2018 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:

- Leon VAN DER TORRE (Co-Chair)
- Giovanni CASINI (Program Committee Member)
- Xavier PARENT (Program Committee Member)
- Livio ROBALDO (Program Committee Member)

3rd Winter School in Computer Science and Engineering on Blockchains and Cryptocurrencies (CSE 2018)

http://ias.huji.ac.il/CSE3

Location: Jerusalem, Israel, 16 Dec 2018 – 20 Dec 2018.

Participating Members:

- Sergei TIKHOMIROV (Attendant)

43nd IEEE Conference on Local Computer Networks (IEEE LCN 2018)

Location: Chicago, United States of America, 1 Oct 2018 – 4 Oct 2018.

Description: The IEEE LCN conference is the premier conference on theoretical and practical aspects of computer networking. LCN is highly interactive, enabling an effective interchange of results and ideas among researchers, users, https://www.ieeelcn.org/prior/LCN43/index.html

and product developers. Major developments from high-speed networks to the global Internet to specialized sensor networks have been reported at past LCNs. Please join us for our 43rd annual meeting in Chicago!

Participating Members:

- Matthias R. BRUST (Technical Program Committee Member)

5th International Workshop on Self-Improving System Integration (SISSY 2018)

Location: Trento, Italy, 7 Sep 2018.

Participating Members:

- Jean BOTEV (Program Committee Member)

6th International Workshop on Self-Optimisation in Autonomic & Organic Computing Systems (SAOS 2018)

Location: Braunschweig, Germany, 9 Apr 2018.

Participating Members:

- Jean BOTEV (Co-Chair)

7th International Workshop on Peer-to-Peer Architectures, Networks and Systems (PANS 2018)

Location: Orléans, France, 17 Jul 2018.

Participating Members:

- Jean BOTEV (Program Committee Member)

8th IEEE Workshop Parallel / Distributed Computing and Optimization (PDCO 2018)

https://pdco2018.sciencesconf.org

Location: Vancouver, Canada, 21 May 2018 – 25 May 2018.

Description: The IEEE Workshop PDCO 2018, Vancouver, Canada, will be the 8th edition of the IEEE Workshop on Parallel / Distributed Computing and Optimization that will be held in conjunction with the 32nd IEEE International Parallel and Distributed Processing Symposium.

Participating Members:

- Pascal BOUVRY (Steering Committee Member)
- Sébastien VARRETTE (Program Committee Member)
- Grégoire DANOY (General Chair)

8th international conference on bioinspired optimization methods and their applications (BIOMA 2018)

https://bioma2018.sciencesconf.org

Location: Paris, France, 16 May 2018 – 18 May 2018.

Participating Members:

- Pascal BOUVRY (Program Committee Member)
- Grégoire DANOY (Program Committee Member)

9th ACM Multimedia Systems Conference (MMSys 2018)

Location: Amsterdam, Netherlands, 12 Jun 2018 – 15 Jun 2018.

Participating Members:

- Jean BOTEV (Program Committee Member)

ATENA workshop

Location: Esch/Alzette, Luxembourg, 18 Oct 2018.

Description: The Workshop was split into a morning session with keynote speeches by Klaus Kursawe of Gridsec and François Thill of the Ministry of Economy, followed by technical presentations of the ATENA work packages and main results. The afternoon session consisted of demonstrations of some of the ATENA tools, followed by short presentations of other related research projects, namely the H2020 project RESISTO and the national projects SGL Cockpit and IDS4ICS. Finally, the day was capped off with a round table involving Klaus Kursawe, Reinhard Hutter, Leonid Lev, and Paolo Pucci, moderated by Carlo Harpes.

Participating Members:

- Florian ADAMSKY (Workshop Organiser / Co-Organiser)

- Thomas ENGEL (Workshop Organiser / Co-Organiser)
- Aurel MACHALEK (Workshop Organiser / Co-Organiser)
- Mohamed Nizar MSADEK (Workshop Organiser / Co-Organiser)
- Stefan SCHIFFNER (Workshop Organiser / Co-Organiser)
- Ridha SOUA (Workshop Organiser / Co-Organiser)

BELGIUM-NETHERLANDS CONFERENCE ON ARTIFICIAL INTELLIGENCE (BNAIC 2018

https://bnaic2018.nl/

Location: ‘s-Hertogenbosch, Netherlands, 8 Nov 2018 – 9 Nov 2018.

Description: This year, the 30th Benelux Conference on Artificial Intelligence (BNAIC 2018) is organized by the Jheronimus Academy of Data Science (JADS), under the auspices of the Benelux Association for Artificial Intelligence (BN-VKI) and the Dutch Research School for Information and Knowledge Systems (SIKS).
BNAIC 2018 will be held at JADS, Den Bosch, The Netherlands, co-located with Benelearn 2018, as a two day event: on Thursday 8 and Friday 9 November, 2018. BNAIC 2018 will include invited speakers, research presentations, posters and demonstrations. Also, a number of special sessions will be organized, including a ‘research meets business’ session.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

CoDeX FutureLaw

https://conferences.law.stanford.edu/futurelaw2018/

Location: Stanford, United States of America, 5 Apr 2018.

Description: On April 5, 2018, CodeX – the Stanford Center for Legal Informatics will host the **CodeX FutureLaw 2018**, CodeX’s sixth annual conference focusing on how technology is changing the landscape of the legal profession, the law itself, and how these changes impact us all.

CodeX FutureLaw 2018 will bring together the academics, entrepreneurs, lawyers, investors, policy makers, and engineers spearheading the tech-driven transformation of our legal system.

Join us for a unique educational event and an opportunity to connect and exchange ideas with legal tech innovators from around the world!

Participating Members:

- Arianna ROSSI (Invited Speaker)

COMPUTATIONAL MODELS OF ARGUMENT (COMMA 2018)

http://comma2018.argdiap.pl

Location: Warsaw, Poland, 12 Sep 2018 – 14 Sep 2018.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)
- Emil WEYDERT (Program Committee Member)

Computer and Communications Security Posters/Demonstrations

Location: Toronto, Canada, 15 Oct 2018 – 19 Oct 2018.

Participating Members:

- Peter Y A RYAN (Program Committee Member)

Cross-Domain Conference for Machine Learning and Knowledge Extraction (CD-MAKE 2018)

https://2018.cd-make.net/

Location: Hambourg, Germany, 27 Aug 2018 – 30 Aug 2018.

Participating Members:

- Sjouke MAUW (Program Committee Member)

Dagstuhl Seminar 18021: Symmetric Cryptography

http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=18021

Location: Wadern, Germany, 7 Jan 2018 – 12 Jan 2018.

Participating Members:

- Alexei BIRYUKOV (Paper presentation)

Dagstuhl Seminar 18152: Blockchains Smart Contracts and Future Applications

http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=18152

Location: Wadern, Germany, 8 Apr 2018 – 13 Apr 2018.

Participating Members:

- Alexei BIRYUKOV (Paper presentation)

Dagstuhl Seminar 18461: Blockchain Security at Scale

http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=18461

Location: Wadern, Germany, 11 Nov 2018 – 16 Nov 2018.

Participating Members:

- Alexei BIRYUKOV (Paper presentation)

Deduktionstreffen 2018

https://fg-dedsys.gi.de/dt2018.html

Location: Esch-sur-Alzette, Luxembourg, 21 Sep 2018.

Description: The annual meeting Deduktionstreffen is the prime activity of the Interest Group for Deduction Systems (FGDedSys) of the German Informatics Society. It is a meeting with a familiar, friendly atmosphere, where everyone interested in deduction can report on their work in an informal setting.

A special focus of the Deduktionstreffen is on young researchers and students, who are particularly encouraged to present their ongoing research projects to a wider audience. Another goal of the meeting is to stimulate networking effects and to foster collaborative research projects.

Participating Members:

- Alexander STEEN (Organising Committee, PC Chair)

DEONTIC LOGIC IN COMPUTER SCIENCE (DEON 2018)

Location: Utrecht, Netherlands, 3 Jul 2018 – 6 Jul 2018.

https://deon2018.sites.uu.nl/

Description: The biennial DEON conferences are designed to promote interdisciplinary cooperation amongst scholars interested in linking the formal-logical study of normative concepts and normative systems with computer science, artificial intelligence, philosophy, organization theory and law.
In addition to these general themes, DEON 2018 will encourage a special focus on the topic:
"Deontic reasoning for responsible AI""

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

DEPENDABLE SYSTEMS AND NETWORKS

https://dsn2018.uni.lu/

Location: Luxembourg, Luxembourg, 25 Jun 2018 – 28 Jun 2018.

Participating Members:

- Nicolas GUELFI (Publicity co-Chair)

DEVOPS 18: First international workshop on software engineering for continuous development and new paradigms of software production and deployment

https://www.laser-foundation.org/devops/2018/

Location: Villebrumier, France, 5 Mar 2018 – 6 Mar 2018.

Participating Members:

- Alfredo CAPOZUCCA (Program Committee Member)

ECRYPT-NET School on Integrating Advanced Cryptography with Applications 2018

Location: Kos, Greece, 16 Sep 2018 – 21 Sep 2018.

Participating Members:

http://www.cosic.esat.kuleuven.be/events/ecrypt-net-school-2018

- Luan CARDOSO DOS SANTOS (Attendant)

ERCIM-Blockchain 2018: Blockchain Engineering: Challenges and Opportunities for Computer Science Research

http://easychair.org/cfp/ERCIMBlockchain2018

Location: Amsterdam, Netherlands, 8 May 2018 – 9 May 2018.

Participating Members:

- Sergei TIKHOMIROV (Paper presentation)

EUROPEAN WORKSHOP ON MULTI-AGENT SYSTEMS (EUMAS 2018)

https://eumas2018.w.uib.no/

Location: Bergen, Norway, 6 Dec 2018 – 7 Dec 2018.

Description: The 16th European Conference on Multi-Agent Systems (EUMAS 2018) will be held December 6 & 7, 2018 in Bergen Norway. EUMAS 2018, 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, Evry 2017), 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 2018 offers three submission types and formal proceedings in a LNCS/LNAI Springer volume. 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)

E-Vote-ID 2018

Location: Bregenz, Austria, 2 Oct 2018 – 5 Oct 2018.

Participating Members:

- Peter Y A RYAN (Program Committee Member)
- Peter ROENNE (Outreach chair, Demo chair)

GCAI 2018

https://easychair.org/smart-program/LuxLogAI2018/GCAI-index.html

Location: Esch-sur-Alzette, Luxembourg, 17 Sep 2018 – 19 Sep 2018.

Description: The 4th Global Conference on Artificial Intelligence (GCAI 2018) will be held in Luxembourg, 17-19 September 2018 and is supported by the Luxembourg National Research Fund (FNR) (12426287).

Participating Members:

- Xavier PARENT (Program Committee Member)
- Christoph SCHOMMER (Program Committee Member)
- Alexander STEEN (Program Committee Member)
- Martin THEOBALD (Program Committee Member)
- Xavier PARENT (Organising Committee)
- Martin THEOBALD (Organising Committee)
- Leon VAN DER TORRE (Organising Committee)

Genetic and Evolutionary Computation Conference (GECCO-2018)

http://gecco-2018.sigevo.org

Location: Kyoto, Japan, 15 Jul 2018 – 19 Jul 2018.

Participating Members:

- Grégoire DANOY (Program Committee Member)

Grande Region Security and Reliability Day (GRSRD 2018)

Location: Saarbruecken, Germany, 12 Mar 2018.

Participating Members:

- Jun PANG (Program Committee Member)

https://cispa.saarland/grsrd18/

HPC School 2018 - Newcomer Training Day

https://hpc.uni.lu/hpc-school/2018/11/index.html

Location: Belval, Luxembourg, 23 Nov 2018.

Description: The UL HPC team 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 the storage data management (backups, git, GDPR, quotas)
- HPC workflow management (for sequential and parallel tasks)
- Advanced scheduling (on Slurm and OAR)
- Parallel programming with OpenMP/MPI

The aim is to cover basic and intermediate-level 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**.

Participating Members:

- Valentin PLUGARU (Co-Chair)

HPC School 2018 - Summer School

https://hpc.uni.lu/hpc-school/2018/06/index.html

Location: Belval, Luxembourg, 12 Jun 2018 – 13 Jun 2018.

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 the storage data management (backups, git, **GDPR**, quotas)
- HPC workflow management (for sequential and parallel tasks)
- HPC programming and usage of the main software available on the platform, with dedicated sessions directed towards Matlab/Mathematica, R, Python, OpenMP/MPI, MultiPhysics, Chemistry, Bioinformatics, Big Data analytics, Deep and Machine learning etc.

- Debugging and profiling
- Software environment management
- Virtualization with containers 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**.

Participating Members:

- Valentin PLUGARU (Co-Chair, Co-Chair)

ICAART 2018

http://www.icaart.org/?y=2018

Location: Funchal, Portugal, 16 Jan 2018 – 18 Jan 2018.

Participating Members:

- Siwen GUO (Invited Speaker)
- Christoph SCHOMMER (PC Member)

ICDE

Location: Paris, France, 16 Apr 2018 – 19 Apr 2018.

Participating Members:

- Martin THEOBALD (Attendant)

ICSE 2018 Student Research Competition

http://www.icse2018.org/track/icse-2018-ACM-Student-Research-Competition

Location: Gothenburg, Sweden, 30 May 2018 – 1 Jun 2018.

Participating Members:

- Jun PANG (Program Committee Member)

IEEE CLOUDCOM 2018

Location: Nicosia, Cyprus, 10 Dec 2018 – 13 Dec 2018.

Description: **CloudCom** is the premier conference on Cloud Computing worldwide, attracting researchers, developers, users, students and practitioners from https://cyprusconferences.org/cloudcom2018/

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 10th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2018) will be held in Nicosia, Cyprus on 10-13 December 2018.

Participating Members:

- Valentin PLUGARU (Program Committee Member)

IEEE Congress on Evolutionary Computation (IEEE CEC 2018)

http://www.ecomp.poli.br/~wcci2018/

Location: Rio de Janeiro, Brazil, 8 Jul 2018 – 13 Jul 2018.

Participating Members:

- Grégoire DANOY (Program Committee Member)

IEEE Consumer Communications & Networking Conference

http://ccnc2018.ieee-ccnc.org/about

Location: Las Vegas, United States of America, 12 Jan 2018 – 15 Jan 2018.

Description: Held in conjunction with the International Consumer Electronics Show (CES), the world's largest tradeshow on consumer technology, the IEEE Consumer Communications and Networking Conference (CCNC) is a major annual international conference organized with the objective of bringing together researchers, developers, and practitioners from academia and industry working in all areas of consumer communications and networking.

IEEE CCNC was organized specifically to help the consumer technology industry drive the advance of the numerous wireless and wireline communications technologies and applications that will one day provide secure and reliable on-demand access to both entertainment and information anytime and anywhere. Included in CCNC's scope are nearly every technological area ranging from cognitive and peer-to-peer networking to the services, tools, and devices used to ensure ease-of-use, privacy and stunning interactivity.

IEEE CCNC 2018 presents the latest developments and technical solutions in the areas of home networking, consumer networking, enabling technologies (such as middleware) and novel applications and services. The conference includes a peer-reviewed program of technical sessions, workshops, business application panels, tutorials, demonstration sessions as well as keynotes from leading figures in industry and academia.

Participating Members:

- Ridha SOUA (Technical Program Committee Member)

IEEE Global Communication Conference 2018 (IEEE GLOBECOM 2018)

https://globecom2018.ieee-globecom.org/

Location: Abu Dhabi, United Arab Emirates, 9 Dec 2018 – 13 Dec 2018.

Description: Themed "Gateway to a Connected World," the conference will offer five full days of original paper presentations, tutorials, workshops, keynotes, demonstrations, industry sessions and social events designed to further career opportunities and the in-depth understanding of the latest communications advancements worldwide.

Participating Members:

- Matthias R. BRUST (Technical Program Committee Member)

IEEE Global Communications Conference (GLOBECOM)

https://globecom2018.ieee-globecom.org/

Location: Abu Dhabi, United Arab Emirates, 9 Dec 2018 – 13 Dec 2018.

Description: Themed "Gateway to a Connected World," the conference will offer five full days of original paper presentations, tutorials, workshops, keynotes, demonstrations, industry sessions and social events designed to further career opportunities and the in-depth understanding of the latest communications advancements worldwide.

Participating Members:

- Latif LADID (Technical Program Committee Member)
- Ridha SOUA (Technical Program Committee Member)

IEEE/IFIP INTERNATIONAL SYMPOSIUM ON THEORETICAL ASPECTS OF SOFTWARE ENGINEERING

Location: Guangzhou, China, 29 Aug 2018 – 31 Aug 2018.

Participating Members:

- Pierre KELSEN (Program Committee Member)

IEEE International Conference on Communications 2018 (IEEE ICC 2018)

https://icc2018.ieee-icc.org/content/welcome-ieee-icc-2018

Location: Kansas City, United States of America, 20 May 2018 – 24 May 2018.

Description: Themed ”Communications for Connecting Humanity,” the conference will offer five full days of original paper presentations, tutorials, workshops, keynotes, demonstrations, industry panels and social events designed to further career opportunities and the in-depth understanding of the latest communications advancements worldwide.

Participating Members:

- Matthias R. BRUST (Technical Program Committee Member)

IEEE International Conference on Computer Communications 2018 (IEEE INFOCOM 2018) - WKSHPS IECCO 2018

https://infocom2018.ieee-infocom.org/

Location: Honolulu, United States of America, 15 Apr 2018 – 19 Apr 2018.

Participating Members:

- Matthias R. BRUST (Technical Program Committee Member)

International Colloquium on Theoretical Aspects of Computing (ICTAC 2018)

Location: Stellenbosch, South Africa, 12 Oct 2018 – 19 Oct 2018.

Participating Members:

https://www.ictac.org.za/

- Ross James HORNE (Program Committee Member)

International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2018)

http://celweb.vuse.vanderbilt.edu/aamas18/

Location: Stockholm, Sweden, 10 Jul 2018 – 15 Jul 2018.

Description: AAMAS (International Conference on Autonomous Agents and Multiagent Systems) 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. AAMAS is the flagship conference of the non-profit International Foundation for Autonomous Agents and Multiagent Systems (IFAAMAS).

AAMAS 2018, the 17th edition of the conference, will be held on July 10-15, in Stockholm, Sweden and is part of the Federated AI Meeting (FAIM), with the other conferences being IJCAI, ICML, ICCBR and SoCS. Please see the preliminary schedule for more information.

The AAMAS conference series was initiated in 2002 in Bologna, Italy as a joint event comprising the 6th International Conference on Autonomous Agents (AA), the 5th International Conference on Multiagent Systems (ICMAS), and the 9th International Workshop on Agent Theories, Architectures, and Languages (ATAL).

Subsequent AAMAS conferences have been held in Melbourne, Australia (July 2003), New York City, NY, USA (July 2004), Utrecht, The Netherlands (July 2005), Hakodate, Japan (May 2006), Honolulu, Hawaii, USA (May 2007), Estoril, Portugal (May 2008), Budapest, Hungary (May 2009), Toronto, Canada (May 2010), Taipei, Taiwan (May 2011), Valencia, Spain (June 2012), Minnesota, USA (May 2013), Paris, France (May 2014), Istanbul, Turkey (May 2015), Singapore (May 2016) and São Paulo (2017).

Participating Members:

- Leon VAN DER TORRE (SPC member)

International Conference on Cryptology and Network Security (CANS)

Location: Naples, Italy, 30 Sep 2018 – 3 Oct 2018.

Participating Members:

- Vincenzo IOVINO (Program Committee Member)
- Alfredo RIAL DURAN (Program Committee Member)
- Peter Y A RYAN (Program Committee Member)
- Vincenzo IOVINO (General Chair)

International Conference on Historical Cryptography (HistoCrypt 2018)

https://www2.lingfil.uu.se/histocrypt2018/home.phtml

Location: Uppsala, Sweden, 20 Jun 2018.

Participating Members:

- Sjouke MAUW (Program Committee Member)

INTERNATIONAL CONFERENCE ON LEGAL KNOWLEDGE AND INFORMATION SYSTEMS (JURIX 2018)

http://jurix2018.ai.rug.nl/

Location: Groningen, Netherlands, 12 Dec 2018 – 14 Dec 2018.

Description: JURIX 2018 is the 31st international conference on Legal Knowledge and Information Systems, hosted by the Faculty of Law and the department of Artificial Intelligence in the Bernoulli Institute of Mathematics, Computer Science and Artificial Intelligence, Faculty of Science and Engineering of the University of Groningen. JURIX is the annual international conference on Legal Knowledge and Information Systems, organised by the Foundation for Legal Knowledge Based Systems (JURIX) since 1988. JURIX 2018 is organised in cooperation with the Dutch Research School for Information and Knowledge Systems (SIKS).

JURIX 2018 is held in Het Kasteel, Melkweg 1, Groningen, The Netherlands, on Wednesday December 12 till Friday December 14, 2018.

Participating Members:

- Livio ROBALDO (Program Committee Member)
- Leon VAN DER TORRE (Program Committee Member)

INTERNATIONAL CONFERENCE ON PRINCIPLES OF KNOWLEDGE REPRESENTATION AND REASONING (KR2018)

http://reasoning.eas.asu.edu/kr2018/

Location: Tempe, United States of America, 30 Oct 2018 – 2 Nov 2018.

Description: Knowledge Representation and Reasoning (KR) is an exciting, well-established field of research. In KR a fundamental assumption is that an agent's knowledge is explicitly represented in a declarative form, suitable for processing by dedicated reasoning engines. This assumption, that much of what an agent deals with is knowledge-based, is common in many modern intelligent systems. Consequently, KR has contributed to the theory and practice of various areas in AI, such as automated planning, natural language understanding, among others, as well as to fields beyond AI, including databases, verification, and software engineering. In recent years KR has contributed to new and emerging fields including the semantic web, computational biology, and the development of software agents.

The KR conference series is a leading forum for timely in-depth presentation of progress in the theory and principles underlying the representation and computational management of knowledge. KR 2018 will be a forum for the exchange and discussion of new ideas, issues, and results on the principles and practice of KR.

Participating Members:

- Giovanni CASINI (Program Committee Member)
- Leon VAN DER TORRE (Program Committee Member)
- Emil WEYDERT (Program Committee Member)

INTERNATIONAL CONFERENCE ON PRINCIPLES OF PRACTICE IN MULTI-AGENT SYSTEMS (PRIMA 2018)

http://2018.prima-conference.org/

Location: Tokyo, Japan, 31 Oct 2018 – 2 Nov 2018.

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.

The 21st International Conference on Principles and Practice of Multi-Agent Systems (PRIMA 2018) invites submissions of original, unpublished, theoretical and applied work on any such topic, and encourages reports on the development of prototype and deployed agent systems, and of experiments that demonstrate novel agent system capabilities.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

INTERNATIONAL JOINT CONFERENCE ON ARTIFICIAL INTELLIGENCE (IJCAI 2018)

https://www.ijcai-18.org/

Location: Stockholm, Sweden, 13 Jul 2018 – 19 Jul 2018.

Description: Welcome to IJCAI-ECAI 2018, the 27th International Joint Conference on Artificial Intelligence and the 23rd European Conference on Artificial Intelligence, the premier international gathering of researchers in AI!IJCAI-ECAI-18 is part of the Federated AI Meeting (FAIM) that takes place at Stockholmsmässan in Stockholm July 9-19. The other conferences include AAMAS, ICML, ICCBR and SoCS. The World Computer Chess Championships will also take place in parallel. Please see the preliminary joint schedule for more information.

Participating Members:

- Giovanni CASINI (Program Committee Member)
- Xavier PARENT (Program Committee Member)
- Livio ROBALDO (Program Committee Member)
- Emil WEYDERT (Program Committee Member)
- Leon VAN DER TORRE (SPC member)

International Symposium on Networks, Computers and Communications (ISNCC)

http://www.isncc-conf.org/

Location: Rome, Italy, 19 Jun 2018 – 21 Jun 2018.

Description: **ISNCC 2018 cover theoretical and practical aspects related to Information Systems, Communication Networks and Computing Technologies. This year, the multi-thematic program focuses on the major future scientific issues for the following scientific topics, divided into eight main tracks:**

- **Wireless and Mobile Communications & Networking**
- **Satellite Communications and Networking**
- **Antenna Systems, Propagation and RF Design**
- 5G Evolution and Implementation
- Cloud, Grid and Social Computing & Networking
- Internet of Everything, Data Analytics and **Smart Cities**
- Smart Communications Systems
- Trust, Security and Privacy

Participating Members:

- Ridha SOUA (Technical Program Committee Member)

International workshop on optimization and learning: Challenges and Applications (OLA 2018)

https://ola2018.sciencesconf.org

Location: Alicante, Spain, 26 Feb 2018 – 28 Feb 2018.

Participating Members:

- Pascal BOUVRY (Programme Chair)
- Grégoire DANOY (Program Committee Member)

International Workshop on Petri Nets and Modeling

https://www.informatik.uni-hamburg.de/TGI/events/pemod18/

Location: Braunschweig, Germany, 21 Feb 2018.

Participating Members:

- Nicolas GUELFI (Program Committee Member)

International Workshop on Petri Nets and Software Engineering

Location: Bratislava, Slovakia, 25 Jun 2018 – 26 Jun 2018.

Participating Members:

- Nicolas GUELFI (Program Committee Member) http://www.informatik.uni-hamburg.de/TGI/events/pnse/

International Workshop on Secure Internet of Things (SIoT)

Location: Barcelona, Spain, 6 Sep 2018.

Participating Members:

- Alfredo RIAL DURAN (Program Committee Member)

INTERNATIONAL WORLD WIDE WEB CONFERENCE

https://www2018.thewebconf.org/

Location: Lyon, France, 23 Apr 2018 – 27 Apr 2018.

Description: **The Web Conference** (formerly www conference) is a yearly international conference on the topic of the future directions of the World Wide Web.

It began in 1994 at CERN and is organized by the **International World Wide Web Conferences Steering Committee (IW3C2)**. The Conference aims to provide the world with a premier forum for discussion and debate about the evolution of the Web, the standardization of its associated technologies, and the impact of those technologies on society and culture. The conference brings together researchers, developers, users and commercial ventures — indeed all those who are passionate about the Web and what it has to offer.

Participating Members:

- Giovanni CASINI (Program Committee Member)

Legal Design as Academic Discipline: Foundations Methodology Applications

http://gdprbydesign.cirsfid.unibo.it/legaldesign-workshop/

Location: Groningen, Netherlands, 12 Dec 2018.

Description: The workshop “Legal Design as Academic Discipline: Foundations, Methodology, Applications” will take place on December 12, 2018 (**full-day**) in Het Kasteel (Melkweg 1, 9718 EP Groningen, Netherlands). The workshop is co-located with JURIX, the 31st international conference on Legal Knowledge and Information Systems.

Legal Design is an interdisciplinary approach to apply human-centered design to prevent or solve legal problems. It can help to create functional, inclusive and transparent legal documents, services, and systems. Whereas Legal Design is enjoying notable success in the business world, it has not yet been established as an academic discipline.

This workshop welcomes **theoretical contributions**, for instance on:

- What is Legal Design? What is it not?
- Which methodologies can be applied and for which purposes?
- From which neighboring research fields can Legal Design benefit?
- What is the added value of Legal Design to the academic field?
- How can Legal Design help to develop and validate new legal theories?

Participating Members:

- Arianna ROSSI (Workshop Organiser / Co-Organiser)

LuxLogAI

https://luxlogai.uni.lu/

Location: Esch-sur-Alzette, Luxembourg, 17 Sep 2018 – 26 Sep 2018.

Description: The Luxembourg Logic for AI Summit (LuxLogAI 2018) brings together, amongst others, the 2nd International Joint Conference on Rules and Reasoning (RuleML+RR 2018), the Reasoning Web Summer School (RW 2018), the 4th Global Conference on Artificial Intelligence (GCAI 2018), DecisionCAMP 2018, the MIREL workshop and the annual meeting of the Deduction Systems group (Deduktionstreffen 2018) of the German Gesellschaft für Informatik. It will take place at the Belval Campus of the University of Luxembourg (Luxembourg) on September 17–26, 2018. See the venue information for details.

With its special focus theme on **"methods and tools for responsible AI"**, a core objective of LuxLogAI is to present the latest developments and progress made on the crucial question of how to make AI more transparent, responsible and accountable.

Participating Members:

- Leon VAN DER TORRE (Chair)
- Amal TAWAKULI (Publicity Chair)
- Shohreh HADDADAN (Web Chair)
- Xavier PARENT (Organising Committee)
- Alexander STEEN (Organising Committee)
- Martin THEOBALD (Organising Committee)
- Emil WEYDERT (Tutorial Organizer)

Malicious Software and Hardware in Internet of Things (MaL-IoT ’18)

Location: Ischia, Italy, 8 May 2018.

Participating Members:

- Vincenzo IOVINO (Invited panelist)

MedRACER

https://sites.google.com/view/medracer/home

Location: Tempe, United States of America, 29 Oct 2018.

Description: Health care is a sensitive area due to the sheer amount and nature of the information used to manage patients. **Medical reasoning** is complex and involves multiple interactions among health conditions, treatments, and expectations from both health professionals and patients. Incomplete and contradictory information is ever present and decisions have to be made relying on it. As such, in order to support these professionals in their activities, it is necessary to accurately capture the constraints of medical reasoning in representations than can be used for supporting decisions, synthesizing medical evidence, discovering conflicts and inconsistencies, and so forth. Computational methods provide ways to analyse the available information and apply medical knowledge to it in order to evaluate the possible conclusions/claims, by considering reasons for and against them. They also allow to center the decisions on patients and their needs, as well as to take into account the preferences of various parties (patient, clinician, health center etc.). We aim to explore computational methods – including defeasible reasoning, computational argumentation, (various forms of) logic programming, ontological inference, machine-interpretable clinical pathways, decision support and recommendation systems, preference-based reasoning – for representation of, reasoning with, and resolving conflicts within, medical knowledge.

The aim of this workshop is to bring together researchers from the fields of (various) computational logics, argumentation, defeasible reasoning and reasoning within KR at large, who are interested in health care and would like to share their perspectives on applications of their research to the medical domain. This workshop is a venue for those researchers to share ways their theories and techniques can be used to support reasoning with medical knowledge, focusing especially on the resolution of conflicts in the context of incomplete information. Furthermore, the workshop intends to establish new collaborations to advance the latest computational models for supporting decision-making in health care.

Participating Members:

- Jérémie DAUPHIN (Program Committee Member)

RuleML+RR 2018

http://2018.ruleml-rr.org/

Location: Esch-sur-Alzette, Luxembourg, 18 Sep 2018 – 21 Sep 2018.

Description: The International Joint Conference on Rules and Reasoning (RuleML+RR), the leading event in rule-based reasoning, calls for high-quality papers covering theoretical advances, novel technologies, and innovative applications of knowledge representation and reasoning with rules. Stemming from the synergy between RuleML and RR events and building on the success of RuleML+RR 2017, one of the main goals of RuleML+RR 2018 is to create bridges between academia, industry, and government.

RuleML+RR 2018 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.

RuleML+RR 2018 will take place in Luxembourg on September 18th-21th 2018 and will be part of the Luxembourg Logic for AI Summit (LuxlogAI), ”Methods and Tools for Responsible AI”, bringing together RuleML+RR 2018, DecisionCAMP 2018, the 14th Reasoning Web Summer School (RW 2018), the 4th Global Conference on Artificial Intelligence (GCAI 2018) and the annual meeting of the Deduction Systems group (Deduktionstreffen 2018) of the German Gesellschaft für Informatik (GIe.V.).

Participating Members:

- Xavier PARENT (Chair)
- Livio ROBALDO (Program Committee Member)
- Leon VAN DER TORRE (Program Committee Member)
- Alexander STEEN (Short Papers, Posters, and Demo Co-Chair)

Second Chinese Conference on Logic and Argumentation (CLAR 2018)

http://www.xixilogic.org/events/clar2018/

Location: Hangzhou, China, 16 Jun 2018 – 17 Jun 2018.

Description: The interplay between logic and argumentation has a long history, from ancient Aristotle’s logic to very recent formal argumentation in AI. This is an interdisciplinary research field, involving researchers from, e.g., logic, philosophy, artificial intelligence, and law.

The goal of the CLAR 2018 conference is to highlight recent advances in the two fields of logic and argumentation, respectively, and to promote communication between researchers in logic and argumentation within and outside China.

CLAR 2018 takes place at Zhejiang University in Hangzhou, China, 16-17 June 2018. Proceedings will be published in Logic in Asia (Springer, Studia Logica Library).

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

Second International Workshop on Software Engineering Education for Millennials

https://seem2018.se-edu.org/

Location: Gothenburg, Sweden, 2 Jun 2018.

Participating Members:

- Nicolas GUELFI (Program Committee Member)

Self-Organising Systems in Art, Business and Science (SOS/ABS)

Location: Esch-sur-Alzette, Luxembourg, 19 Sep 2018.

Participating Members:

- Jean BOTEV (Co-Chair)

Service-Oriented Architectures and Programming Track at Symposium on Applied Computing (SOAP at SAC 2018)

http://sac-soap.sdu.dk/soap2018/

Location: Pau, France, 9 Apr 2018 – 13 Apr 2018.

Participating Members:

- Ross James HORNE (Program Committee Member)

SIGMOD Conference

Location: Chicago, United States of America, 14 May 2017 – 19 Jan 2018.

Participating Members:

http://sigmod2017.org

- Martin THEOBALD (Invited Speaker (Workshops))

Socio-Technical Aspects in Security and Trust

Location: San Juan, Puerto Rico, 4 Dec 2018.

Participating Members:

- Peter Y A RYAN (Program Committee Member)
- Gabriele LENZINI (General Chair)

Software Verification and Testing at Symposium on Applied Computing (SVT at SAC 2018)

http://sac-svt-2018.imag.fr/

Location: Pau, France, 9 Apr 2018 – 13 Apr 2018.

Participating Members:

- Jun PANG (Program Committee Member)

The 11th International Symposium on Foundations and Practice of Security (FPS 2018)

http://fps2018.encs.concordia.ca/

Location: Montreal, Canada, 13 Nov 2018 – 15 Nov 2018.

Participating Members:

- Jun PANG (Program Committee Member)

The 12th International Conference on Information Security Theory and Practice (WISTP 2018)

Location: Brussels, Belgium, 10 Dec 2018 – 11 Dec 2018.

Participating Members:

http://www.wistp.org/

- Sjouke MAUW (Program Committee Member)

The 12th International Conference on Trust Management (IFIPTM 2018)

https://sites.uoit.ca/ifiptm2018/

Location: Toronto, Canada, 9 Jul 2018 – 13 Jul 2018.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 12th International Symposium on Theoretical Aspects of Software Engineering (TASE 2018)

http://tase2018.jnu.edu.cn

Location: Guangzhou, China, 29 Aug 2018 – 31 Aug 2018.

Participating Members:

- Jun PANG (Program Committee Co-Chair)

The 14th International Conference on Information Security and Cryptology (Inscrypt 2018)

Location: Fuzhou, China, 14 Dec 2018 – 16 Dec 2018.

Participating Members:

- Vincenzo IOVINO (Program Committee Member)

The 14th International Conference on Signal Image Technology and Internet Based Systems (SITIS 2018)

Location: Las Palmas de Gran Canaria, Spain, 26 Nov 2018 – 29 Nov 2018.

Participating Members:

http://www.sitis-conf.org/

- Sjouke MAUW (Program Committee Member)

The 14th International Workshop on Security and Trust Management (STM 2018)

https://www.nics.uma.es/pub/stm18

Location: Barcelona, Spain, 6 Sep 2018 – 7 Sep 2018.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 15th IEEE International Conference on Advanced and Trusted Computing (ATC 2018)

http://www.smart-world.org/2018/atc/

Location: Guangzhou, China, 8 Oct 2018 – 12 Oct 2018.

Participating Members:

- Olga GADYATSKAYA (Program Committee Member)

The 16th Annual Conference on Privacy Security and Trust (PST 2018)

https://pstnet.ca/pst2018/

Location: Belfast, United Kingdom, 28 Aug 2018 – 30 Aug 2018.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 18th Privacy Enhancing Technologies Symposium

Location: Barcelona, Spain, 24 Jul 2018 – 27 Jul 2018.

Participating Members:

- Alfredo RIAL DURAN (Program Committee Member)

The 2018 International Workshop on Advances in Mobile App Analysis (A-Mobile 2018)

https://a-mobile.github.io/

Location: Montpellier, France, 4 Sep 2018.

Participating Members:

- Olga GADYATSKAYA (Program Committee Member)

The 20th International Conference on Formal Engineering Methods (ICFEM 2018)

http://www.formal-analysis.com/icfem/2018/

Location: Gold Coast, Australia, 12 Nov 2018 – 16 Nov 2018.

Participating Members:

- Jun PANG (Program Committee Member)

The 23rd European Symposium on Research in Computer Security (ESORICS 2018)

https://esorics2018.upc.edu/

Location: Barcelona, Spain, 3 Sep 2018 – 7 Sep 2018.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 23rd International Conference on Engineering of Complex Computer Systems (ICECCS 2018)

http://formal-analysis.com/iceccs/2018/

Location: Melbourne, Australia, 12 Dec 2018 – 14 Dec 2018.

Participating Members:

- Jun PANG (Program Committee Member)

The 23rd Symposium on Access Control Models and Technologies (SACMAT 2018)

http://www.sacmat.org/2018/index.php

Location: Indianapolis, United States of America, 13 Jun 2018 – 15 Jun 2018.

Participating Members:

- Jun PANG (Program Committee Member)

The 29th International Conference on Genome Informatics (GIW 2018) TCBB Track

http://datamining-web.it.uts.edu.au/giw2018/

Location: Kunming, China, 3 Dec 2018 – 5 Dec 2018.

Participating Members:

- Jun PANG (Program Committee Member)

The 31st Computer Security Foundations Symposium (CSF 2018)

https://www.cs.ox.ac.uk/conferences/csf2018/

Location: Oxford, United Kingdom, 9 Jul 2018 – 12 Jul 2018.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 3rd National Conference on Formal Methods and Applications (FMAC 2018)

http://fmac2018.ecnu.edu.cn/

Location: Chongqing, China, 3 Nov 2018 – 4 Nov 2018.

Participating Members:

- Jun PANG (Program Committee Co-Chair)

The 42nd IEEE Computer Society International Conference on Computers Software and Applications (COMPSAC 2018)

https://www.computer.org/web/compsac2018

Location: Tokyo, Japan, 23 Jul 2018 – 27 Jul 2018.

Participating Members:

- Jun PANG (Program Committee Member)

The 4th International Conference on Cloud Computing Technologies and Applications (CloudTech 2018)

http://www.cloudtechconference.org

Location: Brussels, Belgium, 26 Nov 2018 – 28 Nov 2018.

Participating Members:

- Grégoire DANOY (Program Committee Member)

The 4th Symposium on Dependable Software Engineering (SETTA 2018)

Location: Beijing, China, 4 Sep 2018 – 6 Sep 2018.

Participating Members:

- Jun PANG (Program Committee Member)

http://lcs.ios.ac.cn/setta2018/

The 4th Workshop on the Security of Industrial Control Systems and Cyber-Physical Systems

https://www.ds.unipi.gr/cybericps2018/

Location: Barcelona, Spain, 6 Sep 2018 – 7 Sep 2018.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 5th International Conference on Cryptography and Security Systems

https://fedcsis.org/2018/ccss

Location: Poznan, Poland, 9 Sep 2018 – 12 Sep 2018.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 5th International Workshop on Graphical Models for Security,(GraMSec 2018)

http://www.gramsec.uni.lu/

Location: Oxford, United Kingdom, 8 Jul 2018.

Participating Members:

- Olga GADYATSKAYA (Program Committee Member)
- Sjouke MAUW (Program Committee Member)

The 5th Workshop on CrossCloud Infrastructures and Platforms (CrossCloud 2018)

http://bit.ly/CrossCloud

Location: Porto, Portugal, 23 Apr 2018 – 26 Apr 2018.

Participating Members:

- Ross James HORNE (Program Committee Member)

The Seventh International Conference on Advances in Vehicular Systems, Technologies and Applications (VEHICULAR)

https://www.iaria.org/conferences2018/VEHICULAR18.html

Location: Venice, Italy, 24 Jun 2018 – 28 Jun 2018.

Participating Members:

- Ion TURCANU (Technical Program Committee Member)

The Sixth International Symposium on Security in Computing and Communications (SSCC 2018)

http://www.acn-conference.org/sscc2018/

Location: Bangalore, India, 19 Sep 2018 – 22 Sep 2018.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The UniGR Summer School on Verification Technology Systems and Applications (VTSA 2018)

http://resources.mpi-inf.mpg.de/departments/rg1/conferences/vtsa18/

Location: Nancy, France, 27 Aug 2018 – 31 Aug 2018.

Description: The 11th summer school on verification technology, systems and applications takes place at the Inria Center Nancy, France from August 27th to August 31tst, 2018. All three aspects verification technology, systems and applications strongly depend on each other and that progress in the area of formal analysis and verification can only be made if all three aspects are considered as a whole. Five speakers David Basin, Jean-Christophe Filliatre, Peter Lammich, Anca Muscholl and Carsten Sinz stand for this view in that they represent and will present a particular verification technology and its implementation in a system in order to successfully apply the approach to real world verification problems. There were about 30 participants for the summer school.

Participating Members:

- Jun PANG (Organizing Chair)

Twelfth International Workshop on Juris-informatics (JURISIN 2018)

http://research.nii.ac.jp/jurisin2018/

Location: Yokohama, Japan, 12 Nov 2018 – 13 Nov 2018.

Description: Juris-informatics is a new research area which studies legal issues from the perspective of informatics. The purpose of this workshop is to discuss both the fundamental and practical issues among people from the various backgrounds such as law, social science, information and intelligent technology, logic and philosophy, including the conventional ”AI and law” area. We solicit unpublished papers on theories, technologies and applications on juris-informatics.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

Twenty-sixth International Workshop on Security Protocols

Location: Cambridge, United Kingdom, 19 Mar 2018 – 21 Mar 2018.

Participating Members:

- Peter Y A RYAN (Program Committee Member)

VLDB

Location: Rio de Janeiro, Brazil, 27 Aug 2018 – 31 Jan 2019.

Participating Members:

- Martin THEOBALD (Paper presentation)

Voting’18

Location: Santa Barbara Beach Resort, Curaçao, 2 Mar 2018.

Participating Members:

- Peter Y A RYAN (Program Committee Member)
- Peter ROENNE (PC Member)

Workshop on 5G and Cooperative Autonomous Driving

https://icc2018.ieee-icc.org/workshop/5g-and-cooperative-autonomous-driving

Location: Kansas City, United States of America, 20 May 2018 – 24 May 2018.

Description: The recent progress on 5G ultra reliable and low latency communications is paving the way to applications in future autonomous vehicle communications and unlocking new uses cases for enhanced safe driving at high vehicle speeds, harsh driving conditions, and cooperative driving. A plethora of techniques and protocols in wireless connectivity, localization and navigation such as 802.11p, LTE-V, C-V2X, precise positioning, 3D High Definition (HD) maps, augmented reality, Fog computing, Advanced Driver Assistance Systems (ADAS), etc. are proposed or under development to respond to emerging road safety use cases for 5G communications in vehicular environments. In the path towards fully autonomous and safe coordinated driving, several requirements should be met, such as the availability of a sophisticated environment model for accurate driving decisions, full integration not only with smart road infrastructure but also with satellites and UAVs. Subsequently, it is crucial to investigate how and up to which point the 5G paradigm, as an enabler of evolved vehicular services, is able to meet the requirements of autonomous driving, accommodate the emergency of new roles and behaviors of connected vehicles and handle the heterogeneity of new applications in terms of data rates, latency and hyper-connectivity.

In the spirit of ICC, this workshop aims at favoring a multidisciplinary, cross-layer perspective to 5G and autonomous cooperative driving, bringing together researchers, developers, and practitioners from academia and industry.

Participating Members:

- Ion TURCANU (Technical Program Committee Member)

Workshop on Advances in Permutation-Based Cryptography 2018

http://permutationbasedcrypto.org/2018

Location: Milan, Italy, 10 Oct 2018.

Participating Members:

- Christof BEIERLE (Paper presentation)

Workshop on High Performance Computing facility management

https://wwwen.uni.lu/research/fstc/computer_science_and_communications_research_unit/news_and_events/workshop_on_high_performance_computing_facility_management

Location: Belval, Luxembourg, 11 Jun 2018 – 15 Jun 2018.

Description: This workshop is organised by the University of Luxembourg in collaboration with the National Science and Technology Development Agency (NSTDA) of Thailand. It brings together the team managing the High Performance Computing facilities of University of Luxembourg and experts from NSTDA Research Units - National Electronics and Computer Technology Center (NECTEC), National Center for Genetic Engineering and Biotechnology (BIOTEC), National Nanotechnology Center (NANOTEC) and the National Metal and Materials Technology Center (MTEC).

The workshop will cover HPC facility administration topics, from strategy and policy to operations management. The workshop's technical sessions are oriented towards facility management staff and will incorporate the user-oriented practical sessions of University of Luxembourg's summer HPC School.

Participating Members:

- Valentin PLUGARU (Co-Chair)

Workshop on Privacy in the Electronic Society (WPES)

Location: Toronto, Canada, 15 Oct 2018.

Participating Members:

- Alfredo RIAL DURAN (Program Committee Member)

Workshop on Research for Insider Threats (WRIT 2018)

https://www.ieee-security.org/TC/SPW2018/WRIT/

Location: San Francisco, United States of America, 24 May 2018.

Participating Members:

- Sjouke MAUW (Program Committee Member)

C.2 Doctoral Thesis Defense Committee Memberships

Kolawole John Adebayo, University of Bologna

Date: 27 Apr 2018
Location: Bologna, Italy

PhD Defense Jury Members:

- Leon VAN DER TORRE (Member)

Maxime Audinot, University of Rennes

Date: 17 Dec 2018
Location: Rennes, France

PhD Defense Jury Members:

- Sjouke MAUW (Member)

Alessia Calafiore, University of Turin

Date: 28 Sep 2018
Location: Turin, Italy

PhD Defense Jury Members:

- Livio ROBALDO (Member)
- Leon VAN DER TORRE (Member)

Thierry Derrmann, University of Luxembourg

Date: 7 Feb 2018
Location: Esch/Alzette, Luxembourg

PhD Defense Jury Members:

- Thomas ENGEL (Supervisor)

PhD Defense Jury External Partners:

- Falko Dressler (Vice-chairman)
- Marco Fiore (Member)

Thorsten Doherr, CREA

Date: 18 Jan 2018
Location: Luxemborug, Luxembourg

PhD Defense Jury Members:

- Christoph SCHOMMER (Vice-chairman)

Winfried Höhn, University of Luxembourg

Date: 17 Sep 2018
Location: Belval-Université, Luxembourg

PhD Defense Jury Members:

- Steffen ROTHKUGEL (Chairman)
- Christoph SCHOMMER (Supervisor)

PhD Defense Jury External Partners:

- Andreas Fickers (Member)
- Christof Schoech (Member)
- Karsten Tolle (External Expert)
- Alexander Wolff (Vice-chairman)

Matthieu Jimenez, University of Luxembourg

Date: 2 Oct 2018
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Pierre KELSEN (Chairman)
- Yves LE TRAON (Supervisor)
- Mike PAPADAKIS (Co-supervisor)

PhD Defense Jury External Partners:

- Xavier Blanc (Vice-chairman)
- Federica Sarro (Examiner)

Johannes Klein, University of Luxembourg

Date: 17 Jan 2018
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Denis ZAMPUNIERIS (Chairman)
- Steffen ROTHKUGEL (Supervisor)

PhD Defense Jury External Partners:

- Markus Esch (Member)
- Ingo Scholtes (Member)
- Peter Sturm (Vice-chairman)

Rajesh Kumar, University of Twente

Date: 17 Oct 2018
Location: Twente, Netherlands

PhD Defense Jury Members:

- Sjouke MAUW (Member)

Kevin Milner, University of Oxford

Date: 8 May 2018
Location: Oxford, United Kingdom

PhD Defense Jury Members:

- Sjouke MAUW (Member)

Dayana PIERINA BRUSTOLIN SPAGNUELO, University of Luxembourg

Date: 28 Nov 2018
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Paulo ESTEVES VERISSIMO (Chairman)
- Gabriele LENZINI (Vice-chairman)
- Peter Y A RYAN (Supervisor)

PhD Defense Jury External Partners:

- Simone Fischer-Hübner (Member)
- Jean Everson Martina (Member)

Salah Eddine SAIDI, Université Pierre et Marie Curie

Date: 18 Apr 2018
Location: Paris, France

PhD Defense Jury Members:

- Nicolas NAVET (Examiner)

Danilo Spano, University of Luxembourg

Date: 29 Jun 2018
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Gabriele LENZINI (Chairman)

PhD Defense Jury External Partners:

- Jens Krause (Member)
- Kai-Kit Wong (Member)

Jun Wang, University of Luxembourg

Date: 19 Oct 2018
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Sjouke MAUW (Chairman)
- Peter Y A RYAN (Supervisor)

PhD Defense Jury External Partners:

- Josep Domingo-Ferrer (Member)
- Catuscia Palamidessi (Member)

C.3 Awards

Award from the Office of Naval Research Global (ONRG – US Navy), 15 Aug 2018

Recipients: Pascal BOUVRY, Grégoire DANOY
PCOG's research on swarms of unmanned autonomous systems has been recognised by an award from the Office of Naval Research Global (ONRG – US Navy).

Best Paper Award at ICSSI 2018, 15 Nov 2018

Recipient: Qin MA
Paper entitled ”Enabling Value Co-Creation in Customer Journeys with VIVA”, co-authored with Iván S. Razo-Zapata, Eng K. Chew, Loïc Gammaitoni, and Henderik A. Proper, received the best paper award for the conference ICSSI 2018 (Joint International Conference of Service Science and Innovation and Serviceology).

Best paper award at IEEE ICOIN 2018, 10 Jan 2018

Recipients: Pascal BOUVRY, Abdallah Ali Zainelabden Abdallah IBRAHIM, Sébastien VARRETTE
Best paper award at the 32nd International Conference on Information Networking (ICOIN) for the article "*PRESENCE: Toward a Novel Approach for Performance Evaluation of Mobile Cloud SaaS Web Services*".

Best Paper Award at the 13th International Conference on Digital Information Management (ICDIM 2018), 26 Sep 2018

Recipients: Jean BOTEV, Christian GREVISSE, Steffen ROTHKUGEL
Title: Ontology Coverage Tool and Document Browser for Learning Material Exploration
Authors: C. Grévisse, J. Meder, J. Botev, S. Rothkugel

Best paper Award at the Embedded Real-Time Software and Systems conference (ERTS 2018), 31 Jan 2018

Recipient: Nicolas NAVET
L. Fejoz, B. Régnier, P. Miramont, N. Navet, "Simulation-Based Fault Injection as a Verification Oracle for the Engineering of Time-Triggered Ethernet networks", Proc. Embedded Real-Time Software and Systems (ERTS 2018), Toulouse, France, January 31-February 2, 2018. Best Paper Award. An experimental assessment of the dependability of the Ethernet networks used in space launchers.

Best Paper Award from 32nd IEEE International Conference on Information Networking (ICOIN) 2018, 11 Jan 2018

Recipients: Pascal BOUVRY, Abdallah Ali Zainelabden Abdallah IBRAHIM, Sébastien VARRETTE
Three researchers from Luxembourg University have been awarded during the 32nd IEEE International Conference on Information Networking (ICOIN) which took place on 11 January 2018 in Thailand. Abdallah Ibrahim, Dr. Sébastien Varrette and Prof. Pascal Bouvry have awarded the prestigious "Best Paper Award" for their paper entitled "PRESENCE: Toward a Novel Approach for Performance Evaluation of Mobile Cloud SaaS Web Services". The paper was selected from some 476 papers submitted to the conference and 196 selected to be presented during ICOIN's technical sessions.

ICOIN is an internationally renowned conference which gathers researchers and engineers from all over the world to discuss on recent advances in the areas of computer communication and networking technologies. On this occasion, Ph.D. student Abdallah Ibrahim, Research Associate Dr. Sébastien Varrette and Professor Pascal Bouvry from the Computer Science and Communications Research Unit (CSC) have presented an innovative tool "PRESENCE" to better evaluate Cloud Services Providers (CSPs).

Abdallah Ibrahim explains in details the research project:

Why did you develop such a tool?

"Cloud Services Providers (CSPs) deliver cloud services to cloud customers on a pay-per-use model. The quality of the provided services is defined using Service Level Agreements (SLAs). The recent developments in edge computing and the advent of mobile cloud computing platforms contribute to the success of this approach and the multiplication of offers. Unfortunately, despite the projections foreseeing a growing market for the coming years, there is no standard mechanism which exists to verify and assure that delivered services satisfy the signed SLA agreement. Accurate measures of the provided Quality of Service (QoS) is also missing most of the time."

What is "PRESENCE" about?

"We aim at offering an automatic framework named PRESENCE, to evaluate the QoS and SLA compliance of Web Services (WSs) offered across several CSPs. PRESENCE aims at quantifying in a fair and by stealth way the performance and scalability of the delivered WS. By stealthiness, we refer to the capacity of evaluating a given cloud service by orchestrating multiple workload patterns that make them indistinguishable from a regular user traffic from the provider point of view. PRESENCE defines a set of Common performance metrics handled by a set of agents within a customized client (called the Auditor) for measuring the behavior of cloud applications on top of a given CSP."

What does this award mean to you?

"This paper opens novel perspectives for assessing the SLA compliance of Cloud providers using the PRESENCE framework. This award is a unique achievement in my academic career. It pushes me, keeps me energized and charges me up to take more challenges in my career. The motivation to continue working on PRESENCE framework has increased because it was proven that we are on the right track. This award is the reward for the hard work we all put in together in our team. We will now continue to work with the PRESENCE framework to finalize the stealth model in testing CSPs' web services. Then, we will go further for testing real providers e.g. Amazon and Microsoft to validate our framework."

Note: ICOIN (http://icoin.org) is a prestigious conference sponsored by the IEEE Computer Society. It is one of the oldest forum for the presentation of technological advances and research results in the fields of theoretical, experimental, and industrial communications and information networks. ICOIN 2018 is the 32nd in the series that has been held annually since 1986. It brings together leading engineers and scientists in communication systems, cloud computing and networking from around the world. Research frontiers in fields ranging from grid computing to evolving cloud and edge (fog) computing are regularly advanced by results first reported in ICOIN technical sessions.

Best Paper Award, Siwen Guo et al., 16 Jan 2018

Recipient: Siwen GUO
Best Paper Award for the paper

PERSEUS: A Personalization Framework for Sentiment Categorisation with a Recurrent Network

by

- Siwen Guo, ILIAS Lab, University of Luxembourg
- Sviatlana Höhn, AI Minds Luxembourg
- Feiyu Xu, Head of AI, Lenovo Research, Beijing
- Christoph Schommer, ILIAS Lab, University of Luxembourg

at 10th ICAART 2018 - International Conference on Agents and Artificial Intelligence, Funchal, Madeira, Portugal

Best poster award at APBC'18, 15 Jan 2018

Recipients: Jun PANG, Qixia YUAN
The poster "ASSA-PBN: A software tool for large probabilistic Boolean networks" received the best poster award from the 16th Asia Pacific Bioinformatics Conference - APBC'18.

Best student paper award, 18 Jan 2018

Recipients: Siwen GUO, Sviatlana HOEHN, Christoph SCHOMMER, Feiyu Xu
Best student paper award at ICAART 2018

Junior-Fellowship of the German Gesellschaft für Informatik (GI), 1 Oct 2018

Recipient: Alexander STEEN

Herausragende Jungtalente verdienen es, besonders gefördert zu werden. Denn sie sind unsere Zukunft: nicht nur für Wissenschaft und Berufsfeld, sondern für unsere gesamte Gesellschaft.

2013 hat die Gesellschaft für Informatik e.V. (GI) deshalb das GI Junior-Fellowship begründet, um junge, engagierte Talente ideell wie finanziell zu unterstützen.

Von Wissenschaft bis Gesellschaftspolitik: Wir bieten unseren GI Junior-Fellows den Rahmen, eigenverantwortlich Ideen zu entwickeln, umzusetzen und die Informatik in Gesellschaft, Wissenschaft, Wirtschaft und Schule zu gestalten. Mit unserem Vorstand und Präsidium tauschen sie sich dabei engmaschig aus. So beeinflussen sie direkt die zukünftige Ausrichtung der größten deutschsprachigen IT-Fachgesellschaft. Außerdem bieten wir ihnen zahlreiche Gelegenheiten, sich zu vernetzen – mit renommierten IT-Köpfen aus aller Welt.

Level-2 distinguished PC-member at IJCAI-ECAI-2018, 13 Jul 2018

Recipient: Emil WEYDERT

NSU CRYPTO Olympiad, 27 Nov 2018

Recipient: Aleksei UDOVENKO
Aleksei Udovenko won the NSUCRYPTO Olympiad 2018 in the "Professional" section. NSUCRYPTO is a unique Cryptographic Olympiad containing scientific mathematical problems for professionals, school and university students from any country. Its aim is to involve young researchers in solving curious and tough scientific problems of modern cryptography. http://nsucrypto.nsu.ru/archive/2018/total_results/#data

C.4 Media Appearances

Cuxhavener Wissenschaftler ausgezeichnet (Cuxhavener Nachrichten)

https://www.cnv-medien.de/news/cuxhavener-wissenschaftler-ausgezeichnet.html

Article (Internet), 8 Dec 2018
Members: Alexander STEEN
BERLIN/CUXHAVEN. Mit dem Junior-Fellowship-Programm fördert die Gesellschaft für Informatik seit 2013 jedes Jahr herausragende Jungtalente, die sich um die Informatik in Wissenschaft und Gesellschaft in besonderem Maße verdient gemacht haben.

Kürzlich wurde in Berlin neben Prof. Dr. Andreas Vogelsang (TU Berlin) und Prof. Dr. Simon Nestler (HS Hamm-Lippstadt) auch Dr. Alexander Steen (FU Berlin) zum ”GI-Junior-Fellow” ernannt.

Dr. Alexander Steen (Jahrgang 1990) ist gebürtiger Cuxhavener und hat sein Abitur 2009 am Lichtenberg-Gymnasium gemacht. Nach dem Studium der Informatik und Mathematik promovierte Steen (Dr. rer. nat.) 2018 am Dahlem Center for Machine Learning and Robotics der Freien Universität Berlin. Jetzt arbeitet er an der Universität Luxemburg und entwickelt Methoden für die computergestützte Untersuchung von ethischen Modellen für intelligente autonome Systeme. 2016 wurde er zusammen mit weiteren Kollegen für eine interdisziplinäre Lehrveranstaltung ausgezeichnet, die auf innovative Art und Weise Computersysteme für die formale Analyse von Argumenten der Metaphysik nutzt. Als GI-Junior-Fellow möchte sich Alexander Steen verstärkt für die interdisziplinäre Verknüpfung der Informatik mit weiteren gesellschaftsrelevanten Anwendungsgebieten einsetzen. ”Mit den Junior-Fellowships wollen wir exzellente Informatikerinnen und Informatiker ermutigen, zukunftsweisende Ideen für die Gestaltung der Informatik in allen gesellschaftlichen Bereichen zu entwickeln und umzusetzen”, sagt Prof. Dr. Hannes Federrath, Präsident der Gesellschaft für Informatik.

”Aber auch wir als größte Fachgesellschaft für Informatik im deutschsprachigen Raum profitieren von den neuen Impulsen, welche die Junior-Fellows durch den engen Austausch mit Vorstand und Präsidium setzen. Ich freue mich auf die Zusammenarbeit mit den drei nun ernannten Junior-Fellows.” (dm/red)

Airport Security Market 2018| Worldwide Overview By Industry Size, Market Share, Future Trends, Growth Factors & Leading Players-Autoclear, C.E.I.A., FLIR, L3, OSI, Robert Bosch, Siemens, Westminster (ABNEWSWIRE)

Article (Internet), 29 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

http://www.abnewswire.com/pressreleases/airport-security-market-2018-worldwide-overview-by-industry-size-market-share-future-trends-growth-factors-leading-players-autoclear-ceia-flir-l3-osi-robert-bos

Airport Security Market 2018| Worldwide Overview By Industry Size, Market Share, Future Trends, Growth Factors & Leading Players-Autoclear, C.E.I.A., FLIR, L3, OSI, Robert Bosch, Siemens, Westminster (TheFreeNewsman.com)

http://ct.moreover.com/?a=37830729203&p=2bp&v=1&x=OKN7IXkfbdGiQJxmK0Kw_Q

Article (Internet), 29 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

Airport Security Market 2018| Worldwide Overview By Industry Size, Market Share, Future Trends, Growth Factors & Leading Players-Autoclear, C.E.I.A., FLIR, L3, OSI, Robert Bosch, Siemens, Westminster (Digital Journal)

http://www.digitaljournal.com/pr/4047558

Article (Internet), 29 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

Aida from LuxAI and the QT Robot (RTL)

https://today.rtl.lu/media/rtl-introduces/1267192.html

Interview (Internet), 28 Nov 2018
Members: Leon VAN DER TORRE
This week we meet Aida from LuxAI whose company is behind the QT robot which is having great results in helping children with autism. ©RTL/Crossfire 2018

”Smart” fliegen (Tageblatt)

Article (Newspaper), 19 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

In Luxemburg wurde das Reisen per Flugzeug der Zukunft getestet (Luxembourg Tageblatt)

http://www.tageblatt.lu/headlines/in-luxemburg-wurde-das-reisen-per-flugzeug-der-zukunft-getestet/?reduced=true

Article (Newspaper), 19 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

L’Uni et le Findel testent de nouveaux systèmes de sécurité (Luxemburger Wort)

https://www.wort.lu/fr/economie/l-uni-et-le-findel-testent-de-nouveaux-systemes-de-securite-5be3f8b8182b657ad3b99113

Article (Newspaper), 8 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

Un grand test mené au Findel (L’Essentiel)

Article (Internet), 7 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

Luxembourg Airport and University test new security system (Luxembourg Times)

https://luxtimes.lu/luxembourg/35529-luxembourg-airport-and-university-test-new-security-system

Article (Newspaper), 7 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

Contrôler les passagers selon leur comportement (L'Essentiel Online)

http://www.lessentiel.lu/fr/luxembourg/story/controler-les-passagers-selon-leur-comportement-23623315

Article (Internet), 7 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

Sicherheit geht vor (Luxemburger Wort)

Article (Newspaper), 7 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

Future of airport security field-tested in Luxembourg (TravelDailyNews)

https://www.traveldailynews.com/post/future-of-airport-security-field-tested-in-luxembourg

Article (Internet), 7 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

New security system trialed at Luxembourg Airport (Passenger Terminal Today.com)

https://www.passengerterminaltoday.com/news/security/new-security-system-trialed-at-luxembourg-airport.html

Article (Internet), 7 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

Die Uni Luxemburg und der Flughafen testen neues Sicherheitssystem (Luxemburger Wort)

https://www.wort.lu/de/business/die-uni-luxemburg-und-der-flughafen-testen-neues-sicherheitssystem-5be1d76b182b657ad3b98f17

Article (Newspaper), 6 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

Future of Airport Security Field-tested in Luxembourg (American Journal of Transporta on Online)

https://www.ajot.com/news/future-of-airport-security-field-tested-in-luxembourg

Article (Internet), 6 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

Luxemburg Airport plaatst passagiers in hokjes (Up in the Sky)

https://www.upinthesky.nl/2018/11/06/luxemburg-airport-plaatst-passagiers-in-hokjes/

Article (Internet), 6 Nov 2018
Members: Thomas ENGEL, Detlef FUEHRER, Aurel MACHALEK, David NAVEH

Pwned Trains On An Insecure Platform (Forbes Media LLC)

http://www.forbes.com/sites/simonrockman1/2018/10/02/pwned-trains-on-an-insecure-platform/

News (Internet), 2 Oct 2018
Members: Alexei BIRYUKOV
When the standards for GSM were written in the late 1980s the A5/1 encryption system, was watertight. To crack it would have needed a two terabyte look-up table, at a time when the most powerful public supercomputer only had one terabyte of storage. The security was considered so powerful it needed an export licence. Compared with the contemporary ETACS mobile system which could be eavesdropped with a scanner from your local electronics shop, GSM was unbreakable. Until 1999, when Alex Biryukov and Adi Shamir demonstrated the first verifiable breach of A5/1. That was only in lab conditions and not of immediate concern but the mobile world still upgraded to the more secure A5/3.

Künstliche Intelligenz: Sophia, Watson und der Hype (Tageblatt)

Article (Newspaper), 10 Sep 2018
Members: Sviatlana HOEHN, Leon VAN DER TORRE

http://www.tageblatt.lu/headlines/kuenstliche-intelligenz-sophia-watson-und-der-hype

Riding the Chatbot Train (Delano)

https://issuu.com/maisonmoderne/docs/delano_september_2018/12

Interview (Magazine), 10 Sep 2018 , p. 12
Members: Sviatlana HOEHN

Networked UAV Defense Swarms to Defend Against Malicious Drones (ACM TECHNEWS)

https://cacm.acm.org/news/230909-networked-uav-defense-swarms-to-defend-against-malicious-drones/fulltext

Article (Internet), 7 Sep 2018
Members: Pascal BOUVRY, Matthias R. BRUST, Grégoire DANOY

Die Maschinen nach menschlichem Vorbild (Tageblatt)

https://www.wort.lu/de/business/maschinen-nach-menschlichem-vorbild-5b890e35182b657ad3b9219e

Interview (Newspaper), 31 Aug 2018
Members: Christoph SCHOMMER

Networked UAV Defense Swarms to defend against malicious drones (TechXplore)

https://techxplore.com/news/2018-08-networked-uav-defense-swarms-defend.html

Article (Internet), 31 Aug 2018
Members: Pascal BOUVRY, Matthias R. BRUST, Grégoire DANOY

The War on ASIC Resistant Continues as Zcash Mining Study Underway (BitcoinExchangeGuide.com)

http://bitcoinexchangeguide.com/the-war-on-asic-resistant-continues-as-zcash-mining-study-underway/

News (Internet), 16 Jun 2018
Members: Alexei BIRYUKOV, Daniel FEHER
ASIC Miners Amount To 30% Of The Equihash Mining Hashrate, University of Luxembourg Study Finds.

Study Reveals ASIC Miners Represent 30% of the Equihash Mining Hashrate (Bitcoin.com)

http://news.bitcoin.com/study-reveals-asic-miners-represent-30-of-the-equihash-mining-hashrate/

News (Internet), 15 Jun 2018
Members: Alexei BIRYUKOV, Daniel FEHER

This week the Zcash Foundation and researchers from the University of Luxembourg have released a study that finds the presence of ASIC and FPGA miners may be controlling around 30 percent of the overall Equihash mining hashrate. The study speaks volumes to cryptocurrency developers and communities who have attempted to produce proof-of-work mechanisms that were meant to provide ASIC resistance.

La société doit être convertie aux sciences du digital (Le Quotidien)

http://www.lequotidien.lu/a-la-une/formation-aux-sciences-du-digital-on-est-meilleur-a-luni/

Interview (Newspaper), 23 Apr 2018
Members: Nicolas GUELFI

Pionier bei digitalem Studiengang (Le Journal)

Interview (Newspaper), 16 Apr 2018
Members: Nicolas GUELFI

https://www.journal.lu/top-navigation/article/pionier-bei-digitalem-studiengang/

Meetup ’Artificial Companions, Chatbots and Robots Luxembourg’ (Meetup)

https://www.meetup.com/Artificial-Companions-Chatbots-and-Robots-Luxembourg/

Blog (Internet), 1 Apr 2018
Members: Sviatlana HOEHN
Social network with local meetings

Outsourcing computational tasks. How can you trust the result? (science.lu)

https://www.science.lu/de/my-research-90-seconds/outsourcing-computational-tasks-how-can-you-trust-result

Article (Internet), 9 Feb 2018
Members: Balazs PEJO

Learning meaningful location embeddings from unlabeled visits (Sentiance Company Blog)

https://www.sentiance.com/2018/01/29/learning-meaningful-location-embeddings-from-unlabeled-visits/

Blog (Internet), 29 Jan 2018
Members: Jun PANG
The developers in the company apply the DeepCity deep learning framework (by Pang and Zhang, 2017)
to learn a representation of a location that embeds different types of meaningful information, and then
use these representations in venue mapping and other models.

Le Luxembourg veut son superordinateur (Wort)

https://www.wort.lu/fr/economie/la-richesse-par-la-donnee-le-luxembourg-veut-son-superordinateur-5a647113c1097cee25b7c2c0

Article (Newspaper), 21 Jan 2018
Members: Pascal BOUVRY, Sébastien VARRETTE

HPC: Luxembourg au cœur de la stratégie européenne (PaperJam)

http://paperjam.lu/news/hpc-luxembourg-au-coeur-de-la-strategie-europeenne

Article (Internet), 12 Jan 2018
Members: Pascal BOUVRY, Sébastien VARRETTE
La proposition de la Commission d'installer au Luxembourg le siège de la société qui gérera les futurs supercalculateurs européens, EuroHPC, est la concrétisation d'années d'efforts pour le chercheur Sébastien Varrette, l'un des pionniers du «high performance computing» (HPC) au Luxembourg.

C.5 Guest Researchers

The following guest researchers were invited to the CSC:

Prof. Florian Adamsky (Hochschule Hof)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

David Arroyo

Period: 10 Oct 2018 – 11 Oct 2018
Hosted by: Peter Y A RYAN

Stephanie Baldinucci (Banque de Luxembourg)

Period: 4 Dec 2018
Hosted by: Sviatlana HOEHN
Reason: Speaker at the meetup 'Bots for Banks' with the presentation 'Chatbots:

A strong companion for employees. Use case on how digital assistants can improve employees' work experience.'.

Sevdenur Baloglu (Middle East Technical University, Turkey)

Period: 30 Nov 2018
Hosted by: Jun PANG

Tiziano Bianchi

Period: 7 Feb 2018 – 8 Feb 2018
Hosted by: Peter Y A RYAN

Prof. Roland Bouffanais (Singapore University of Technology and Design (SUTD))

Period: 17 Sep 2018 – 21 Sep 2018
Hosted by: Pascal BOUVRY, Matthias R. BRUST

Torsten Braun (University of Bern)

Period: 12 Feb 2018 – 13 Feb 2018
Hosted by: Thomas ENGEL, Ridha SOUA
Reason: F2F Project Meeting

Dr. Walter Bronzi (BMW)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Achim D. Brucker (The University of Sheffield, the UK)

Period: 9 Aug 2018
Hosted by: Stanislav DASHEVSKYI, Sjouke MAUW

Dr Smadar Bustan (University of Paris Diderot)

Period: 19 Dec 2018
Hosted by: Christoph SCHOMMER

Dr. Martin Caminada (Cardiff University)

Period: 3 Sep 2018 – 4 Sep 2018
Hosted by: Leon VAN DER TORRE

Dr. Valentin Cassano (Universidad Nacional de Cordoba)

Period: 1 Jul 2018 – 10 Sep 2018
Hosted by: Leon VAN DER TORRE

Dr. German Castignani (Motion-S)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Ugo Chirico

Period: 6 Dec 2018 – 7 Dec 2018
Hosted by: Peter Y A RYAN

Dr. Ivan Cibrario Bertolotti (National Research Council of Italy)

Period: 3 Apr 2018 – 5 Apr 2018
Hosted by: Nicolas NAVET
Reason: Dr. Ivan Cibrario Bertolotti is a senior researcher from the National Research Council of Italy, with intensive research experience in real-time and networked embedded systems that are in line with the research focus of the CRTES group. This visit established the foundation of our collaboration in the direction of model-driven engineering for real-time embedded systems.

Richard Clayton

Period: 11 Apr 2018 – 12 Apr 2018
Hosted by: Peter Y A RYAN

Dr. Andrea Cohen (Universidad Nacional del Sur)

Period: 29 Jun 2018 – 30 Jul 2018
Hosted by: Leon VAN DER TORRE

Geoffroy Couteau

Period: 19 Jun 2018 – 20 Jun 2018
Hosted by: Peter Y A RYAN

Jerome De Cecco (Banque de Luxembourg)

Period: 4 Dec 2018
Hosted by: Sviatlana HOEHN
Reason: Presenter at the meetup ’Bots for Banks’ with the presentation Chatbots: A strong companion for employees. Use case on how digital assistants can improve employees’ work experience.

Dr. Thierry Derrmann (Talkwalker)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Dr. Riadh Dhaou (Institut National Polytechnique de Toulouse)

Period: 11 Jul 2018
Hosted by: Thomas ENGEL, Ridha SOUA
Reason: Dr. Riadh Dhaou gave a scientific talk on Adaptive Load Sharing and Load Control in Hybrid Terrestrial/Satellite Networks in the 5G Era.

Prof. Falko Dressler (University of Paderborn)

Period: 7 Feb 2018
Hosted by: Thomas ENGEL
Reason: Member of a PhD defense committee.

Dr. Elsa Estevez (Universidad Nacional del Sur)

Period: 1 Feb 2018 – 28 Feb 2018
Hosted by: Leon VAN DER TORRE

Dr. Sébastien Faye (Luxembourg Institute of Science and Technology)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Dr. Daniel Fischer (European Space Agency (ESA))

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Bryan Ford

Period: 5 Dec 2018 – 6 Dec 2018
Hosted by: Peter Y A RYAN

David Fuenmayor (Free University Berlin)

Period: 16 Apr 2018 – 20 Apr 2018
Hosted by: Leon VAN DER TORRE

Dr Hagen Fürstenau (Amazon Development Center)

Period: 20 Jun 2018
Hosted by: Christoph SCHOMMER
Reason: Distinguished lecture

Dr. Volker Fusenig (Siemens AG)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Prof. Dov Gabbay

Period: 7 Apr 2018 – 22 Apr 2018
Hosted by: Leon VAN DER TORRE

Prof. Dov Gabbay

Period: 5 Nov 2018 – 12 Nov 2018
Hosted by: Leon VAN DER TORRE

Prof. Mario Gerla (UCLA, University of Los Angeles)

Period: 24 Apr 2018
Hosted by: Thomas ENGEL
Reason: Supervision of a PhD student.

Ass. Prof. Alfredo Grieco (Politecnico di Bari Via Orabona)

Period: 24 Apr 2018
Hosted by: Thomas ENGEL
Reason: Supervision of a PhD student.

Michael Harrison (University of Cape Town)

Period: 27 Jul 2018 – 4 Aug 2018
Hosted by: Giovanni CASINI, Leon VAN DER TORRE

Prof. Dr. Mateja Jamnik (University of Cambridge)

Period: 6 Jun 2018
Hosted by: Christoph Ewald BENZMÜLLER, Christoph SCHOMMER
Reason: Distinguished lecture

Hugo Jonker (Open University, the Netherlands)

Period: 19 Jul 2018
Hosted by: Sjouke MAUW

Hugo Jonker (Open University, the Netherlands)

Period: 7 Nov 2018
Hosted by: Sjouke MAUW

Adam Kaliski (University of Cape Town)

Period: 27 Jul 2018 – 4 Aug 2018
Hosted by: Giovanni CASINI, Leon VAN DER TORRE

Vincent Kalmes (Banque de Luxembourg)

Period: 4 Dec 2018
Hosted by: Sviatlana HOEHN
Reason: Presenter at the meetup 'Bots for Banks' with the presentation 'Chatbots: A strong companion for employees. Use case on how digital assistants can improve employees' work experience'.

Eirini Kalogeinton (University of Bern)

Period: 12 Feb 2018 – 13 Feb 2018
Hosted by: Thomas ENGEL, Ridha SOUA
Reason: F2F Project Meeting

Liza Kayser (BMW)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Bernd Kiefer (DFKI GmbH, Saarbrücken)

Period: 14 Nov 2018
Hosted by: Sviatlana HOEHN
Reason: Meetup speaker 'A Virtual Companion to Support Children with Type 1 Diabetes'. See more at https://www.meetup.com/Artificial-Companions-Chatbots-and-Robots-Luxembourg/

Mirko Koscina

Period: 10 Jul 2018 – 11 Jul 2018
Hosted by: Peter Y A RYAN

Prof. Kittichai Lavangnananda (KMUTT University, Bangkok, Thailand)

Period: 13 Jun 2018 – 20 Jun 2018
Hosted by: Pascal BOUVRY

Dr. Francisco Lera (University of Leon)

Period: 28 Nov 2018 – 2 Dec 2018
Hosted by: Leon VAN DER TORRE

Cheng-Te Li (National Cheng Kung University, Taiwan)

Period: 19 Apr 2018
Hosted by: Jun PANG

Cheng-Te Li (National Cheng Kung University, Taiwan)

Period: 1 Oct 2018 – 12 Oct 2018
Hosted by: Jun PANG

Cheng-Te Li (National Cheng Kung University, Taiwan)
Period: 18 Sep 2018 – 21 Sep 2018
Hosted by: Jun PANG

Prof. Beishui Liao (Zhejiang University)
Period: 18 Feb 2018 – 15 Apr 2018
Hosted by: Leon VAN DER TORRE

Thomas Maitre (Vizir.co)
Period: 4 Dec 2018
Hosted by: Sviatlana HOEHN
Reason: Invites Speaker for the Meetup 'Bots for Banks' with the presentation 'Automating processes of the financial industry with chatbots (claim management & contract creation)'.

Gaetano Manzo (HES-SO)
Period: 12 Feb 2018 – 13 Feb 2018
Hosted by: Thomas ENGEL, Ridha SOUA
Reason: F2F project meeting

Karola Marky
Period: 27 Mar 2018 – 28 Mar 2018
Hosted by: Peter Y A RYAN

Dr. Maria Vanina Martinez (Universidad Nacional del Sur)
Period: 29 Jun 2018 – 30 Jul 2018
Hosted by: Leon VAN DER TORRE

Dr. Foued Melakessou (Luxembourg Institute of Science and Technology)
Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Sabrine Mellek (Ecole des Mines de Nancy, France)
Period: 27 Sep 2018
Hosted by: Yunior RAMIREZ CRUZ

Casius Morea (Emailtree)
Period: 24 Oct 2018
Hosted by: Sviatlana HOEHN
Reason: Invited speaker for the Meetup 'Email Management using Natural Language Processing and Machine Learning'

Frank Mousset

Period: 9 Oct 2018 – 10 Oct 2018
Hosted by: Peter Y A RYAN

Dr. Jedrzej Musial (TU Poznan, Poland)

Period: 29 Jun 2018 – 2 Sep 2018
Hosted by: Pascal BOUVRY

David Naccache

Period: 29 May 2018 – 30 May 2018
Hosted by: Peter Y A RYAN

Dr. Maria Rita Palattella (Luxembourg Institute of Science and Technology)

Period: 24 Apr 2018
Hosted by: Thomas ENGEL
Reason: Supervision of a PhD student.

Dr. Maria Rita Palattella (Luxembourg Institute of Science and Technology)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Prof. Andriy Panchenko (Brandenburg University of Technology)

Period: 7 Dec 2018
Hosted by: Thomas ENGEL
Reason: Supervision of a PhD student.

Prof. Andriy Panchenko (Brandenburg University of Technology)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Dr. Apivadee Piyatumrong (NECTEC, Thailand)

Period: 30 Sep 2018 – 15 Dec 2018
Hosted by: Pascal BOUVRY

Dr. Andrei Popleteev (Luxembourg Institute of Science and Technology)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting.

Dr. Thorsten Ries (Post Luxembourg)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Dr. Marco Riore (National Research Council of Italy)

Period: 7 Feb 2018
Hosted by: Thomas ENGEL
Reason: Member of a PhD defense committee.

Gianluca Rizzo (HES-SO)

Period: 12 Feb 2018 – 13 Feb 2018
Hosted by: Thomas ENGEL, Ridha SOUA
Reason: F2F Project Meeting

Prof. Stefanie Roos (TU Delft)

Period: 15 Oct 2018
Hosted by: Thomas ENGEL, Stefan SCHIFFNER
Reason: Prof. Stefanie Roos gave a scientific talk on Performance Improvements in Anonymous Communication Networks.

Dr. Thomas Scherer (Telindus)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Lara Schmid

Period: 13 Mar 2018 – 14 Mar 2018
Hosted by: Peter Y A RYAN

Alain Schumacher (SICAP, Luxembourg)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Mina Sheikhalishahi (CNR, Italy)

Period: 30 May 2018
Hosted by: Sjouke MAUW, Yunior RAMIREZ CRUZ

Dr. Carlo Simon (Research fellow, University of Luxembourg)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Boris Skoric

Period: 15 Mar 2018 – 16 Mar 2018
Hosted by: Peter Y A RYAN

Prof. Otto Spaniol (RWTH Aachen University)

Period: 22 Mar 2018
Hosted by: Thomas ENGEL, Andriy PANCHENKO
Reason: Supervision of a PhD student.

Dr. Eugen Staab (N4 Group)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Alexander Steen (Free University Berlin)

Period: 16 Apr 2018 – 20 Apr 2018
Hosted by: Leon VAN DER TORRE

Dr. Alexandru Tantar (Luxembourg Institute of Science and Technology)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Dr. Emilia Tantar (PWC, Luxembourg)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting

Daniel Thomas

Period: 25 Oct 2018 – 26 Oct 2018
Hosted by: Peter Y A RYAN

Prof. Fernando Tohme (Universidad Nacional del Sur)

Period: 30 Jun 2018 – 31 Jul 2018
Hosted by: Leon VAN DER TORRE

Jeroen van der Graaf

Period: 3 Jul 2018 – 4 Jul 2018
Hosted by: Peter Y A RYAN

Peerasak Wangsom (KMUTT University, Bangkok, Thailand)

Period: 15 Apr 2018 – 14 Jul 2018
Hosted by: Pascal BOUVRY

Yan Wu

Period: 1 Oct 2018 – 30 Sep 2018
Hosted by: Martin THEOBALD

Semen Yurkov (Rostelecom, Russia)

Period: 7 Sep 2018
Hosted by: Ross James HORNE, Sjouke MAUW

Yang Zhang (CISPA Helmholtz Center, Germany)

Period: 20 Sep 2018 – 21 Sep 2018
Hosted by: Jun PANG

Yury Zhauniarovich (Qatar Computing Research Institute, Qatar)

Period: 29 Jun 2018
Hosted by: Olga GADYATSKAYA

Prof. Andreas Zinnen (RheinMain University of Applied Sciences)

Period: 10 Dec 2018 – 11 Dec 2018
Hosted by: Thomas ENGEL
Reason: SECAN-Lab annual meeting.

C.6 Visits

The following visits by CSC members to external organisations took place:

Florian ADAMSKY

Institution: Honda R&D Europe
Location: Offenbach, Germany
Period: 5 Apr 2018.
Reason: Final presentation of the project Securing Smart Entry Systems.

Florian ADAMSKY

Institution: hack.lu 2018
Location: Luxembourg, Luxembourg
Period: 18 Oct 2018.
Reason: Dr. Florian Adamsky gave a talk on Serial-Killer: Security Analysis of Industrial Serial Device Servers.

Gergely BANA
Institution: Polish National Institute of Sciences
Location: Warsaw, Poland
Period: 27 Feb 2018 – 12 Mar 2018.
Reason: Visiting Wojtek Jamroga

Gergely BANA
Institution: Keio University
Location: Tokyo, Japan
Period: 1 Jun 2018 – 24 Jun 2018.
Reason: Visiting Mitsuhiro Okada

Jean BOTEV
Institution: Vrije Universiteit Brussel
Location: Brussels, Belgium
Period: 22 Jan 2018.

Jean BOTEV
Institution: Aston University
Location: Birmingham, United Kingdom
Period: 19 Apr 2018 – 20 Apr 2018.

Giovanni CASINI
Institution: University of Cape Town
Location: Cape Town, South Africa
Period: 23 Apr 2018 – 6 Jun 2018.

Jérémie DAUPHIN
Institution: National Institute of Informatics
Location: Tokyo, Japan
Period: 30 Apr 2018 – 22 Jun 2018.
Reason: I have met with Prof. Ken Satoh and we have continued a collaborative work started in 2017 on argumentative reasoning with a focus on explanatory capabilities of the systems to improve transparency and understandability of the outputs. This will make the tools based on these reasoning techniques more accessible and useful for lawyers who might not be familiar with the underlying technical details.

Augusto Wladimir DE LA CADENA RAMOS
Institution: Brandenburg University of Technology
Location: Cottbus, Germany
Period: 16 Oct 2018 – 19 Oct 2018.
Reason: Wladimir De La Cadena carried out a research visit to Prof. Dr. Andriy Panchenko at the Brandenburg University of Technology, where he evaluated the current results regarding multi-path onion routing-based approaches, and he discussed future publication activities.

Antonio DI MAIO

Institution: 5G-V2X Summer School at King's College
Location: London, United Kingdom
Period: 11 Jun 2018.
Reason: Antonio di Maio participated to the 5G-V2X Summer School at King's College held in London – UK on the 11th of June 2018: https://nms.kcl.ac.uk/toktam.mahmoodi/v2x-summer-school/index.htm

Antonio DI MAIO

Institution: IIOT - Industrial Internet of Things summer school at IMT Atlantique
Location: Saint Malo, France
Period: 4 Sep 2018 – 7 Sep 2018.
Reason: Antonio Di Maio participated to the IIOT - Industrial Internet of Things summer school at IMT Atlantique (September 4-7 in St. Malo - France): http://conferences.imt-atlantique.fr/iiot-summer-school/

Antonio DI MAIO

Institution: University of Bern
Location: Bern, Switzerland
Period: 18 Oct 2018 – 19 Oct 2018.

Thomas ENGEL

Institution: RWTH Aachen University
Location: Aachen, Germany
Period: 22 Nov 2018.
Reason: Member of a PhD defense committee.

Shohreh HADDADAN

Institution: I3S
Location: Sophia Antipolis, France
Period: 13 Nov 2018 – 17 Nov 2018.
Reason: During this visit, we discussed mainly the implementation of a Neural network based algorithm for the classification of argument components in the dataset of political debates. We also discussed the release of the dataset and the future planning for my research.

Sviatlana HOEHN

Institution: BTU Cottbus-Senftenberg
Location: Cottbus, Germany
Period: 5 Jul 2018 – 7 Jul 2018.
Reason: Kolloquium der Forschungsgruppe ›Kognitive Systeme‹ der BTU Cottbus-Senftenberg

Organisation: PD Dr. Dr. Peter Klimczak, Samuel Schilling, M.A., Prof. Dr. Christer Petersen

Sjouke MAUW

Institution: University of Oxford
Location: Oxford, United Kingdom
Period: 7 May 2018 – 9 May 2018.

Sjouke MAUW

Institution: University of Dundee
Location: Dundee, United Kingdom
Period: 1 Jul 2018 – 6 Jul 2018.

Sjouke MAUW

Institution: University of Rennes
Location: Rennes, France
Period: 18 Sep 2018 – 20 Sep 2018.

Sjouke MAUW

Institution: University of Twente
Location: Twente, Netherlands
Period: 16 Oct 2018 – 18 Oct 2018.

Sjouke MAUW

Institution: University of Rennes
Location: Rennes, France
Period: 15 Dec 2018 – 18 Dec 2018.

Asya MITSEVA

Institution: Brandenburg University of Technology
Location: Cottbus, Germany
Period: 14 Oct 2018 – 21 Oct 2018.
Reason: Asya Mitseva carried out a research visit to Prof. Dr. Andriy Panchenko at the Brandenburg University of Technology, where she discussed current research activities.

Asya MITSEVA

Institution: RWTH Aachen University
Location: Aachen, Germany
Period: 22 Nov 2018.
Reason: Annual PhD meeting with the CET commitee.

Jun PANG

Institution: Hosei University
Location: Tokyo, Japan
Period: 18 Jan 2018 – 19 Jan 2018.

Jun PANG

Institution: Nanyang Technological University
Location: Singapore, Singapore
Period: 5 Mar 2018 – 9 Mar 2018.

Jun PANG

Institution: East China Normal University
Location: Shanghai, China
Period: 9 Sep 2018 – 11 Sep 2018.

Jun PANG

Institution: Southwest University
Location: Chongqing, China
Period: 30 Oct 2018 – 5 Nov 2018.

Jun PANG

Institution: Teesside University
Location: Middlesbrough, United Kingdom
Period: 2 Dec 2018 – 4 Dec 2018.

Xavier PARENT

Institution: Stanford University
Location: Stanford, United States of America
Period: 10 Jul 2018 – 2 Aug 2018.

Valentin PLUGARU

Institution: HLRS - High Performance Computing Center Stuttgart
Location: Stuttgart, Germany
Period: 1 Oct 2018 – 2 Oct 2018.
Reason: European HPC User Forum meeting that will take place October 1-2, 2018 (midday to midday) at the High Performance Computing Center Stuttgart (HLRS).

The agenda will focus on HPC developments in Europe, including updates on quantum technologies, the European Processor Initiative and the Fortissimo Project for SMEs, along with perspectives from the Gauss Center for Supercomputing and the directors of Germany's national supercomputing centers.

Also featured will be new developments in HPC supported automotive design and AI in the automotive industry and urban environments.

Yunior RAMIREZ CRUZ

Institution: University of Milan
Location: Crema, Italy
Period: 25 Jun 2018 – 27 Jun 2018.

Livio ROBALDO
Institution: Nomotika SRL
Location: Turin, Italy
Period: 17 Jan 2018 – 31 Jan 2018.

Livio ROBALDO
Institution: Nomotika SRL
Location: Turin, Italy
Period: 28 Feb 2018 – 7 Mar 2018.

Livio ROBALDO
Institution: Nomotika SRL
Location: Turin, Italy
Period: 23 Mar 2018 – 3 Apr 2018.

Livio ROBALDO
Institution: Nomotika SRL
Location: Turin, Italy
Period: 20 Apr 2018 – 3 May 2018.

Livio ROBALDO
Institution: Nomotika SRL
Location: Turin, Italy
Period: 11 Jun 2018 – 13 Jun 2018.

Livio ROBALDO
Institution: Nomotika SRL
Location: Turin, Italy
Period: 26 Jun 2018 – 27 Jun 2018.

Livio ROBALDO
Institution: Nomotika SRL
Location: Turin, Italy
Period: 30 Jul 2018 – 1 Aug 2018.

Livio ROBALDO
Institution: Nomotika SRL
Location: Turin, Italy
Period: 22 Aug 2018 – 24 Aug 2018.

Livio ROBALDO
Institution: Nomotika SRL
Location: Turin, Italy
Period: 27 Sep 2018 – 29 Sep 2018.

Livio ROBALDO
Institution: Nomotika SRL
Location: Turin, Italy
Period: 18 Nov 2018 – 26 Nov 2018.

Livio ROBALDO
Institution: Nomotika SRL
Location: Turin, Italy
Period: 22 Dec 2018 – 24 Dec 2018.

Livio ROBALDO
Institution: Nomotika SRL
Location: Turin, Italy
Period: 27 Dec 2018 – 31 Dec 2018.

Christoph SCHOMMER
Institution: University of Potsdam
Location: Potsdam, Germany
Period: 9 Apr 2018 – 9 Jul 2018.

Christoph SCHOMMER
Institution: Freie University Berlin
Location: Berlin, Germany
Period: 15 May 2018 – 15 Jun 2018.

Christoph SCHOMMER
Institution: Freie University Berlin
Location: Berlin, Germany
Period: 19 Nov 2018 – 29 Nov 2018.

Zachary Daniel SMITH
Institution: Seoul National University
Location: Seoul, South Korea
Period: 2 Apr 2018 – 4 Apr 2018.

Ridha SOUA
Institution: Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services
Location: Esch/Alzette, Luxembourg
Period: 6 Jul 2018.

Ridha SOUA
Institution: University of Bern
Location: Bern, Switzerland
Period: 18 Oct 2018 – 19 Oct 2018.

Cui SU
Institution: Universite Paris-Saclay
Location: Paris, France
Period: 15 May 2018 – 16 May 2018.

Cui SU
Institution: Universite Paris-Saclay
Location: Paris, France
Period: 30 Sep 2018 – 6 Oct 2018.

Martin THEOBALD
Institution: Univerita Roma Tre
Location: Rome, Italy
Period: 12 Feb 2018 – 16 Feb 2018.
Reason: Invited guest lecture on "Big Data Analytics" for Master/PhD students.

Martin THEOBALD
Institution: University of Zurich
Location: Zurich, Switzerland
Period: 15 Nov 2018 – 16 Nov 2018.
Reason: PhD defense of Katerina Papaioannou (external reviewer).

Jorge Luis TORO POZO
Institution: CISPA Helmholtz Center
Location: Saarbruecken, Germany
Period: 9 Oct 2018 – 10 Oct 2018.

Jorge Luis TORO POZO
Institution: ETH
Location: Zurich, Switzerland
Period: 5 Nov 2018 – 7 Nov 2018.

Ion TURCANU

Institution: Honda R&D Europe
Location: Offenbach, Germany
Period: 5 Apr 2018.
Reason: HIGE 2018 project kick off meeting

Ion TURCANU

Institution: University of Bern
Location: Bern, Switzerland
Period: 18 Oct 2018 – 19 Oct 2018.

Leon VAN DER TORRE

Institution: University of Turin
Location: Turin, Italy
Period: 17 Jan 2018 – 31 Jan 2018.

Leon VAN DER TORRE

Institution: University of Cape Town
Location: Cape Town, South Africa
Period: 18 May 2018 – 27 Jun 2018.

Leon VAN DER TORRE

Institution: Stanford University
Location: Stanford, United States of America
Period: 10 Jul 2018 – 1 Aug 2018.

Leon VAN DER TORRE

Institution: University of Turin
Location: Turin, Italy
Period: 27 Sep 2018 – 29 Sep 2018.

Leon VAN DER TORRE

Institution: Cambridge University
Location: Cambridge, United Kingdom
Period: 9 Oct 2018 – 10 Oct 2018.

Leon VAN DER TORRE

Institution: Oxford University
Location: Oxford, United Kingdom
Period: 14 Oct 2018 – 17 Oct 2018.

Appendix D

Software

Accord

https://accord.uni.lux

License: Internal use only

Members: 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 and bug fixes have been applied to Accord in 2018. The most significant changes are:

- The rewriting of the database models that store ORBi^{lu} data, removing a dependency on a third-party module for the management of publications that did not fit our use case anymore.
- The implementation of a connection to the ACME database in preparation of future requirements regarding teaching KPI calculation.
- The implementation of a simple task management system that assists users with their data entry tasks.

ACVTool

https://github.com/pilgun/acvtool

License: APACHE License, Version 2.0

Members: Stanislav DASHEVSKYI (Designer), Olga GADYATSKAYA (Designer), Artsiom KUSHNIAROU (Developer, Tester), Aleksandr PILGUN (Architect, Developer)

Description: ACVTool is a tool designed to measure code coverage for an Android application without source code. The tool repackages an Android application, instruments bytecode and produce the code coverage report after the tests were applied. ACVTool was demonstrated at ACM CCS 2018, Toronto, Canada and released at https://github.com/pilgun/acvtool.

ADTool

http://satoss.uni.lu/software/adtool

License: free use

Members: Olga GADYATSKAYA (Designer), Sjouke MAUW (Analyst), Rolando TRUJILLO RASUA (Designer)

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 quantitative 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.

Changes: Stable version of ADTool is available at http://satoss.uni.lu/members/piotr/adtool/

The tool has been used in Master and Bachelor security courses.

The latest version of the tool allows to specify custom domains, i.e. define new bottom-up computation approaches in the tool itself.

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

AMT: Assessment Management Tool

License: to be defined

Members: Alfredo CAPOZUCCA (Analyst), Nicolas GUELFI (Analyst), Thibault Jean Angel SIMONETTO (Developer)

Description: AMT: Assessment Management Tool is a software to assess an observed element (e.g. course, student) according to an evaluation model. Each evaluation model uses one or multiple scale(s) to evaluate the observed element. The development of this tool was initiated in the context of a Bachelor in Informatics (BINFO)'s thesis and it's still under construction. Currently, there exists only a beta version available to internal members of the group.

Changes: AMT: after an initial archived prototype, a newer version is under development to improve the deployment process of the tool. Thus rather than improvements on the tool itself, currently the focus is on optimising the development, deployment and release of the tools.

ASSA-PBN

http://satoss.uni.lu/software/ASSA-PBN/

License: free use

Members: Jun PANG (Analyst), Soumya PAUL (Designer), Cui SU (Developer), Qixia YUAN (Developer)

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/.

Changes: The new version ASSA-PBN 3.0 has been accepted at the journal IEEE IEEE/ACM Transactions on Computational Biology and Bioinformatics (TCBB).

The latest update of the package, i.e., ASSA-PBN~3.0.0, is available from http://satoss.uni.lu/software/ASSA-PBN/. The new features of the latest release are listed at http://satoss.uni.lu/software/ASSA-PBN/#newfeature.

at-decorator

https://github.com/vilena/at-decorator/tree/master/CSP_decorator

License: GNU General Public License v3.0

Members: Olga GADYATSKAYA (Architect, Developer), Sjouke MAUW (Designer), Rolando TRUJILLO RASUA (Designer)

Description: **at-decorator** is a tool designed to compute values for an attack tree (fully decorate an attack tree) given some available data points and predicates on data values (relationships between attack tree node values). In contrast to the standard bottom-up approach, our tool does not require to have all leaf node values available to fully decorate a tree.

The tool is available as open source, and it utilizes Constraint Programming and the Z3 theorem prover. The tool is available here https://github.com/vilena/at-decorator/tree/master/CSP_decorator

BiCS Management Tool (BMT)

https://messir.uni.lu/bmt/login

License: to be defined

Members: Adriano FRANCI (Developer), Nicolas GUELFI (Analyst), Alen JAHIC (Developer), Stanislav KONCHENKO (Designer), Thibault Jean Angel SIMONETTO (Developer)

Description: Development of the BiCS Management Tool, a web application for managing the BiCS Semester Projects.

Changes: The development of the BiCS Management Tool has been continued. Several user needs have been taken into account and implement. Some new views and functionalities have been added for managing the user's projects. A big refactoring of the back-end has been performed to make the tool more maintainable. Additionally, there has been a conceptual change of the database. Due to the novel approach for evaluating BiCS Semester Projects, we defined new roles for the actors assigned to a BiCS Semester Projects. The conceptual change improves the management of the actors that are supposed to evaluate a given BiCS Semester project.

BiCS Website

License: to be defined

Members: Tiago Alexandre DE JESUS SOUSA (Developer), Charel FELTEN (Developer), Nicolas GUELFI (Analyst), Benjamin JAHIC (Analyst), Stanislav KONCHENKO (Architect), Albert KOPPELMAA (Developer), Gilles MAGALHAES (Developer), Benoit RIES (Analyst)

Description: The modern website should be a first entrance door for the new Bachelor. People from outside should get all information around the Bachelor and the projects done within the BiCSLab. One the one hand, our goal is to make the Bachelor visible to the World and attract people to enrol inside the Bachelor. On the other hand, we would like to make our projects visible to the outside, to attract industrial partners for proposing projects within the BiCS and the BiCSLab. Student's can work on these projects within their BiCS Semester Project course in cooperation with the industrial partners.

Changes: We have started the development of a novel website for the Bachelor in Computer Sciences (BiCS) and the BiCSLab. The website has currently not been deployed yet and is still under development.

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.

Crypren Decryptor

License: GPL-3.0

Members: Ziya Alper GENÇ (Developer)

DBVerify

http://satoss.uni.lu/software/DBVerify/

License: Open source

Members: Sjouke MAUW (Designer), Zachary Daniel SMITH (Developer), Jorge Luis TORO POZO (Developer), 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 verification methodology proposed in our paper "Distance-Bounding Protocols: Verification without Time and Location" (published at IEEE S&P'18). It was developed by Zach Smith (ZS) and Jorge Toro-Pozo (JT).

Changes: An updated version can be found at https://github.com/jorgetp/dbverify.

ELRA Language Corpus

License: LC/ELDA/DISTR-S/2014-11/001-UNILU

Members: Sviatlana HOEHN (Architect), 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:

1. Excalibur minor bugfixes for BINFO semester 4 students
2. Excalibur v1.9.0 packaged for Eclipse Photon
3. Archived in the long-term repository Zenodo under the following DOI
   - https://doi.org/10.5281/zenodo.1458158

Findel

https://github.com/cryptolu/findel

License: GPL-3.0

Members: Alexei BIRYUKOV (Designer), Dmitry KHOVRATOVICH (Designer), Sergei TIKHOMIROV (Developer)

Description: Findel (Financial Derivatives Language) is a domain-specific language that implements the composable approach to modeling financial derivatives on the Ethereum platform. For more information on Findel see paper ”Findel: Secure Derivative Contracts for Ethereum”.

IDP

http://icr.uni.lu/mcramer/index.php?id=3

License: Public

Members: 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.

MAPS

https://github.com/cryptolu/maps

License: GNU General Public License Version 3

Members: Yann LE CORRE (Developer)

Description: MAPS is a micro-architectural power simulator for Cortex-M3 microcontrollers capable to generate power consumption traces that can be used to mount a Differential Power Analysis (DPA) attack.

MiCS Management System

http://demos.uni.lux/mics

License: non-redistributable, for internal use only

Members: Christian FRANCK (Analyst, Architect), 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.

Changes: The MICS management system was rewritten in 2018. The new version was extensively redesigned, both from a data structure as well as from a user interface point of view. The new user interface is implemented as a web-component based web application that talks to the database backend through a REST-based API.

MinUS

License: free use

Members: Jun PANG (Analyst)

http://satoss.uni.lu/software/MinUS

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.

Model Decomposer

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.

Changes: Initial work was done on a new version of the model decomposer to support novel decomposition techniques.

NHC

https://github.com/minimap-xl/nhc

License: AGPL-3.0 license (Affero GPL)

Members: Tingting HU (Developer), Nicolas NAVET (Architect)

Description: NHC is an automated tool that can be used to augment models written in the CPAL Domain-Specific Language, with non-functional features such as dependability. Model-to-model transformation is achieved by first constructing an Abstract Syntax Tree corresponding to the initial model and then manipulating the AST tree to add non-functional features and last dump it back as CPAL source file.

Copyright (C) 2018 University of Luxembourg, National Research Council of Italy, and RealTime-at-Work.

Authors: Tingting Hu, Nicolas Navet, Ivan Cibrario Bertolotti, Loïc Fejoz, and Lionel Havet

ReCon

https://github.com/cryptolu/ReCon

License: GPL-3.0

Members: Alexei BIRYUKOV (Designer), Daniel FEHER (Developer), Dmitry KHOVRATOVICH (Designer)

Description: ReCon is a Universal Reputation Module for Distributed Consensus Protocols. This is the simulation of the protocol written in Python 2.7 based on the paper ”Guru: Universal Reputation Module for Distributed Consensus Protocols”.

Selene User Interface

License: Internal use only

Members: Marie-Laure ZOLLINGER (Developer)

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.

WFP toolbox

License: TBA

Members: 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.

Whitebox

https://github.com/cryptolu/whitebox

License: GNU General Public License Version 3

Members: Alexei BIRYUKOV (Designer), Aleksei UDOVENKO (Developer)

Description: This repository contains white-box analysis and implementation tools, in particular proof-of-concept code for the paper ”Attacks and Countermeasures for White-box Designs” by Alex Biryukov and Aleksei Udovenko (ASIACRYPT 2018).

The code is split into three parts:

1. Implementation: Proof-of-concept implementation of AES using the new nonlinear masking scheme.
2. Verification: Code for verifying algebraic security of gadgets.
3. Attacks: Several attacks from the paper.

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.

Yactul

License: N/A

Members: Steffen ROTHKUGEL (Architect)

Description: Yactul is a game-based student response framework for interactive education.

Changes: New iOS and Android apps.

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	68.99
Research Associate	32.53
Professor / Associate Professor	22.99
Student / Intern	17.71
Research Scientist	15.08
Postdoctoral Researcher	11.67
Scientific / Technical Support Staff	8.3
Administrative Staff	6.01
Program Coordinator	1
Project Coordinator	0.47
Total	*184.75*

Table E.1: Number of Staff by Category

E.2 Distribution of Staff by Category

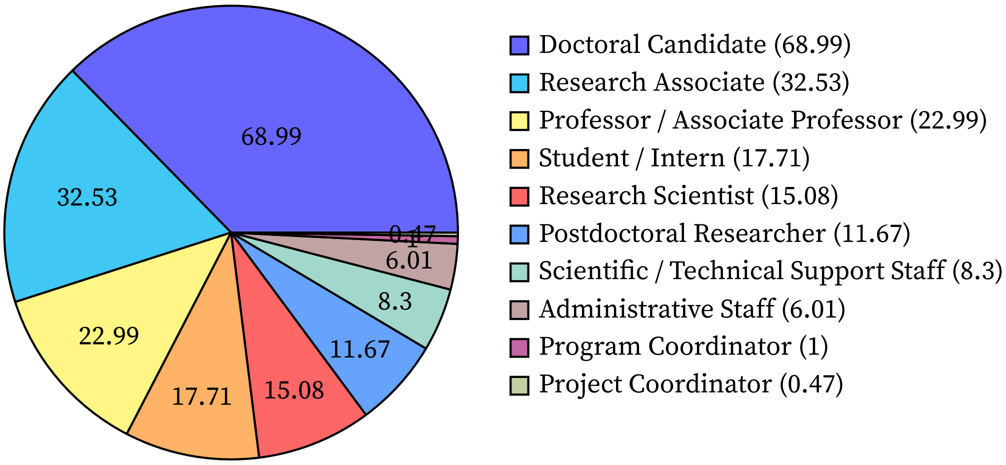


Figure E.1: Staff Distribution

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.

Category	Last Name	First Name
Professor / Associate Professor	BIRYUKOV	Alexei
	BOUVRY	Pascal
	BRIAND	Lionel
	CORON	Jean-Sébastien
	ENGEL	Thomas
	ESTEVES VERISSIMO	Paulo
	GUELFI	Nicolas
	KELSEN	Pierre
	LE TRAON	Yves
	LEPREVOST	Franck
	MAUW	Sjouke
	MÜLLER	Volker
	NAVET	Nicolas
	OTTERSTEN	Björn
	ROTHKUGEL	Steffen
	RYAN	Peter Y A
	SACHAU	Juergen
	SCHOMMER	Christoph
	SORGER	Ulrich

Category	Last Name	First Name
	STEENIS	Bernard
	THEOBALD	Martin
	VAN DER TORRE	Leon
	ZAMPUNIERIS	Denis
Postdoctoral Researcher	BLEUSE	Raphaël
	CASINI	Giovanni (0.5 FTE)
	COGLIATI	Benoît-Michel
	ELLAMPALLIL VENUGOPAL	Vinu (0.8 FTE)
	GROSZSCHÄDL	Johann
	HOEHN	Sviatlana (0.96 FTE)
	HORNE	Ross James (0.33 FTE)
	HU	Tingting
	MARKOVICH	Réka (0.33 FTE)
	OSVIK	Dag Arne (0.8 FTE)
	PARENT	Xavier
	PAUL	Soumya (0.46 FTE)
	RIAL DURAN	Alfredo (0.84 FTE)
	RODRIGUEZ LERA	Francisco Javier (0.75 FTE)
	SIRAJZADE	Joshgun (0.48 FTE)
	STEEN	Alexander (0.42 FTE)
Research Scientist	BERNARD	Nicolas
	BISSYANDE	Tegawendé François d Assise
	BOTEV	Jean
	CAPOZUCCA	Alfredo
	DANOY	Grégoire
	FRANCK	Christian
	KLEIN	Jacques
	LENZINI	Gabriele
	MA	Qin (0.5 FTE)
	PANCHENKO	Andriy (0.58 FTE)
	PANG	Jun
	PAPADAKIS	Mike
	RIES	Benoit
	VARRETTE	Sébastien
	VOLP	Marcus
	WEYDERT	Emil
Research Associate	ADAMSKY	Florian (0.83 FTE)
	ALEKSANDROVA	Marharyta
	ALLIX	Kevin (0.55 FTE)
	BANA	Gergely
	BARTEL	Alexandre
	BEIERLE	Christof (0.59 FTE)

Category	Last Name	First Name
	BENZMÜLLER	Christoph Ewald (0.49 FTE)
	BHAUMIK	Ritam (0.42 FTE)
	BOYTSOV	Andrey
	BRUST	Matthias R.
	CASINI	Giovanni (0.49 FTE)
	CRAMER	Marcos (0.58 FTE)
	DASHEVSKYI	Stanislav
	DECOUCHANT	Jérémie
	DELERUE ARRIAGA	Afonso (0.04 FTE)
	FUEHRER	Detlef (0.58 FTE)
	GADYATSKAYA	Olga
	HARTMANN	Thomas (0.58 FTE)
	IOVINO	Vincenzo
	KAISER	Daniel (0.75 FTE)
	KHOVRATOVICH	Dmitry (0.01 FTE)
	KIM	Dongsun (0.87 FTE)
	KINTIS	Marinos
	KOZHAYA	David (0.16 FTE)
	KUSHNIAROU	Artsiom (0.45 FTE)
	LI	Daoyuan (0.21 FTE)
	LI	Li (0.12 FTE)
	LIU	Zhe (0.43 FTE)
	MESTEL	David (0.29 FTE)
	MSADEK	Mohamed Nizar
	NAVEH	David (0.25 FTE)
	OSTREV	Dimiter
	PAUL	Soumya (0.53 FTE)
	RAHLI	Vincent
	RAMIREZ CRUZ	Yunior
	RIAL DURAN	Alfredo (0.16 FTE)
	ROBALDO	Livio
	ROBERT	Jérémy
	ROENNE	Peter
	ROSALIE	Martin (0.58 FTE)
	SCHIFFNER	Stefan
	SKROBOT	Marjan (0.04 FTE)
	SOUA	Ridha
	SYMEONIDIS	Iraklis (0.33 FTE)
	TRUJILLO RASUA	Rolando (0.12 FTE)
	TURCANU	Ion (0.99 FTE)
	WANG	Jun (0.16 FTE)
	WANG	Qingju (0.96 FTE)
	YU	Jiangshan (0.66 FTE)
	YUAN	Qixia (0.33 FTE)
Program Coordinator	LADID	Latif
Project Coordinator	OCHSENBEIN	Anne (0.19 FTE)

Category	Last Name	First Name
	OESTLUND	Stefanie (0.25 FTE)
	VIAU-COURVILLE	Mathieu (0.03 FTE)
Scientific / Technical Support Staff	BRANT	Florence (0.21 FTE)
	CARTIAUX	Hyacinthe (0.55 FTE)
	CHARPIOT	Louise (0.14 FTE)
	EDDS	Liam (0.04 FTE)
	GIOTTI	Domenico (0.16 FTE)
	GLODT	Christian
	KONCHENKO	Stanislav (0.25 FTE)
	LE CORRE	Yann (0.91 FTE)
	MACHALEK	Aurel
	PARISOT	Clément
	PLUGARU	Valentin
	REIS	Sandro
	STEMPER	André
	WASIM	Muhammad Umer (0.04 FTE)
Doctoral Candidate	ANTONIADIS	Nikolaos
	ATASHPENDAR	Arash
	BARTHEL	Jim Jean-Pierre (0.29 FTE)
	BENEDICK	Paul-Lou
	BHADAURIA	Anshuman Singh
	CAO	Tong (0.91 FTE)
	CAPPONI	Andrea
	CARDOSO DOS SANTOS	Luan (0.5 FTE)
	CHANGAIVAL	Boonyarit
	CHARPIOT	Louise (0.71 FTE)
	DAMODARAN	Aditya Shyam Shankar (0.33 FTE)
	DAUPHIN	Jérémie
	DE LA CADENA RAMOS	Augusto Wladimir
	DI MAIO	Antonio
	EL ORCHE	Fatima Ezzahra (0.33 FTE)
	ESMAEILZADEH DILMAGHANI	Saharnaz (0.84 FTE)
	FARJAMI	Ali
	FEHER	Daniel
	FERNANDES	Maria
	FISCARELLI	Antonio Maria
	FU	Shange (0.13 FTE)
	GAO	Jun
	GENÇ	Ziya Alper

Category	Last Name	First Name
	GREVISSE	Christian
	GUO	Siwen
	HADDADAN	Shohreh
	HURIER	Médéric
	HÖHN	Winfried (0.4 FTE)
	IBRAHIM	Abdallah Ali Zainelabden Abdallah
	JAFARNEJAD	Sasan
	JAHIC	Benjamin (0.96 FTE)
	JIMENEZ	Matthieu (0.79 FTE)
	KAMLOVSKAYA	Ekaterina
	KIEFFER	Emmanuel
	KIM	Kisub
	KLEIN	Johannes (0.08 FTE)
	KOLBE	Niklas
	KONG	Pingfan
	LAMBERT	Christoph
	LAMHAR	Salima (0.83 FTE)
	LI	Daoyuan (0.04 FTE)
	LIU	Chao
	LIU	Kui
	LOPEZ BECERRA	Jose Miguel
	MA	Wei (0.08 FTE)
	MAI	TIEU LONG (0.42 FTE)
	MEDER	Paul Joseph Yves (0.16 FTE)
	MIRTO	Cristian (0.75 FTE)
	MITSEVA	Asya
	MOULINE	Ludovic
	NEYENS	Gilles
	NOTARNICOLA	Luca
	PARRY	Gowher
	PEJO	Balazs
	PEREIRA	Vitor
	PIERINA BRUSTOLIN SPAGNUELO	Dayana (0.91 FTE)
	PILGUN	Aleksandr
	PINTO GOUVEIA	Ines (0.88 FTE)
	RIDA	Ahmad (0.29 FTE)
	RIOM	Timothée (0.5 FTE)
	ROSSI	Arianna (0.25 FTE)
	RWEMALIKA	Renaud
	SALA	Petra
	SAMIR LABIB	Nader
	SANCHEZ GUINEA	Alejandro (0.66 FTE)
	SMITH	Zachary Daniel
	SOROUSH	Najmeh
	STOJKOVSKI	Borce

Category	Last Name	First Name
	SU	Cui
	SUNDHARAM	Sakthivel Manikandan (0.75 FTE)
	TAWAKULI	Amal
	TIKHOMIROV	Sergei
	TITCHEU CHEKAM	Thierry
	TORCHYAN	Khachatur
	TORO POZO	Jorge Luis
	UDOVENKO	Aleksei
	VAN WIER	Jeroen (0.08 FTE)
	VAZQUEZ SANDOVAL	Itzel
	VITTO	Giuseppe (0.29 FTE)
	VUKOTIC	Ivana
	WANG	Jun (0.83 FTE)
	WASIM	Muhammad Umer (0.32 FTE)
	YUAN	Qixia (0.04 FTE)
	ZHONG	Zhiqiang (0.71 FTE)
	ZOLLINGER	Marie-Laure
Administrative Staff	BRANT	Florence (0.41 FTE)
	CARTIAUX	Hyacinthe (0.45 FTE)
	EDWARDSDOTTIR FINNSSON	Helga Fanney
	FLAMMANG	Danièle (0.75 FTE)
	OCHSENBEIN	Anne (0.63 FTE)
	OESTLUND	Stefanie (0.44 FTE)
	SCHMITZ	Fabienne
	SCHROEDER	Isabelle (0.5 FTE)
	VIAU-COURVILLE	Mathieu (0.32 FTE)
	WOLTERS	Nicola (0.5 FTE)
Student / Intern	ABDOELLAH MOHAMMED	Abdalla Adam (0.33 FTE)
	ATASHPENDAR	Aryobarzan (0.68 FTE)
	BAUDIN	Alexis (0.21 FTE)
	BERNARDO	Lutiano Gabriel (0.07 FTE)
	CHENG	Hao (0.32 FTE)
	CHRISNACH	Maurice (0.33 FTE)
	DE JESUS SOUSA	Tiago Alexandre (0.09 FTE)
	DEMARCHE	Eric (0.83 FTE)
	FELTEN	Charel (0.13 FTE)
	FILTER	Julian (0.25 FTE)
	FRANCI	Adriano (0.18 FTE)
	GIFFRA	Alessandro (0.16 FTE)
	HAGEN	Ciaran (0.51 FTE)

Category	Last Name	First Name
	HALE	Miriam-Linnea (0.32 FTE)
	HAWLADER	Faisal (0.08 FTE)
	HENTGES	Laurent Philippe (0.37 FTE)
	IBRAHIM	Chris (0.36 FTE)
	IONESCU	Andrei-Sabin (0.74 FTE)
	JACOBS	Kwinten (0.14 FTE)
	JAHIC	Alen (0.25 FTE)
	JAYAKUMAR	Raji (0.5 FTE)
	KEPUSKA	Ema (0.5 FTE)
	KONCHENKO	Stanislav (0.54 FTE)
	KOPPELMAA	Albert (0.05 FTE)
	KREMER	Michel (0.02 FTE)
	KRYVCHENKO	Roman (0.37 FTE)
	LENOU-TAGO	Cyrille (0.08 FTE)
	MAGALHAES	Gilles (0.1 FTE)
	MARQUEZ SANCHEZ	ANA PATRICIA (0.77 FTE)
	MAYER	Joe (0.2 FTE)
	MEDER	Jeff Alphonse Antoine (0.5 FTE)
	MEHDI	Syed Baqar Bilal (0.65 FTE)
	NASIB	Sadi (0.43 FTE)
	OLSZEWSKI	Maya Alexandra (0.46 FTE)
	OUHSSAIN	Hamza (0.72 FTE)
	PEREIRA GONÇALVES	Mike (0.2 FTE)
	POGOSIAN	Davit (0.2 FTE)
	RAMAKRISHNA	Soumya (0.27 FTE)
	REBONATO ENDRINGER	DIONI (0.46 FTE)
	RETUNSKAIA	Tatiana (0.24 FTE)
	RINALDI	Giulia (0.5 FTE)
	SAGLIK	TOLGA (0.45 FTE)
	SAUVAGE	Thomas (0.36 FTE)
	SCHWEICH	Tonie (0.68 FTE)
	SIMONETTO	Thibault Jean Angel (0.6 FTE)
	TEMPERONI	Alessandro (0.29 FTE)
	TOMASONI	Mattia (0.08 FTE)
	VIJAYAKUMAR	Bharathi (0.17 FTE)
	VITELLO	Piergiorgio (0.12 FTE)
	WILSON	Marc (0.35 FTE)
	XU	Teng Andrea (0.5 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