CSC | Computer Science and Communications

UNIVERSITY OF LUXEMBOURG

FACULTY OF SCIENCE, TECHNOLOGY AND COMMUNICATION

Computer Science and Communications

Activity Report 2019

CSC | Computer Science and Communications

Computer Science and Communications

Activity Report 2019

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

Computer Science and Communications
Activity Report 2019

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:

Isabelle Glemot-Schroeder, Andrea Puech and Fabienne Schmitz
Email: dcs@uni.lu

Editor:	Christian Glodt
Release date:	04-06-2020
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 Department of Computer Science in 2019, including our research projects, teaching programs, organized events, awarded papers, visiting researchers and publications.

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

Best regards,

Sjouke Mauw
Leon van der Torre

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 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 183 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. CSC is responsible for two bachelor programs, three master programs, a doctoral program, and a certificate Smart ICT for business innovation.

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

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

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

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

Head

- Sjouke Mauw, professor, head of CSC

Vice head

- Leon van der Torre, professor, 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, 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
- Ulrich Sorger, professor
- Bernard Steenis, associate professor
- Martin Theobald, professor, head of ILIAS
- Leon van der Torre, professor, vice head of CSC
- 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 2019 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 2019 annual report for information regarding the activities and contributions of professors Briand and Ottersten and their respective groups.

Chapter 3

Research Areas

History

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

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

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

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

Research Program

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

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

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

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

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

Detailed Research Program

Communicative Systems

The Communicative Systems Laboratory (ComSys) performs state of the art research in digital communications. The rapidly growing demand for information exchange in people's daily lives requires technologies like ubiquitous and pervasive computing to meet the expectations of the information society and novel adaptive concepts tackling the continuing data challenges. Embracing the end-to-end arguments in system design, ComSys focuses on integrated research in the areas of Information Transfer and Communicating Systems. Information Transfer is concerned with information transmission over potentially complex channels and networks. Communicating Systems in turn are the composition of multiple distributed entities employing communication networks to collaboratively achieve a common goal. ComSys has strong technical and personal facilities to improve existing and develop new solutions in the following research topics:

- Secure communication protocols
- Network and systems security, 5G and beyond, IoT
- Collaborative socio-technical systems

- Virtual and augmented reality
- Vehicular communication (V2X, in car, C-ITS)
- Reliable distributed energy-systems
- Buffered PV Integration in Utility Grids
- Distributed anonymity and privacy
- Machine learning and adaptive networking
- Network science

ComSys consists of the following collaborating groups and labs performing research in complementary fields: the Collaborative and Socio-Technical Systems (COaST) group, the Digital Power Systems and Control Engineering (DPSCE) group, and the Security and Networking (SECAN) lab.

COaST focuses on distributed collaborative systems, complex networks and self-organisation, socio-technical modelling, educational technologies and mediated reality. The group operates the VR/AR Lab at the Department of Computer Science.

DPSCE 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.

SECAN-Lab conducts 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.

Intelligent and Adaptive Systems

The *Intelligent and Adaptive Systems Research Group* (ILIAS; see ilias.uni.lu) is home to 5 Professors, 5 Guest Professors, 13 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 coevolve 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. We are in contact to the *Luxembourgish Ethics Council* concerning the questions to *Artificial Intelligence and Ethics*.

Algorithmics, Cryptology and Security

The 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.

Advanced Software and Systems

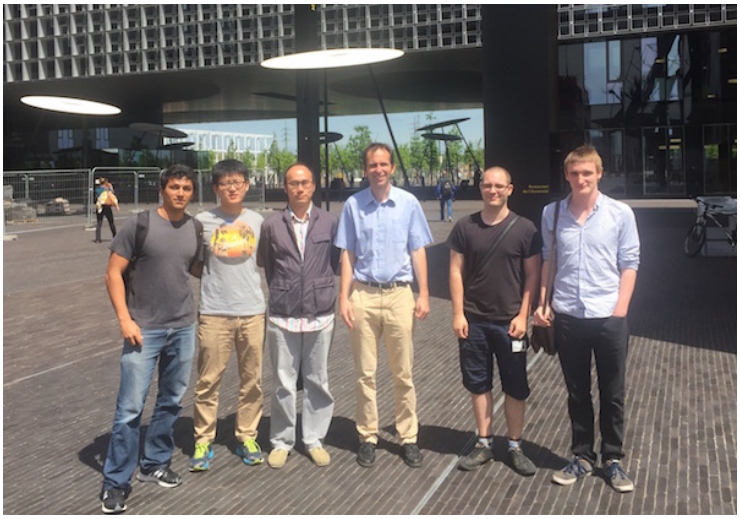
Our research on Advanced Software and Systems (LASSY) can be structured into five partly overlapping dimensions: modelling, methodology, computing paradigms, dependability (including security) and main application domains.

- Modelling: we investigate the foundations of model-driven engineering (MDE) as well as applications of MDE in fields as diverse as mobile computing, internet of things and the automotive sector, to name just a few.
- Methodology: a new integrated approach has been developed supported by an open-source tool that integrates theories, methods and tools from several software engineering subdisciplines such as requirements, testing and maintenance.
- Computing paradigms: the topic of pro-active computing, which is based on anticipating the user's needs, is investigated.
- Dependability: several research topics deal with dependability. In particular, innovative software testing and debugging techniques are studied. Another research topic within this dimension is the study of software intensive real-time systems, trying to improve their safety and lower their development costs. This line of investigation is supported by analytic and simulation models as well as by software engineering concepts such as domain-specific languages and system synthesis. Finally, mobile security and reliability are studied using static code analysis and machine learning techniques.
- Application domains: examples are automotive and aerospace embedded systems, enterprise architectures, cyberphysical systems, e-learning and pervasive healthcare systems.

Chapter 4

Research Groups

4.1 Applied Crypto Group (ACG)



Head of research group: Jean-Sébastien 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 2019

- FNR INTER-ANR project SWITECH has been accepted (519.000 EUR).

Three most interesting publications (or other achievements) in 2019

- Jean-Sébastien Coron, Hilder V. L. Pereira: On Kilian's Randomization of Multilinear Map Encodings. ASIACRYPT (2) 2019: 325-355
  We describe a key-exchange protocol between N parties, non-interactively.
- Jean-Sébastien Coron, Luca Notarnicola: Cryptanalysis of CLT13 Multilinear Maps with Independent Slots. ASIACRYPT (2) 2019: 356-385
  We describe an attack against the CLT multilinear map scheme

4.2 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 primitives 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 2019

2019 was a fruitful year for APSIA: 1 new CORE proposal was awarded. The group grew to close to 30 members. Three members successfully defended their PhD theses. Overall, the group published over 30 papers, many in highly prestigious conferences such as Crypto. Arguably, the highlight of the year was the group's hosting of ESORICS, the premiere European conference on computer security. The 2019 edition of ESORICS was the most successful in the conference's history, both in terms of number and quality of submissions and attendance. This was chaired by Prof. Ryan with the support of Dr. Roenne as Local-Chair. The Verifiable Voting Workshop in association with Financial Crypto, founded by Ryan in 2016, had its fourth, successful edition in Curacao. We have a number of international projects with Poland, Belgium, UK and France, mainly around secure voting systems. We established the APSIA Quantum Lab that now has eight members working on quantum and post-quantum information assurance.

APSIA also hosted the visit of Prof Jintai Ding from the University of Cincinnati, to work with members of the Quantum Lab on quantum-safe crypto, in particular the design and analysis of a quantum-safe version of the J-PAKE protocol (Hao and Ryan 2008).

We have filed a European patent, by Peter Ryan and Bill Roscoe (Oxford University), called Secure Fair Exchange.

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 as organizing the bulk of the SRMs, the joint SATOSS/APSIA seminars.

Three most interesting publications in 2019

1. Aditya Damodaran, Maria Dubovitskaya (Dfinity, Switzerland), Alfredo Rial, "UC Priced Oblivious Transfer with Purchase Statistics and Dynamic Pricing", International Conference on Cryptology in India, pp. 273-296. Springer, Cham, 2019.
   Priced oblivious transfer (POT) is a cryptographic protocol that allows

a buyer to purchase digital items from a seller without disclosing what items are bought. We propose a POT protocol that improves previous POT protocols in three ways. First, our POT protocol allows the seller to modify the prices of items at any time, while previous POT protocols need to be restarted to allow price modifications. Second, our POT protocol allows the seller to optionally receive statistics about the items bought by buyers, while previous POT protocols do not allow it. This feature is added with negligible impact on efficiency. Third, our protocol is designed modularly. Despite that previous POT protocols are extensions of some oblivious transfer (OT) scheme, they do not use the OT scheme as a building block. Consequently, the security of the OT scheme needs to be reanalyzed. Our modular design allows our POT protocol to be instantiated with any securer OT scheme, which yields multiple implementations and avoids reanalyzing the security of the OT scheme.

2. Verena Distler, Marie-Laure Zollinger, Carine Lallemand, Peter B. Roenne, Peter YA Ryan, and Vincent Koenig. "Security-Visible, Yet Unseen?" In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1-13. 2019.
An unsolved debate in the field of usable security concerns whether security mechanisms should be visible, or black boxed away from the user for the sake of usability. However, tying this question to pragmatic usability factors only might be simplistic. This study aims at researching the impact of displaying security mechanisms on user experience (UX) in the context of e-voting. Two versions of an e-voting application were designed and tested using a between-group experimental protocol (N=38). Version D displayed security mechanisms, while version ND did not reveal any security-related information. We collected data on UX using standardized evaluation scales and semi-structured interviews. Version D performed better overall in terms of UX and need fulfilment. Qualitative analysis of the interviews gives further insights into factors impacting perceived security. Our study adds to existing research suggesting a conceptual shift from usability to UX and discusses implications for designing and evaluating secure systems.

3. David Mestel, "Quantifying Information Flow in Interactive Systems," 2019 IEEE 32nd Computer Security Foundations Symposium (CSF), Hoboken, NJ, USA, 2019, pp. 414-41413. doi: 10.1109/CSF.2019.00035.
We consider the problem of quantifying information flow in interactive systems, modelled as finite-state transducers in the style of Goguen and Meseguer. Our main result is that if the system is deterministic then the information flow is either logarithmic or linear, and there is a polynomial-time algorithm to distinguish the two cases and compute the rate of logarithmic flow. To achieve this we first extend the theory of information leakage through channels to the case of interactive systems, and establish a number of results which greatly simplify computation. We then show that for deterministic systems the information flow corresponds to the growth rate of antichains inside a certain regular language, a property called the width of the language. In a companion work we have shown that there is a dichotomy between polynomial and exponential antichain growth, and a polynomial time algorithm to distinguish the two cases

and to compute the order of polynomial growth. We observe that these two cases correspond to logarithmic and linear information flow respectively. Finally, we formulate several attractive open problems, covering the cases of probabilistic systems, systems with more than two users and nondeterministic systems where the nondeterminism is assumed to be innocent rather than demonic.

4.3 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 Saarbrücken, at the University of Antwerp, and at Ulm University. The group currently consists of two PhD students, Alessandro Temperoni and Paul Meder, and two post-doctoral researchers, Dr. Maciej Skorski and Dr. Vinu Venugopal. Two more PhD students are 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. We currently also have one open PhD position in the context of above FNR-PRIDE DTU. As in the previous years, 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 an 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 has been held in 2019; further joint research activities are planned along these lines.

(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 Michael Böhlen, University of Zurich) are in the context of temporal database models that now also fully support the afore-described probabilistic extensions. Further ongoing collaborations in this domain are with Northeastern University (Wolfgang Gatterbauer) and the University of Antwerp (Floris Geerts). Moreover, Martin Theobald served as PC co-chair of the "13th International Conference on Scalable Uncertainty Management" (SUM 2019), which was held in Compiègne, France, on December 16-18, 2019.

(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 performance gains of a factor of up to 15 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. The group supervised 6 Master theses in the above areas and contributed to more than 420 hours of teaching in 2019.

Summary of the group's achievements in 2019

1. Maarten Van den Heuvel, Peter Ivanov, Wolfgang Gatterbauer, Floris Geerts, Martin Theobald: Anytime Approximation in Probabilistic Databases via Scaled Dissociations. SIGMOD Conference 2019: 1295-1312

2. Katerina Papaioannou, Martin Theobald, Michael H. Böhlen: Outer and Anti Joins in Temporal-Probabilistic Databases. ICDE 2019: 1742-1745

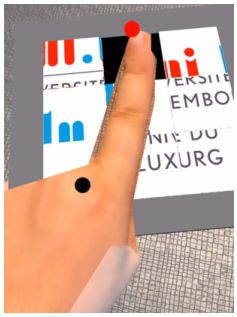
3. Nahla Ben Amor, Benjamin Quost, Martin Theobald: Scalable Uncertainty Management - 13th International Conference, SUM 2019, Compiègne, France, December 16-18, 2019, Proceedings. Lecture Notes in Computer Science 11940, Springer 2019

4.4 Collaborative and Socio-Technical Systems (COaST)

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

The COaST group focuses on distributed collaborative systems, complex networks and self-organization, socio-technical modelling, educational technologies and mediated reality. The group operates the VR/AR Lab at the Department of Computer Science.

Summary of the group's achievements in 2019



By the end of 2019, the COaST group counted 5 members (1 professor, 1 senior researcher, 3 PhD candidates) and 6 publications. The group's research in the context of the ongoing projects CollaTrEx and Yactul appeared in renowned academic publications and was presented at various international conferences and scientific events, again winning a best paper award. The FNR-INTER project DELICIOS officially started toward the end of the year. An invited talk on mixed reality approaches for digital and visual history bears further witness to the group's commitment to interdisciplinary collaboration. In addition, members of the group were involved in the organization of various international scientific events and conferences such as IEEE SASO, SAOS, ACM MMSys/MMVE, OLA and IEEE ACSOS. 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. Dr. Jean Botev received the University of Luxembourg Teaching Award.

Three most important publications in 2019

1. **Jean Botev, Joe Mayer, Steffen Rothkugel. Immersive Mixed Reality Object Interaction for Collaborative Context-Aware Mobile Training and Exploration.** In Proc. 11th International Workshop on Immersive Mixed and Virtual Environment Systems at the 10th ACM Multimedia Systems Conference, pp.4-9, 2019.
   This paper discusses an immersive object interaction approach based on gestural input generated solely from the integrated camera of current mobile devices. Going well beyond basic user-device interaction paradigms, it particularly aims at in-situ multiuser interaction with shared virtual objects. A set of demo implementations showcase how collaboration between users can be supported and entertaining yet challenging activities can be provided on site and with varying degrees of difficulty.

2. **Christian Grévisse, Steffen Rothkugel, Robert Reuter. Scaffolding Support through Integration of Learning Material.** In Smart Learning Environments, 6(28), pp.1-24, 2019.
   This article gives an overview of the ALMA-Yactul ecosystem, which pro-

vides scaffolding support to students by retrieving and integrating learning material in different tools. After discussing the cognitive foundations of the work, the paper showcases use cases of the comprised tools in various study domains. Both quantitative and qualitative analysis with students from the BINFO as well as an experiment carried out in two Luxembourgish high schools yielded significant results.

3. **Aryobarzan Atashpendar, Christian Grévisse, Steffen Rothkugel. Enhanced Sketchnoting through Semantic Integration of Learning Material.** In Proc. 2nd International Conference on Applied Informatics, pp.340-353, 2019. Best Paper Award.
This paper discusses the retrieval and integration of learning material in an enhanced sketchnoting app. Through handwriting recognition and semantic annotation, resources relevant for the concepts mentioned in the handwritten notes are retrieved from existing Knowledge Graphs. In addition, drawing recognition enables visual queries, allowing for enhanced search capabilities.

4.5 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 institutes. 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 two people; besides the head there is Andrea Capponi who joined in 2016 as a PhD candidate. 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.

Most relevant publications of 2019

1. [Best Paper Award at IEEE Globecom '19 - CQRM Symposium]: Vitello, P., Capponi, A., Fiandrino, C., Cantelmo, G., & Kliazovich, D. The Impact of Human Mobility on Edge Data Center Deployment in Urban Environments. In IEEE Globecom, Kona, HI, US, 2019.

2. A. Capponi, C. Fiandrino, B. Kantarci, L. Foschini, D. Kliazovich and P. Bouvry, "A Survey on Mobile Crowdsensing Systems: Challenges, Solutions, and Opportunities," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2419-2465, third quarter 2019.

3. Capponi, A., Vitello, P., Fiandrino, C., Cantelmo, G., Kliazovich, D., Sorger, U., & Bouvry, P. Crowdsensed Data Learning-Driven Prediction of Local

Businesses Attractiveness in Smart Cities. In IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 2019.

4.6 Critical Real-Time Embedded Systems (CRTES)

Head of research group: Associate Prof. Nicolas Navet

The CRTES group, part of the LASSY laboratory, studies how to build provably safe mission-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).

Summary of the group's achievements in 2019

In 2019 the CRTES group was made up of 4 members (1 associate-professor, 1 research scientist, 2 PhD students) and had 6 peer-reviewed publications published or accepted, including 3 journal papers, with 3 conference program participation. Prof. Navet was in the defense board of 4 Phd thesis and in 3 Phd supervisory committees. The group's members contributed to CSC teaching programs by teaching 5 courses, both at the Bachelor (professional and academic) and Master levels, and supervising 9 Bachelor semester projects (BSP).

In the field of Model-Driven Engineering (MDE), we explored how to "augment" in an automated manner control system models with dependability mechanisms, so as to meet non-functional concerns such as safety using the most effective mechanisms. The group participates in the redesign of the motion-planning system of Robox company. The innovative aspects of this industrial contract are the use of an MDE flow from the early design stages, and the support of multi-core processors in an application with stringent timing constraints.

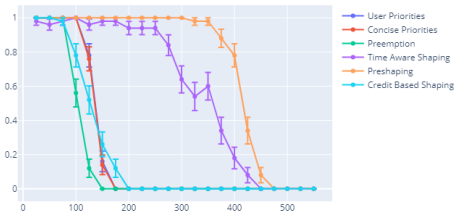
Most of our work was in the field of E/E architecture design and real-time communication systems with contributions on well-established networks like CAN and emerging standards like Ethernet Time Sensitive Networking (TSN). Our work aims to further automate the design activities based on constraints and goals. We develop an approach rooted in computational thinking where system designers break down the general multi-dimensional design problem into smaller problems that algorithmics tools can solve in a near optimal way. Progresses were made this year in developing machine learning algorithms that speed-up by several orders of magnitude the performance evaluation of computer systems with respect to simulation or mathematical analysis.

Three most interesting publications in 2019

1) T. Hu, I. Cibrario Bertolotti, N. Navet, L. Havet, "Automated Fault Tolerance Augmentation in Model-Driven Engineering for CPS", to appear in Computer Standards & Interfaces, Elsevier. We propose an approach implemented in

an open-source model-transformation framework which allows system designers to decouple functional and non-functional concerns, and express dependability properties at design time using domain-specific languages. The functional control models are then automatically "augmented" with dependability mechanisms while preserving their real-time behavior. The practicality of the approach is demonstrated with the automated implementation of N-Version Programming in the CPAL model-driven engineering workflow

2) N. Navet, J. Villanueva, J. Migge, "Early-stage topological and technological choices for TSN-based communication architectures", 2019 IEEE Standards Association Ethernet Automotive Day, Detroit, USA, September 24-25, 2019. We propose a design-space-exploration (DSE) approach based on synthetic data to quantify the "capacity" of an E/E architecture, which allows to make early stage design choices based on quantified metrics at a time when communication needs are mainly unknown. The approach is applied on Renault's FACE service-oriented E/E architecture.



Probability to successfully schedule a given number of streams on the TSN backbone for different QoS options.

3) T.L. Mai, N. Navet, J. Migge, "On the use of supervised machine learning for assessing schedulability: application to Ethernet TSN", Proc. 27th International Conference on Real-Time Networks and Systems (RTNS'2019), Toulouse, France, November 6-8, 2019. In this work, we ask if Machine Learning (ML) can provide a viable alternative to schedulability analysis to determine whether a real-time Ethernet network meets a set of timing constraints. We study the problem when the topology of the networks is fixed and known in advance but the traffic unknown. The experimental results suggest that standard feature-based ML algorithms are efficient at predicting the feasibility of realistic TSN networks, with an accuracy above 90%. The large speedup brought by ML will facilitate the implementation of DSE algorithms in the design of E/E architectures.

4.7 CryptoLux

Head of research group: Professor Dr. Alex Biryukov

The CryptoLux group is part of LACS/DSC/FSTM as well as SnT and works on all aspects of symmetric cryptography, ranging from design and analysis of primitives over efficient and secure implementation to the deployment in real-world systems and networks. CryptoLux is also pursuing research on crypto currencies, smart contracts, and other emerging areas in information security, privacy, and anonymity. Further information about the group is available at http://cryptolux.org.

Summary of the group's achievements in 2019

In 2019 the CryptoLux group consisted of 11 members (1 full professor, 1 senior researcher (shared), 3 postdocs, 6 Ph.D. students), who published more than 12 papers in major international journals and conference proceedings. One Ph.D. student (Aleksei Udovenko) graduated with excellent overall mark. The FNR CORE project FinCrypt, which deals with financial cryptography, entered its second year. Professor Biryukov served on the technical program committee of several international conferences including CT-RSA, Financial Cryptogaphy, ACNS, as well as the top-tier cryptography conference EUROCRYPT. He was also a member of the editorial board of the IACR journal "Transactions on Symmetric Cryptography (ToSC)". Furthermore, he served as program co-chair of the 3rd edition of the workshop "Cryptocurrencies and Blockchain Technology (CBT 2019)", which took place in Luxembourg and was attended by over 70 researcher from all over the world. CryptoLux members taught various courses in the bachelor and master programs and supervised student projects.

Most interesting achievements in 2019

1. The Cryptolux group won the Whitebox cryptography competition WhiBox'19 in both the design and analysis category. This competition was organized by an international community of researchers to address the growing interest of the industry towards white-box cryptography (most particularly for DRMs and mobile payments) and the obvious difficulty of designing secure solutions in a scientifically valid sense.

2. The group submitted the newly-designed authenticated encryption algorithm Schwaemm and hash function Esch to the Lightweight Cryptography Project of the U.S. National Institute of Standards and Technology (NIST), whose goal is to standardize new symmetric algorithms that are suitable for the Internet of Things. A total of 67 candidates were submitted, of which 32 made it into the second round of the evaluation process. The proposal of the CryptoLux group is among these 2nd-round candidates.

3. As part of the research activities of the FinCrypt project, the CryptoLux group demonstrated the presence of subliminal channels in Groth's zk-SNARK proof protocol (EUROCRYPT 2016) and Pedersen's commitment scheme, which are both currently used by the crypto currency Zcash. These discoveries and how they can be used to actively tag Zcash shielded transactions were presented at thetop-tier security conference ACM CCS in London.

Top academic publications

1. Alex Biryukov, Daniel Feher, Giuseppe Vitto: Privacy Aspects and Subliminal Channels in Zcash. ACM CCS 2019: 1795-1811

2. Alex Biryukov, Sergei Tikhomirov: Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis. EuroS&P 2019: 172-184

3. Daniel Dinu, Yann Le Corre, Dmitry Khovratovich, Léo Perrin, Johann Großschädl, Alex Biryukov: Triathlon of lightweight block ciphers for the Internet of things. Journal of Cryptographic Engineering 9(3): 283-302 (2019)

4.8 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 2019: Qin Ma (research scientist) 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 2019

In 2019, the team pursued the research on lightweight modeling initiated in 2018. We have contributed a modeling framework for example-driven modeling and model transformation specification. The research findings and the framework itself were taught in the MDSD course of the MICS programme. An associated tool, named Fudomo, was developed by Christian Glodt for the Atom editor platform, including support for editing, validation and transformation functionalities. Qin Ma continued her collaboration with colleagues from the University of Duisburg-Essen and from the Mexico Autonomous Institute of Technology in the field of smart grids, whereby conceptual modeling languages and model-based analysis techniques are used in tandem to enable valuation and strategic analysis of smart grid initiatives. Qin Ma was a PC member of the FiCloud 2019 conference. Qin Ma also participated in the teaching of lab sessions for the "Programming Fundamentals 1" course in the BICS program.

Besides his work on the Fudomo tool Christian Glodt also maintainted and improved "Accord", the research information database of the CSC. In addition, he maintained and improved MICSM, the information management system of the Master in Computer Science degree, participated in the organisation of lab sessions for the "Programming Fundamentals 1" course and supervised several BSP projects in the "Bachelor in Computer Science (BICS)".

Three most interesting publications (or other achievements) in 2019

1. Loïc Gammaitoni, Pierre Kelsen (2019) F-Alloy: a relational model transformation language based on Alloy. Software and Systems Modeling 18(1): 213-247.
   In this paper we introduce a new model transformation language - named

F-Alloy - based on the formal language Alloy. F-Alloy's semantics are given as a direct translation to Alloy; hence, F-Alloy specifications are analyzable using the powerful automatic analysis features of Alloy.

2. Amalio, Nuno and Briand, Lionel and Kelsen, Pierre (2019) An Experimental Scrutiny of Visual Design Modelling: VCL up against UML+OCL. Empirical Software Engineering. ISSN 1382-3256 (In Press).
   The paper presents the results of a controlled experiment, which compares VCL against UML and OCL and whose goal is to provide insight on benefits and limitations of visual modelling. Results suggest VCL benefits in defect detection, model comprehension, and modelling of operations.

3. Sybren de Kinderen, Monika Kaczmarek-Heß, Iván S. Razo-Zapata, Qin Ma. Strategic Analysis in the Realm of Enterprise Modeling - On the Example of Blockchain-Based Initiatives for the Electricity Sector. Wirtschaftsinformatik 2019 (the 14th International Conference on business informatics). 154-168.
   In this paper, we introduce a model based instrument for strategic analysis of digital transformations in which application of IT technologies is a key enabler. To show the applicability of the proposed approach, we carried out a case study on the blockchain- based NRGCoin initiative from the smart grid domain.

4.9 Individual and Collective Reasoning Group (ICR)

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

ICR is a major group of the Interdisciplinary Lab for Intelligent and Adaptive Systems, a cornerstone of the Department of Computer Science. Its interdisciplinary scope is illustrated by its collaboration with a vast range of UL components, including SnT, the Center for Contemporary and Digital History, for FSTM: Mathematics and Computational Engineering, for FDEF: Law and the Centre for Logistics, and for FLSHASE: Humanities, and Behavioural and Cognitive Sciences, not to forget long-standing links with LIST. There are furthermore extensive connections with leading research institutes on all five continents, to mention just Stanford (USA) and Zhejiang University (Hangzhou, China).

ICR is interested in the theoretical and computational modeling and study of high-level cognitive tasks of intelligent agents, like reasoning, learning, inquiry, planning, communication and argumentation. More specifically, ICR research addresses normative reasoning in multi-agent contexts (deontic logics, AI ethics - also from the perspective of the AIs, social robotics), logics for robots and intelligent systems (from model-theoretic semantics to actual provers), legal knowledge representation, reasoning, and mining, up to NLP-based applications, formal argumentation, defeasible reasoning, and belief change for dynamic, uncertain, incomplete, and inconsistent information. Robot activities are coordinated by the AI Robolab.

Summary of the group's achievements in 2019

ICR hosted 27 researchers (not all simultaneously): 1 full professor, 2 visiting and 2 guest professors, 1 research scientist, 8 resident and 3 visiting postdocs, 3 local, 2 LAST-JD, and 4 visiting PhD students.

MIREL (Mining and Reasoning with Legal Texts), a large H2020-MSCA-RISE network coordinated by ICR, completed its 4th and final year and brought a number of fruitful short- to longterm exchange activities. ICR continued to be involved in the ERASMUS MUNDUS network LAST-JD (Joint International Doctoral Degree in Law, Science, and Technology), resp. started to participate to its sequel, the MSCA ITN program LAST-JD-RIoE (Rights of the Internet of Everything). 2 former LAST-JD students finished their PhD in 2019. The AI Robolab participated in a COST action on Explainable AI (XAI). Our student Maya Olszewski won the Germain Dondelinger prize for the best master thesis of the University of Luxembourg for her work "Exploring permission in I/O Logic". At the World Championship for Automatic Theorem Proving in Brazil, Alexander Steen won a first prize for his theorem prover Leo-III based on higher-order logic, which he started to apply to normative reasoning. Livio Robaldo successfully completed the Dapreco project which produced a freely available KB formalizing GDPR rules based on reified I/O Logic, joining also the technical committee of LegalRuleML. Réka Markovich has been elected to the board of the Benelux Association for AI. Sviatlana Höhn published her book "Artificial Companion for Second Language Conversation". In addition to becoming a guest professor at Zhejiang University, a top institution in China, Prof. Leon van der Torre has also been recruited in China as a national high-end foreign expert. Last but not least, the Jiminy Cricket paper on mechanisms for moral decision making found its way into the Daily Mirror.

Most important publications in 2019

1. **B. Liao, M. Slavkovik, L.W.N. van der Torre.** *Building Jiminy Cricket: An Architecture for Moral Agreements Among Stakeholders.* AIES 2019: 147-153.

2. **L. Robaldo, C. Bartolini, M. Palmirani, A. Rossi, M. Martoni, G. Lenzini.** *Formalizing GDPR provisions in reified IO-logic, the DAPRECO knowledge base.* Journal of Logic, Language, and Information, 2019 (online).

3. **S. Haddadan, E. Cabrio, S. Villata.** *Yes, we can! Mining Arguments in 50 Years of US Presidential Campaign Debates.* Proc. of the 57th Meeting of the Association for Computational Linguistics: 4684-4690, 2019.

4. **R. Booth R., G. Casini, T. Meyer, I. Varzinczack.** *On Rational Entailment for Propositional Typicality Logic.* Artificial Intelligence Journal, vol. 277, 2019 (online).

4.10 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 application of Machine Learning. In this context, we have cooperated with colleagues from the C2DH, the Department of Linguistics, and the Department of Cognitive as well as with industrial partners (RTL, KPMG). MINE consists of 1 professor, 4 PostDocs, and 4 PhD candidates, whose research concerns fields like Sentiment Analysis, Topic Modeling, and Natural Language Understanding in general, and other applications related to Machine Learning. A central focus lies in the education of students on Bachelor, Master, and Doctoral Levels with courses on *Machine Learning, Knowledge Discovery, Data Science,* and *Information Retrieval* - both in Computer Science and Mathematics and in Luxembourg and abroad. Current research projects have concerned Sentiment Analysis with Luxembourgish Language (RTL), Topic Modeling of Australian Aborigines Literature, and Deep Learning approaches for Twitter data. Additionally, we applied Convolutional Networks (Tensorflow) to text and image data and produced, among others, pictures in van Gogh- and Matisse-style. We also have got in close contact with Prof Rejko Krüger in view of his research on Parkinson-diseased patients. Further selected achievements in 2019 have been: **Siwen Guo** has defended her PhD thesis with the mark "Outstanding". An international committee with reviewers from Amazon Alexa Berlin, Lenovo Beijing, and LuxAI as well from the Universities of Bonn, Potsdam, and Luxembourg has confirmed this excellence. In addition to his teaching duty at UL, **Christoph Schommer** has given invited lectures at Singapore University SUTD and FU Berlin (Erasmus+ grant) in Summer 2019. **Juliana Stropp** has received a *Marie-Curie Fellowship project* by the European Union. **Vladimir Despotovic**, an international expert in *speech technology*, has decided to join the *MINE* research group. In the scope of the *CLAIRE* network, we have received a letter of support by the Prime Minister Xavier Bettel and the

Ministry of Higher Education and Research, Claude Meisch. **Christoph Schommer** has actively supported the *"Schülerwettbewerbe der Bundeszentrale für politische Bildung in Zusammenarbeit mit dem Zentrum fir politesch Bildung in Luxemburg"* with students from schools (Dudelange, and Kirchberg). MINE contributes the internal activities with Human-Computer Interaction and Cognitive Science (see our ACC – *AI and Cognitive Concepts Lab*). Finally, we have got in close contact to *Zortify*, a start-up company in Luxembourg.

Selected Publications in 2019

1. Guo, S., Höhn, S., & Schommer, C. (2019). *A Personalized Sentiment Model with Textual and Contextual Information.* The SIGNLL Conference on Computational Natural Language Learning, Hong Kong 3-4 November 2019.
2. Guo, S., Höhn, S., & Schommer, C. (2019). *Looking into the Past: Evaluating the Effect of Time Gaps in a Personalized Sentiment Model.* ACM/SIGAPP Symposium On Applied Computing, Limassol 8-12 April 2019.
3. Guo, S., Höhn, S., Xu, F., & Schommer, C. (2019). *Personalized Sentiment Analysis and a Framework with Attention-Based Hawkes Process Model.* Agents and Artificial Intelligence. Springer.
4. Schommer, C. (2019). *Künstliche Intelligenz für die Medizin.* Luxemburger Wort, 244(171), p. 16-17.
5. Schommer, C. (2019). *Ein europäisches CERN für die Künstliche Intelligenz.* Luxemburger Wort, 170(298), p. 18.
6. Sirajzade, J., & Schommer, C. (2019). *The LuNa Open Toolbox for the Luxembourgish Language.* In P., Perner (Ed.), Advances in Data Mining, Applications and Theoretical Aspects, Poster Proceedings 2019. Leipzig, Germany: ibai publishing.

4.11 Methods and Tools for Software Engineering, DevOps and Artificial Intelligence (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 2019

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 2019

1. Jahic Benjamin; Guelfi Nicolas; Ries, Benoît. “Software Engineering for Dataset Augmentation using Generative Adversarial Networks”. Proceedings of the 10th IEEE International Conference on Software Engineering and Service Science. This paper presents a novel software engineering approach for dataset augmentation using neural networks. It proposes a rigorous process for generating synthetic data to improve the training of neural networks. An experimentation with the MNIST dataset has been performed which demonstrates a successful usage of our approach. Lastly, current issues are discussed.

2. The first international workshop on Frontiers in Software Engineering Education (FISEE19 - https://www.laser-foundation.org/fisee/fisee-2019/) was co-organised with the LASER Foundation and colleagues from Innopolis University to discuss what education in Software Engineering needs, what should be changed and how new and traditional institutions can adapt to the fast pace of technology. The outcomes of this workshop are published as a volume of the Springer Lecture Notes in Computer Science (LNCS) to appear in 2020.

3. Yasir Imtiaz Khan, Alexandros Konios, and Nicolas Guelfi. 2019. “A Survey of Petri Nets Slicing”. ACM Computing Surveys Volume 51, Issue 5 January 2019, 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.

4.12 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. In addition, PCOG is at the heart of the digital strategy of the university by managing the High Performance Computing (HPC) developments and the associated facility since 2007. Detailed information about the group is available at http://pcog.uni.lu/.

Summary of the group's achievements in 2019

In 2019, the PCOG team counted 20 members (1 professor, 3 research scientists, 5 postdocs, 8 PhD students, 2 research and development specialists, 1 technical support staff member) and produced a total of 27 publications (1 book, 8 journal articles, 3 book chapters, 10 conference articles, 5 reports). Two PhD students defended their thesis in 2019. 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 three joint technical reports on "Smart ICT : Gap Analysis Between Scientific Research and Technical Standardization". These were officially presented during the World Standards Day on October 11, 2019.

PCOG has run three research projects in 2019. The "Digital Trust in Smart ICT" project with the ILNAS, the HUNTED (Heterogeneous multi-swarms of UNmanned auTonomous systEms for mission Deployment) project funded by the Office of Naval Research Global (ORNG – US Navy) and the H2020 PRACE-6IP, the 6th implementation phase of the "Partnership for Advanced Computing", which is a permanent pan-European High Performance Computing service. PCOG was also leading one technology transfer project funded by the FNR Proof-of-Concept program, SIMMS (Swarms of Intelligent Missions systeMS).

PCOG additionally participates in the new NVidia joint AI lab of Luxembourg with Digital Luxembourg, SnT, LCSB and LIST, providing advanced HPC/research support on GPU/AI workflows.

PCOG received an award in 2019. Prof. Pascal Bouvry and Dr. Matthias Brust

received the Security Project of the Year Award during the Security Made in Luxembourg's Information Security Day 2019 for the project, Technical Standardisation for Trusted Use in the Field of Smart ICT, in collaboration with the ILNAS. The project tackles the challenge of standardisation and regulation in the rapidly developing worlds of big data and artificial intelligence, Internet of Things, and cloud computing.

PCOG team members taught in several Bachelor, Master and PhD programs (BICS, BINFO, Bachelor en Sciences de la Vie, MICS, Doctoral School in Computer Science), in the HPC workshop as well as in a pilot training program in Data Sciences for the employees of the Digital Pole for the European Commission.

PCOG is also in charge of the management of the High-Performance Computing (HPC) platform of the University. Its 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). The first HPC Service contracts were signed with the industry (Arcelor-Mittal, Ceratizit, etc.) and the HPC team has strongly supported the EuroHPC developments within the country. Dr. Varrette was also mandated as HPC expert for the European Commission within the Enhanced Regional EU-ASEAN Dialogue Instrument (E-READI) program to conduct a mapping study of ASEAN (Association of Southeast Asian Nations) policy orientations and related HPC research infrastructures.

Most interesting achievements in 2019

1) **Security Project of the Year Award - Security Day 2019**

PCOG's team working in collaboration with the Luxembourg Institute of Standardisation, Accreditation, Safety and Quality of Products and Services (ILNAS), has won the Information Security Day 2019's Security Project of the Year Award.

2) **The High-Performance Computing platform of the UL**

Managed by Prof. Bouvry and Dr. Varrette, it is currently the reference HPC facility within the country. End of 2019, the HPC platform featured a computational power of 1262 TFlops (11228 computing cores) and 9.8 PBytes for storage (incl. 1 PB for backups), serving hundreds of users. A set of specialized hardware accelerating AI and Big Data workflows were installed (adding 96 cutting-edge NVidia GPU accelerators and 4 Large-memory systems).

3) **Professor Dr. El-Ghazali Talbi appointed as Invited Professor**

In January 2019, Professor Dr. El-Ghazali Talbi from University of Lille/INRIA/CNRS, a long-term collaborator of PCOG, was appointed as Invited Professor in Computer Science by the Governing Board of the University of Luxembourg.

4) **Visiting Professor Dr. Roland Bouffanais**

Professor Dr. Roland Bouffanais from the Singapore University of Technology and Design (SUTD) visited PCOG in September 2019. Besides deepening the collaboration, Prof. Bouffanais provided the course DP-CSCE: Using Network Science to Design and Control Networked Systems at the doctoral school.

4.13 Proactive Computing

Head of research group: Prof. Dr. Denis Zampuniéris

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

Summary of the group's achievements in 2019

Apart from their regular research and publication work and their participation in teaching programmes offered by our Faculty, the group welcomed and supervised several students (local or from universities abroad) in internship for their Bachelor or Master thesis. In October 2019, the candidate Gilles Neyens successfully defended his PhD thesis entitled "Confidence-Based Decision-Making Support for Multi-Sensor Systems".

Most interesting publications in 2019

1. **Gilles Neyens and Denis Zampuniéris. Proactive Middleware for Fault Detection and Advanced Conflict Handling in Sensor Fusion.** In Proc. International Conference on Artificial Intelligence and Soft Computing, Zakopane (Poland), 2019.
   Robots traditionally have a wide array of sensors that allow them to react to the environment and make appropriate decisions. These sensors can give incorrect or imprecise data due to malfunctioning or noise. Sensor fusion methods try to overcome some of these issues by using the data coming from different sensors and combining it. However, they often don't take sensor malfunctioning and a priori knowledge about the sensors and the environment into account, which can produce conflicting information for the robot to work with. In this paper, we present an architecture and process in order to overcome some of these limitations based on a proactive rule-based system.
2. **Gilles Neyens and Denis Zampuniéris. Proactive Model for Handling Conflicts in Sensor Data Fusion Applied to Robotic Systems.** In Proc. International Conference on Software Technologies, Prague (Czech Repub-

lic), 2019.
Robots have to be able to function in a multitude of different situations and environments. To help them achieve this, they are usually equipped with a large set of sensors whose data will be used in order to make decisions. However, the sensors can malfunction, be influenced by noise or simply be imprecise. Existing sensor fusion techniques can be used in order to overcome some of these problems, but we believe that data can be improved further by computing context information and using a proactive rule-based system to detect potentially conflicting data coming from different sensors. In this paper, we will present the architecture and scenarios for a generic model taking context into account.

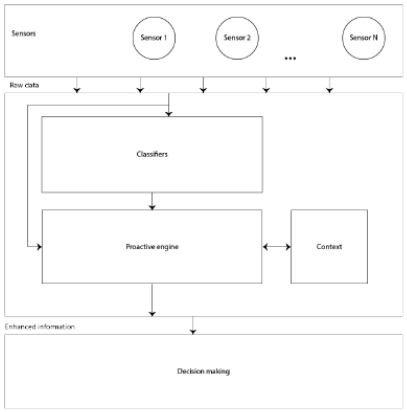


Figure 5.2: System architecture

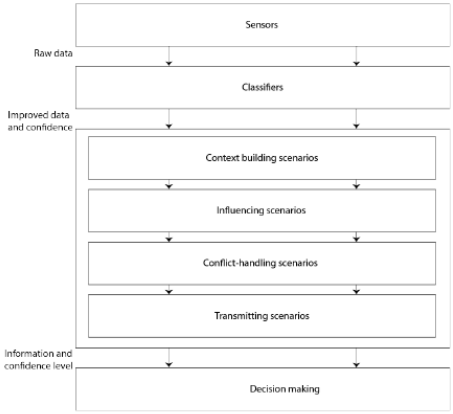


Figure 5.3: Scenario flow

4.14 Security and Networking Lab (SECAN-Lab)

Head of research group: Prof. Dr. Thomas Engel

SECAN-Lab addresses both fundamental and applied research activities in computer networking and security. The group's main research activities cover the following areas:

- Privacy in data communications, privacy by distribution, protection against network traffic analysis
- V2X and C-V2X communications
- Network and systems security including machine learning for big data analysis, malware detection and IT forensics
- SCADA and cyber security
- Wireless networks and mobile security
- Vehicular and multimodal traffic management based on V2X communications
- Automotive Ethernet
- Internet of Things, Quality of Service, IPv6 integration
- 5G key technologies (Software Defined Networks, Network Function Virtualization, Multi-Access Edge Computing)

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 2019

In 2019, SECAN-Lab was involved in 14 research projects in parallel where the majority of projects focussed on the group's core areas such as mobile and vehicular communication including involved security and privacy aspects. In the scope of the two large EU H2020 projects 5G-DRIVE and 5G-MOBIX, which both started in late 2018, we have been closely collaborating with major international players in the automotive and communication technology industry including BMW, Daimler, Siemens, Nokia, and Ericsson. 5G-DRIVE conducts a trial and validation of the interoperability between EU and China 5G networks operating at 3.5 GHz bands for enhanced Mobile Broadband (eMBB) and 3.5 and 5.9 GHz bands for V2X scenarios. 5G-MOBIX develops and tests automated vehicle functionalities using 5G core technological innovations along multiple cross-border corridors and urban trial sites, under conditions of vehicular traffic, network coverage, service demand, as well as considering the inherently distinct legal, business and social local aspects. The FNR CORE project CONTACT 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. Furthermore, the team was also able to intensify the collaboration with Honda R&D Europe in the scope of a second project accepted for funding by the Honda Initiation Grant Europe Program (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. Another project, we would like to highlight, is the FNR CORE project PETIT which is conducted in collaboration with the University College London. The goal of 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.

In terms of academic contributions, the SECAN-Lab team was also very successful in 2019 with more than 20 publications in international workshops, conferences, and journals.

Furthermore, team members were involved in the organizational or technical program committees of 7 international conferences and workshops, including the 8th International Conference on Advances in Vehicular Systems Technologies and Applications (VEHICULAR) and the 2nd International Workshop on 5G and Cooperative Autonomous Driving (5G Auto).

Furthermore, by the end of 2019 an experienced Research Scientist has joined

the team to reinforce the team's security and privacy research activities. The labs' activities on in-car networking could also be extended by means of two further Postdoctoral Researchers who closely collaborate with industry partners.

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.

Three most interesting publications in 2019

1. G. Rinaldi, F. Adamsky, R. Soua, A. Baiocchi, T. Engel: Softwarization of SCADA: Lightweight Statistical SDN-Agents for Anomaly Detection. In Proceedings of 10th International Conference on Networks of the Future (NoF), Rome, Italy, October 2019. IEEE.
   The increasing connectivity of restricted areas such as Critical Infrastructures (CIs) raises major security concerns for Supervisory Control And Data Acquisition (SCADA) systems, which are deployed to monitor their operation. Given the importance of an early anomaly detection, Intrusion Detection Systems (IDSs) are introduced in SCADA systems to detect malicious activities as early as possible. Agents or probes form the cornerstone of any IDS by capturing network packets and extracting relevant information. However, IDSs are facing unprecedented challenges due to the escalation in the number, scale and diversity of attacks. Software-Defined Network (SDN) then comes into play and can provide the required flexibility and scalability. Building on that, we introduce Traffic Agent Controllers (TACs) that monitor SDN-enabled switches via OpenFlow. By using lightweight statistical metrics such as Kullback-Leibler Divergence (KLD), we are able to detect the slightest anomalies, such as stealth port scans, evenin the presence of background traffic. The obtained metrics can also be used to locate the anomalies with precision over 90% inside a hierarchical network topology.

2. A. Di Maio, M. R. Palattella, T. Engel: Multi-flow congestion-aware routing in software-defined vehicular networks. In Proceedings of 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, USA, September 2019. IEEE.
   5G-enabled vehicular networks will soon allow their users to exchange safety and non-safety related information over heterogeneous communication interfaces. Routing vehicular data flows over multi-hop Vehicle-to-Vehicle (V2V) communications is one of the hardest challenges in vehicular networking, and it has been tackled in literature by using distributed algorithms. The distributed approach has shown significant inefficiencies in such dynamic vehicular scenarios, mainly due to poor network congestion control. To overcome the complexity of the envisioned architecture, and the inefficiency of distributed routing algorithms, we hereby propose to leverage the coordination capabilities of Software-Defined Net-

working (SDN) to determine optimal V2V multi-hop paths and to offload traffic from the Vehicle-to-Infrastructure-to-Vehicle (V2I2V) to the V2V communications, using both cellular and Wi-Fi technologies. In order to achieve this goal, we propose Multi-Flow Congestion-Aware Routing (MFCAR), a centralized routing algorithm that relies on graph theory to choose short and uncongested V2V paths. Realistic simulations prove that MFCAR outperforms well-established centralized routing algorithms (e.g. Dijkstra's) in terms of Packet Delivery Ratio (PDR), goodput and average packet delay, up to a five-fold performance gain.

3. M. R. Palattella, R. Soua, A. Stemper, T. Engel: Aggregation of MQTT Topics over Integrated Satellite-Terrestrial Networks. In ACM SIGMETRICS Performance Evaluation Review, Januar 2019. ACM.
   The MQTT application protocol was originally designed for monitoring an oil pipeline through the desert by collecting sensor data via satellite link. Thus, by design MQTT is very suitable for data collection over integrated satellite-terrestrial networks. Leveraging on the MQTT Bridge functionality, in this work we propose a novel architecture with two MQTT Brokers located at the satellite terminal and the satellite gateway. By using the topic pattern option, supported by the bridge, a subscriber can request several topics with in a single request. To reduce the amount of traffic exchanged over the satellite return channel, we introduce in the architecture a new entity, namely MQTT message aggregation filter, which aggregates all the MQTT topics matching the topic pattern in the same response.

4.15 Security and Trust of Software Systems (SaToSS)

Head of research group: Prof. Sjouke Mauw

Since its establishment in 2007, the SaToSS group has been focusing on formalizing and applying formal reasoning to real-world security problems. The group carries out research on a variety of topics such as:

- security protocols (e.g., e-voting, distance-bounding, blockchain),
- attack trees and security analysis,
- privacy (e.g., location privacy, privacy in social networks and machine learning),
- 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),
- security in space

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 achievement in 2019

In 2019, the SaToSS group has experienced a large growth and counted 23 researchers (1 professor, 1 senior researcher, 10 postdocs, 11 PhD students). Currently the group runs one Junior CORE project (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), two FNR PRIDE projects (SP-squared on deep learning and DRIVEN on social analysis) and one AFR project (PriML on privacy in machine learning). The group has also secured funding for a research associate position within the FNR INTER project SLANT which will start in 2020. In 2019, the group has successfully completed the Junior CORE project COMMA. The junior PI of COMMA, Dr. Olga Gadyatskaya, has joined Leiden University, Netherlands, as an assistant professor. The group has contributed to the organization of scientific events (e.g., VTSA 2019 as the local organizer). Our regular research seminar SRM co-organized jointly with the ASPIA group has featured 27 international speakers. SaToSS has been actively involved in teaching and student supervision for bachelor and master programs in Computer Science (BINFO, BICS, MICS, MSSI).

Three most interesting publications in 2019

1. **Post-collusion Security and Distance Bounding. Sjouke Mauw, Zach Smith, Jorge Toro-Pozo, Rolando Trujillo-Rasua**, in Proceedings of 26th ACM Conference on Computer and Communications Security (CCS) 2019: 941-

958. Verification of cryptographic protocols is traditionally built upon the assumption that participants have not revealed their long-term keys. However, in some cases, participants might collude to defeat some security goals, without revealing their long-term secrets. We develop a model based on multiset rewriting to reason about collusion in security protocols. We introduce the notion of post-collusion security, which verifies security properties claimed in sessions initiated after the collusion occurred. We use post-collusion security to analyze terrorist fraud on protocols for securing physical proximity, known as distance-bounding protocols. In a terrorist fraud attack, agents collude to falsely prove proximity, whilst no further false proximity proof can be issued without further collusion. Our definitions and the Tamarin prover are used to develop a modular framework for verification of distance-bounding protocols that accounts for all types of attack from literature. We perform a survey of over 25 protocols, which include industrial protocols such as Mastercard's contactless payment PayPass and NXP's MIFARE Plus with proximity check. For the industrial protocols we confirm attacks, propose fixes, and deliver computer-verifiable security proofs of the repaired versions.

2. **Sequential Reprogramming of Boolean Networks Made Practical.** Hugues Mandon, **Cui Su**, Stefan Haar, **Jun Pang**, and Loïc Paulevé, in Proceedings of International Conference on Computational Methods in Systems Biology (CMSB) 2019: 3-19. We address the sequential reprogramming of gene regulatory networks modelled as Boolean networks. We develop an attractor-based sequential reprogramming method to compute all sequential reprogramming paths from a source attractor to a target attractor, where only attractors of the network are used as intermediates. Our method is more practical than existing reprogramming methods as it incorporates several practical constraints: (1) only biologically observable states, viz. attractors, can act as intermediates; (2) certain attractors, such as apoptosis, can be avoided as intermediates; (3) certain nodes can be avoided to perturb as they may be essential for cell survival or difficult to perturb with biomolecular techniques; and (4) given a threshold k, all sequential reprogramming paths with no more than k perturbations are computed. We compare our method with the minimal one-step reprogramming and the minimal sequential reprogramming on a variety of biological networks. The results show that our method can greatly reduces the number of perturbations compared to the one-step reprogramming, while having comparable results with the minimal sequential reprogramming. Moreover, our implementation is scalable for networks of more than 60 nodes.

3. **Breaking Unlinkability of the ICAO 9303 Standard for e-Passports Using Bisimilarity.** Ihor Filimonov, **Ross Horne**, **Sjouke Mauw**, **Zach Smith**, in Proceedings of 24th European Symposium on Research in Computer Security (ESORICS) 2019: 577-594. We clear up confusion surrounding privacy claims about the ICAO 9303 standard for e-passports. The ICAO 9303 standard includes a Basic Access Control (BAC) protocol that should protect the user from being traced from one session to another. While it is well known that there are attacks on BAC, allowing an attacker to link multiple uses of the same passport, due to differences in implementation; there

still remains confusion about whether there is an attack on unlinkability directly on the BAC protocol as specified in the ICAO 9303 standard. This paper clarifies the nature of the debate, and sources of potential confusion. We demonstrate that the original privacy claims made are flawed, by uncovering attacks on a strong formulation of unlinkability. We explain why the use of the bisimilarity equivalence technique is essential for uncovering our attacks. We also clarify what assumptions lead to proofs of formulations of unlinkability using weaker notions of equivalence. Furthermore, we propose a fix for BAC within the scope of the standard, and prove that it is correct, again using a state-of-the-art approach to bisimilarity.

4.16 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 2019

SerVal has been successful in several dimensions in 2019. The number of researchers is around 35 researchers. Three PhD students defended in 2019. Overall, the group published around 35 papers in top venues such as FSE, ICSE, Empirical Software Engineering, ISSTA, IST, IEEE TSE etc. The two projects with Paypal started, and new projects were initiated with with BGL BNP Paribas. A couple of FNR Projects have been funded (CORE, Junior and Bridges). Together with Dr. Papadakis, Dr. M. Jimenez, R. Rwemalika, Prof. Le Traon received a Distinguished Paper award for their ACM ESEC-FSE 2019, and the Facebook Testing and Verification 2019 - Research Award. Dr. Papadakis and Prof. Le Traon have been appointed General Chair of the International Conference on Software Maintenance and Evolution 2021 (ICSME 21). Prof. Klein and Bissyandé have been appointed GC of the 35th IEEE/ACM International Conference Automated Software Engineering 2022 (ASE 2022).

In terms of collaboration, the team expects to launch to new partnerships in 2020, one with Luxtrust, the other with Ceratizit.

At the end of 2019, SerVal is split and a spin-off group from the initial group, called TrustX, headed by Prof. J. Klein and involving Prof. Bissyandé is created. Next year, Serval will refocus on challenges related to software testing and about making machine-learning based systems robust and trustable.

Main publications and achievements in 2019

1. The importance of accounting for real-world labelling when predicting software vulnerabilities: Matthieu Jimenez, Renaud Rwemalika, Mike Papadakis, Federica Sarro, Yves Le Traon, Mark Harman. Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (FSE 2019) - Distinguished paper award.
   Previous work on vulnerability prediction assume that predictive models are trained with respect to perfect labelling information (includes labels from future, as yet undiscovered vulnerabilities). In this paper we present results from a comprehensive empirical study of 1,898 real-world vulnerabilities reported in 74 releases of three security-critical open source systems (Linux Kernel, OpenSSL and Wireshark). Our study investigates the effectiveness of three previously proposed vulnerability prediction approaches. The results reveal that the unrealistic labelling assumption can profoundly mislead the scientific conclusions drawn; suggesting highly effective and deployable prediction results vanish when we fully account for realistically available labelling in the experimental

methodology. The community therefore needs to upgrade experimental and empirical methodology for vulnerability prediction evaluation and development to ensure robust and actionable scientific findings.

2. Learning to spot and refactor inconsistent method names: Kui Liu, Dongsun Kim, Tegawendé F Bissyandé, Taeyoung Kim, Kisub Kim, Anil Koyuncu, Suntae Kim, Yves Le Traon. 2019 IEEE/ACM 41st International Conference on Software Engineering (ICSE)
   To ensure code readability and facilitate software maintenance, program methods must be named properly. In particular, method names must be consistent with the corresponding method implementations. Debugging method names remains an important topic in the literature, where various approaches analyze commonalities among method names in a large dataset to detect inconsistent method names and suggest better ones. We note that the state-of-the-art does not analyze the implemented code itself to assess consistency. We thus propose a novel automated approach to debugging method names based on the analysis of consistency between method names and method code. The approach leverages deep feature representation techniques adapted to the nature of each artifact.

3. Semantic fuzzing with zest: Rohan Padhye, Caroline Lemieux, Koushik Sen, Mike Papadakis, Yves Le Traon. Proceedings of the 28th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2019) - Distinguished Artifact award ISSTA 2019.
   Programs expecting structured inputs often consist of both a syntactic analysis stage, which parses raw input, and a semantic analysis stage, which conducts checks on the parsed input and executes the core logic of the program. Generator-based testing tools in the lineage of QuickCheck are a promising way to generate random syntactically valid test inputs for these programs. We present Zest, a technique which automatically guides QuickCheck-like random input generators to better explore the semantic analysis stage of test programs. Zest converts random-input generators into deterministic parametric generators. We present the key insight that mutations in the untyped parameter domain map to structural mutations in the input domain. Zest leverages program feedback in the form of code coverage and input validity to perform feedback-directed parameter search. Zest is the most effective technique in finding these bugs reliably and quickly, requiring at most 10 minutes on average to find each bug of the existing benchmarks.

4. Search-based test and improvement of machine-learning-based anomaly detection systems: Maxime Cordy, Steve Muller, Mike Papadakis, Yves Le Traon. Proceedings of the 28th ACM SIGSOFT International Symposium on Software Testing and Analysis.
   Machine-learning-based anomaly detection systems can be vulnerable to new kinds of deceptions, known as training attacks, which exploit the live learning mechanism of these systems by progressively injecting small portions of abnormal data. The injected data seamlessly swift the learned states to a point where harmful data can pass unnoticed. We focus on the systematic testing of these attacks in the context of intrusion detection systems (IDS). We propose a search-based approach to test IDS by

making training attacks. Going a step further, we also propose searching for countermeasures, learning from the successful attacks and thereby increasing the resilience of the tested IDS. By co-evolving our attack and defence mechanisms we succeeded at improving the defence of the IDS under test by making it resilient to 49 out of 50 independently generated attacks.

4.17 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 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 2019

In 2019, the works were focused towards research on distributed grid support, curtailment and hosting capacity enhancement. Both overcurrent and overvoltage constraints are being investigated for the complete subsets of radial and meshed MV-grid configurations, laying the ground for the cooperative control methods including droops and fair curtailment references. The complete subset analysis guarantees supply security within the tolerances required, while maintaining reconfiguration freedom of the grid operator. The work has been presented in the SEST2019 conference by the PhD candidate K. Torchyan. The research continues on the development of extended droop control for PV integration in the medium voltage grids.

Within the scope of Erasmus+ project, the group has hosted an intern student, M. F. Koc working on the development of a 43-bus representation of Luxembourg's medium voltage grid model, under the supervision of Prof. J. Sachau and K Torchyan.

Cooperation with Eurosolar and the Swiss Solar Agency have been continued with Prof. Sachau as member of the Norman Foster committee and the European Solarprize committee. During the winter semester, he has been seconded to JRC Ispra contributing to the field of EU electrical energy security.

Most interesting achievements in 2019

1. SEST 2019 paper presentation: K. Torchyan and J. Sachau, "Increasing DG Integration Level by Network Configuration Subset Analysis," 2019 International Conference on Smart Energy Systems and Technologies (SEST),

Porto, Portugal, 2019, pp. 1-6. doi: 10.1109/SEST.2019.8848994.
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. Grid-wide voltage profile, overloading of substation transformers and overloading of lines may become bottlenecks for largescale integration of PV plants. Here, measures to avoid cost-intensive network reinforcement are of interest. In this paper, analysis of grid reconfiguration and its impact on hosting capacity (HC) and grid operation are studied. Additionally, several PV control scenarios are considered according to current grid codes and grid code enhancement suggestions are made. The study is performed on a 43-bus 20 kV MV network model representative of Luxembourg's grid structure. 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 approximately four times compared to the worst configuration and the grid code improvement can further increase the HC by another 15%, depending on the configuration.

2. 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 programs, 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 long-term energy-economical needs: accommodation of large-scale fluctuating electricity feed-in transition to solar electrical mobility & transport corresponding integration of storage portfolios under techno-economical and supply-security conditions. The works aim at reinforcing techno-scientific know-how in energy-security, complementing recent progress financed by the university, Luxembourg's net-work operator CREOS and the FNR, for sustainable integration of distributed electricity generation in Luxembourg.

4.18 Team Leprévost

Head of research group: Prof. Dr. Franck Leprévost

Summary of the group's achievements in 2019

A series of organizational events occurred during the year 2019. The departure of Nicolas Bernard (in December 2019) on the one hand and the arrival (in September 2019) of Raluca Chitic as a PhD student on the other hand had an impact on this year's activities and are likely to have an impact on next year's as well. We needed to organize the transfer of knowledge between people, to finalize some activities, reschedule some others due to the situation. The scientific focus was on evolutionary algorithms and their usage to fool neural networks for image recognition. A series of experiments were (and are) conducted on the HPC for this purpose. Despite the reorganization of the small team, a paper was finalized and is accepted for publication (in 2020).

Moreover, the French version of the book entitled "the clash of universities?" by Franck Leprévost was completed during the second half of 2019. It was sent to prominent readers to get their feedback and comments. A revised version is currently finalized, and discussions are on-going with potential editors (for a publication in 2020 if things work out).

CSC asked Prof Leprévost to coordinate the CSC cluster activities in the context of the teaching evaluation 2020. This time and energy-consuming task was performed during the second half of 2019 and continues during 2020.

Talks:

- OLA'2019 International Conference on Optimization and Learning (Bangkok, Thailand, Jan 29-31, 2019):
  - Invited plenary talk F. Leprévost: "Malevich's painted squares and the Birch and Swynnerton-Dyer conjecture".
  - Session "Learning based optimization", talk F. Leprévost (joined work with N. Bernard): "How evolutionary algorithms and information hiding deceive machines and humans for image recognition – A research program"
- Colloque ADGS (Toulouse, France, 20-21 June, 2019): Invited talk F. Leprévost: "Internationalisation des universités: pour quoi faire?"
- Conférence DGESI-DGRI (Paris, France, 5/11/2019): Invited talk F. Leprévost: "La France et *the making of world-class universities*"

Most important publications

1. Nicolas Bernard and Franck Leprévost: "How evolutionary algorithms and information hiding deceive machines for image recognition: A research program". Proceedings of the OLA'2019 Int. Conf. on Optimization and Learning, pp. 12-15, Bangkok, Thailand.

2. Nicolas Bernard and Franck Leprévost: "Evolutionary Algorithms for Convolutional Neural Network Visualisation". In Meneses E., Castro H., Bar-

rios Hernández C., Ramos-Pollan R. (eds) High Performance Computing. CARLA 2018. Communications in Computer and Information Science, vol. 979. Springer, Cham pp. 18-32

3. Franck Leprévost: “Le choc des universités? Esquisse d’une dynamique en matière de géostratégie du savoir académique”. Work in progress.

4. Raluca Chitic, Nicolas Bernard and Franck Leprévost: “A proof of concept to deceive humans and machines at image classification with evolutionary algorithms”. To appear in the ACIIDS 2020 Proceedings.

4.19 Team Müller

Volker Müller and his small research team are interested in algorithmic aspects of common number-theoretic problems. Together with his assistant Jim Barthel, a paper on specific properties of integral binary quadratic forms has been submitted for publication (decision pending). Research on Simultaneous Chinese Remaindering (S-CR), a generalization of the well-known Chinese Remainder Theorem popular in number theory, has led to both new theoretical results on solution bounds and a graph-based algorithm for finding certain solutions. Currently, the new algorithm is implemented and tested in practice to better understand its practical usability (very large directed graphs are involved in the algorithm). In addition, Jim Barthel is examining the relationship of the “Lonely Runner Problem” from number theory with S-CR.

During this research, it became clear that techniques used in the solution algorithm for S-CR show strong similarities with other number-theoretic problems like integer factorization or possibly even the discrete logarithm problem modulo primes. A new, still unpublished, algorithm for integer factorization is currently under development and implementation. Again, the practical relevance of this new algorithm is still unclear and will be researched in the coming months, before a publication about this result is planned.

As programme director of the “Bachelor in Applied Information Technology” and its life-long learning variant “Bachelor in Applied Information Technology – Continuing Education Programme”, Volker Müller was strongly involved in smooth organization of the two programmes and continuous programme adaptions for a better reflection of the professional needs in Luxembourg.

CHAPTER 5

Organizational Structure

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

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

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

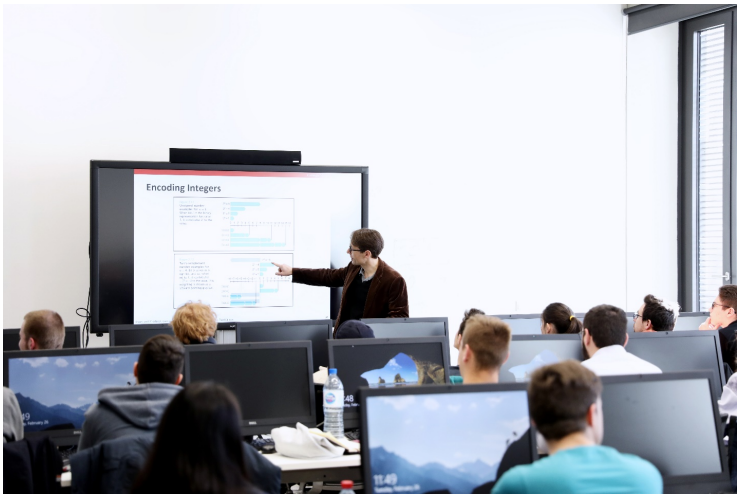
- There are three hierarchical levels within CSC: CSC (all members of CSC) + LAB (a substructure of CSC) + GRP (a research group consisting of a CSC professor and his team members).
  The duties, responsibilities and organization of a department and the tasks and duties of individual professors (and 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 groups are named after their main topic(s) of study.

- 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.
- The 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.

CHAPTER 6

Education



6.1 Doctoral Programme in Computer Science and Computer Engineering

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

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

Altogether there were approximately 180 doctoral candidates in the doctoral programme in 2019.

6.2 Master in Information and Computer Sciences (MiCS)

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

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

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

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

In 2019 there were around 90 students from more than 30 countries in the MICS.

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

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

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

In 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”.

6.4 Interdisciplinary Space Master

The growing research and innovation in space exploration and exploitation will require university graduates who are prepared to contribute to this growing and dynamic industry. In Luxembourg, the space industry includes telecommunications and broadcast services as well as manufacturers and systems operators. This industry offers career opportunities across multiple disciplines. In addition to these industrial sectors, two public research organizations, the Luxembourg Institute of Science and Technology and the University of Luxembourg, are also developing space research activities.

The domains covered by industry and the public research institutes include

- The space segment comprising manufacturing of satellite and instrument structures, electronic equipment and systems integration for micro-satellites.
- The ground segment, consisting of ground station development, mechanical and electrical ground support equipment, and communication networks.
- The service segment, embracing teleport, satellite broadband, risk management and automatic identification system (AIS) services.

To respond to a growing need for people educated to contribute to these fields in Luxembourg and Europe, we propose a master level study track, the “Interdisciplinary Space Master” (ISM). The UL will partner with Luxembourg and European industrial and government actors in the area of space research to undertake this study track.

Through a project-based learning approach, graduates will obtain a fundamental understanding of the science that motivates space sector industry and what is technically required to establish and manage space missions. Students will also learn computer skills required to interpret observations from space (big data; machine learning, artificial intelligence). In addition, the graduates will be educated in the business, entrepreneurial, finance, and legal aspects required to develop start-ups that will contribute to the value chain for space exploration and exploitation in Luxembourg. The space value chain is a commercial space venture that includes commercial or research operations on the Moon and near-Earth asteroids.

More specifically, courses will touch upon space systems engineering, space operations, space data mining and intelligent systems, satellite communications, and robotics. Theoretical concepts in business, entrepreneurship, finance and project management are also components of the study programme. These lectures will be delivered by UL professors, LIST researchers, and industrial experts having significant experience working in the space sector. In the fourth semester of the master, the students will be placed in internships with industry, the UL, or LIST.

The first four-years of the programme will be supported by the Luxembourg Ministry of the Economy (MECO). The funding will support 1) the establishment

of two laboratories to support project-based learning and 2) three professors (preferably experts in the space sector) who will contribute to further developing the study programme and research in the field.

The ISM is designed to be scalable meaning that as research, expertise, and interest in space topics at the UL and LIST evolve, the master will offer different tracks in the third semester to allow students to focus on either more technical, more business, or more computer science.

The programme has been preliminarily reviewed by CEOs in the industrial space-sector (Arianespace, Thales Alenia, Airbus, Boeing, OHB, and SES) and has received their endorsement, i.e. all agree that they would be happy to hire graduates with this type of education.

6.5 Bachelor in Computer Science (BiCS)

The Computer Science and Communication research offers a 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.

The figures for academic year 2018/2019 are:

- 89 total applicants (24% female, 76% male)
- admission rate: 60%
- high school degrees: 90% classic, 10% vocational
- high school country: 51% Luxembourg
- 77 currently registered to the program (39 first year, 23 second year, 15 third year)

6.6 Bachelor in Applied Information Technology (BINFO)

The "Bachelor in Applied Information Technology" (BINFO) offers a practice-oriented study programme that provides 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 continuous 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 2019-2020, a total of 135 students are registered within the BINFO program (73 in the first year, 22 in the second, and 40 students in the

third year). The number of BINFO graduates in 2019 is 18. More information on the programme can be found at https://binfo.uni.lu.

6.7 Bachelor in Applied Information Technology – Continuous Education Programme (BINFO-CEP)

The "Bachelor in Applied Information Technology – Continuous Education Programme" (BINFO-CEP) offers a practice-oriented part-time study programme that corresponds to the needs of the Luxembourgish labor market for continued professional development. The programme is organized in cooperation with the Lifelong Learning Center of the Chambre des Salaires (CSL). 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-CEP 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 continuous training and further professional development during their future professional career. Beyond technical training in practically relevant IT-related technologies, BINFO-CEP 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-CEP 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, blockchains, 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 2019-2020, a total of 27 students are registered within the BINFO-CEP program (8 in the first, 19 students in the second/third year). The number of BINFO-CEP graduates in 2019 is 10. More information on the programme can be found at https://binfo-fc.uni.lu.

6.8 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. Please note that the list of books includes those where a CSC member contributed as an editor.

Publication Category	**Quantity**	**Section**
Books	10	A.1 (p.54)
Book Chapters	12	A.2 (p.54)
Journal Articles	83	A.3 (p.56)
Conference Papers	159	A.4 (p.64)
Theses	24	A.5 (p.80)
Total	*288*	

Table A.1: Overview of publications per category

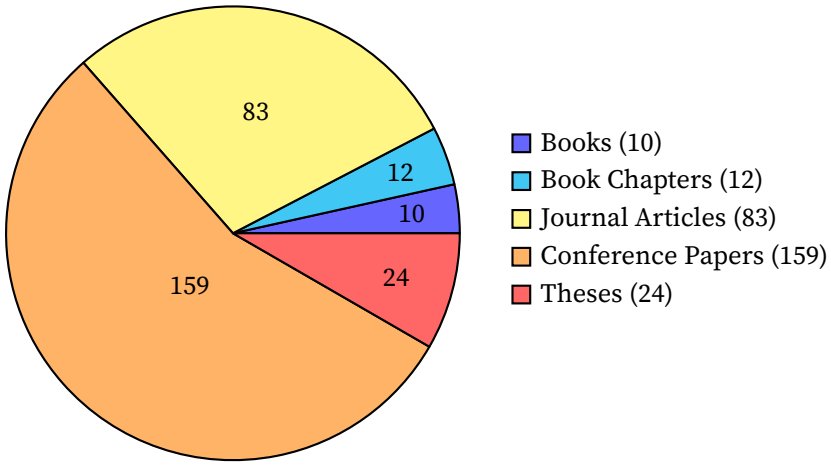


Figure A.1: Distribution of Types of Publications

A.1 Books

[1] Michael Abraham, Israel Belfer, and Dov M. Gabbay. *Theories of Joint Ownership in Talmudic Logic (Hebrew)*. Collge Publications, 2019. URL: http://hdl.handle.net/10993/42676.

[2] Francesca Arcelli, Bartosz Walter, Apostolos Ampatzoglou, Fabio Palomba, Gilles Perrouin, Mathieu Acher, et al., eds. *Proceedings of the 3rd ACM SIGSOFT International Workshop on Machine Learning Techniques for Software Quality Evaluation*. ACM, 2019. URL: http://hdl.handle.net/10993/42059.

[3] Nahla Ben Amor, Benjamin Quost, and Martin Theobald, eds. *Scalable Uncertainty Management - 13th International Conference (SUM 2019), Compiegne, France, December 16-18, 2019, Proceedings*. Springer, 2019. ISBN: 978-3-030-35513-5. URL: http://hdl.handle.net/10993/41709.

[4] Christoph Benzmüller, Xavier Parent, and Alexander Steen, eds. *Selected Student Contributions and Workshop Papers of LuxLogAI 2018*. EasyChair, 2019. URL: http://hdl.handle.net/10993/40249.

[5] Christoph Benzmüller and Heiner Stuckenschmidt, eds. *KI 2019: Advances in Artificial Intelligence – 42nd German Conference on AI, Kassel, Germany, September 23-26, 2019, Proceedings*. Springer, Cham, Cham, 2019. DOI: 10.1007/978-3-030-30179-8. URL: http://hdl.handle.net/10993/40543.

[6] 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, 2019. ISBN: 978-2-1008-0089-6. URL: http://hdl.handle.net/10993/42081.

[7] Sviatlana Höhn. *Artificial Companion for Second Language Conversation*. Springer International Publishing, 2019. ISBN: 978-3-030-15504-9. DOI: 10.1007/978-3-030-15504-9. URL: http://hdl.handle.net/10993/39689.

[8] Sjouke Mauw and Mauro Conti, eds. *Proceedings of the 15th International Workshop on Security and Trust Management (STM 2019)*. Springer, 2019. URL: http://hdl.handle.net/10993/41604.

[9] Jun Pang and Jing Sun, eds. *Proceedings of the 24th International Conference on Engineering of Complex Computer Systems*. IEEE, 2019. URL: http://hdl.handle.net/10993/40846.

[10] Ahmet Soylu, Sotiris Moschoyiannis, Guido Governatori, Mantas Simkus, Petros Stefaneas, Alexander Steen, et al., eds. *RuleML+RR 2019 Doctoral Consortium and Rule Challenge*. CEUR-WS.org, 2019. URL: http://hdl.handle.net/10993/40368.

A.2 Book Chapters

[11] Jean Botev, Anthony Stein, and Sven Tomforde. “7th International Workshop on Self-Optimisation in Autonomic and Organic Computing Sys-

tems". In: *ARCS 2019 Workshop Proceedings*. VDE Verlag, 2019. URL: http://hdl.handle.net/10993/41904.

[12] Pascal Bouvry, Sébastien Varrette, Muhammad Umer Wasim, Abdallah Ali Zainelabden Abdallah Ibrahim, Xavier Besseron, T. A. Trinh, et al. "Security, reliability and regulation compliance in Ultrascale Computing System". In: *Ultrascale Computing Systems*. Ed. by J. Carretero and E. Jeannot. IET, 2019, pp. 65–83. ISBN: 978-178-5618-33-8. DOI: 10.1049/pbpc024e_ch3. URL: http://hdl.handle.net/10993/36371.

[13] Katarina Britz, Giovanni Casini, Thomas Meyer, Ivan Varzinczak, Anni-Yasmin Turhan, and Frank Wolter. "A KLM Perspective on Defeasible Reasoning for Description Logics". In: *Description Logic, Theory Combination, and All That - Essays Dedicated to Franz Baader on the Occasion of His 60th Birthday*. Ed. by Carsten Lutz, Uli Sattler, and Cesare Tinelli. Springer, 2019, pp. 147–173. ISBN: 978-3-030-22101-0. DOI: 10.1007/978-3-030-22102-7. URL: http://hdl.handle.net/10993/40666.

[14] Jérémie Dauphin, Marcos Cramer, and Leendert van der Torre. "A dynamic approach for combining abstract argumentation semantics". In: *Dynamics, Uncertainty and Reasoning*. Springer, 2019, pp. 21–43. URL: http://hdl.handle.net/10993/41184.

[15] Fletcher, Martin Theobald, Sharif Sakr, and Albert Y. Zomaya. "Indexing for Graph Query Evaluation". In: *Encyclopedia of Big Data Technologies*. Springer, 2019. ISBN: 978-3-319-63962-8. URL: http://hdl.handle.net/10993/41708.

[16] David Fuenmayor and Christoph Benzmüller. "A Computational-Hermeneutic Approach for Conceptual Explicitation". In: *Model-Based Reasoning in Science and Technology – Inferential Models for Logic, Language, Cognition and Computation*. Ed. by A. Nepomuceno, L. Magnani, F. Salguero, C. Bares, and M. Fontaine. Springer, 2019, pp. 441–469. ISBN: 978-3-030-32721-7. DOI: 10.1007/978-3-030-32722-4_25. URL: http://hdl.handle.net/10993/40905.

[17] Dov M. Gabbay, Marcos Cramer, Jérémie Dauphin, Ali Farjami, Lydia Rivlin, and Leon van der Torre. "Machine Argumentation. Can We Replace Taxi Drivers by Robots?" In: *Natural Argument, A tribute to John Woods*. College Publications, 2019. URL: http://hdl.handle.net/10993/42683.

[18] Dov M. Gabbay and Michael Gabbay. "Argumentation as information input". In: *Argumentation-based Proofs of Endearment*. College Publications, 2019. URL: http://hdl.handle.net/10993/42681.

[19] Gabriele Lenzini and Marinella Petrocchi. "Modelling of Railways Signalling System Requirements by Controlled Natural Languages: A Case Study". In: *From Software Engineering to Formal Methods and Tools, and Back*. Springer, Cham, 2019, pp. 502–518. ISBN: 978-3-030-30984-8. DOI: 10.1007/978-3-030-30985-5_29. URL: http://hdl.handle.net/10993/40645.

[20] Ariel Oleksiak, Laurent Lefèvre, Pedro Alonso, Georges Da Costa, Vincenzo De Maio, Neki Frasheri, et al. “Energy aware ultrascale systems”. In: *Ultrascale Computing Systems*. Ed. by J. Carretero, E. Jeannot, and A.Y. Zomaya. IET, 2019, pp. 127–188. ISBN: 978-178-5618-33-8. URL: http://hdl.handle.net/10993/42067.

[21] Anne-Cecile Orgerie, Sébastien Varrette, and A. Y Zomaya. “A Full-Cost Model for Estimating the Energy Consumption of Computing Infrastructures”. In: *Ultrascale Computing Systems*. Ed. by J. Carretero and E. Jeannot. IET, 2019, pp. 161–176. ISBN: 978-178-5618-33-8. DOI: 10.1049/pbpc024e_ch5. URL: http://hdl.handle.net/10993/36377.

[22] Arianna Rossi and Monica Palmirani. “DaPIS: an Ontology-Based Data Protection Icon Set”. In: *Knowledge of the Law in the Big Data Age*. Ed. by Ginevra Peruginelli and Sebastiano Faro. IOS Press, 2019, pp. 181–195. ISBN: 978-1-61499-984-3 || 978-1-61499-985-0. URL: http://hdl.handle.net/10993/40117.

A.3 Journal Articles

[23] Nuno Amalio, Lionel Briand, and Pierre Kelsen. “An experimental scrutiny of visual design modelling: VCL up against UML+OCL”. In: *Empirical Software Engineering* (2019). DOI: 10.1007/s10664-019-09784-9. URL: http://hdl.handle.net/10993/41995.

[24] Alexandre Bartel, Jacques Klein, and Yves Le Traon. “MUSTI: Dynamic Prevention of Invalid Object Initialization Attacks”. In: *IEEE Transactions on Information Forensics and Security* (2019). URL: http://hdl.handle.net/10993/42590.

[25] Cesare Bartolini and Gabriele Lenzini. “Sistemi Medici e Conformità Legale”. In: *Rivista Italiana di Medicina Legale: Dottrina, Casistica, Ricerca Sperimentale, Giurisprudenza e Legislazione* XLI (2019), pp. 225–242. URL: http://hdl.handle.net/10993/40575.

[26] Cesare Bartolini, Gabriele Lenzini, and Livio Robaldo. “The DAta Protection REgulation COmpliance Model”. In: *IEEE Security and Privacy* 17 (2019), pp. 37–45. DOI: 10.1109/MSEC.2019.2937756. URL: http://hdl.handle.net/10993/40980.

[27] Cesare Bartolini, Gabriele Lenzini, and Cristiana Santos. “An Agile Approach to Validate a Formal Representation of the GDPR”. In: *International Symposium on Artificial Intelligence* 11717 (2019). URL: http://hdl.handle.net/10993/40576.

[28] Alexis Baudin, Soumya Paul, Cui Su, and Jun Pang. “Controlling large Boolean networks with single-step perturbations”. In: *Bioinformatics* 35 (2019), pp. i558–i567. DOI: 10.1093/bioinformatics/btz371. URL: http://hdl.handle.net/10993/39934.

[29] Christof Beierle, Alex Biryukov, and Aleksei Udovenko. “On degree-d zero-sum sets of full rank”. In: *Cryptography and Communications* (2019), pp. 1–26. DOI: 10.1007/s12095-019-00415-0. URL: http://hdl.handle.net/10993/41002.

[30] Christof Beierle, Gregor Leander, Amir Moradi, and Shahram Rasoolzadeh. "CRAFT: Lightweight Tweakable Block Cipher with Efficient Protection Against DFA Attacks". In: *IACR Transactions on Symmetric Cryptology* 2019 (2019), pp. 5–45. DOI: 10.13154/tosc.v2019.i1.5-45. URL: http://hdl.handle.net/10993/39112.

[31] Christoph Benzmüller. "Universal (Meta-)Logical Reasoning: The Wise Men Puzzle (Isabelle/HOL Dataset)". In: *Data in Brief* 24 (2019), pp. 1–5. DOI: 10.1016/j.dib.2019.103823. URL: http://hdl.handle.net/10993/40544.

[32] Christoph Benzmüller and Peter Andrews. "Church's Type Theory". In: *Stanford Encyclopedia of Philosophy* (2019), 1–62 (in pdf version). URL: http://hdl.handle.net/10993/40548.

[33] Christoph Benzmüller, Ali Farjami, Paul Joseph Yves Meder, and Xavier Parent. "I/O Logic in HOL". In: *Journal of Applied Logics – IfCoLoG Journal of Logics and their Applications (Special Issue on Reasoning for Legal AI)* 6 (2019), pp. 715–732. URL: http://hdl.handle.net/10993/41332.

[34] Christoph Benzmüller, Ali Farjami, and Xavier Parent. "Åqvist's Dyadic Deontic Logic E in HOL". In: *Journal of Applied Logics – IfCoLoG Journal of Logics and their Applications (Special Issue on Reasoning for Legal AI)* 6 (2019), pp. 733–755. URL: http://hdl.handle.net/10993/41333.

[35] Christoph Benzmüller, Xavier Parent, and Francesco Ricca. "Report on the Second International Joint Conference on Rules and Reasoning". In: *AI Magazine* 40 (2019), pp. 73–74. DOI: 10.1609/aimag.v40i2.2888. URL: http://hdl.handle.net/10993/40950.

[36] Christoph Benzmüller and Dana Scott. "Automating Free Logic in HOL, with an Experimental Application in Category Theory". In: *Journal of Automated Reasoning* (2019). DOI: 10.1007/s10817-018-09507-7. URL: http://hdl.handle.net/10993/37593.

[37] Alex Biryukov and Daniel Feher. "ReCon: Sybil-Resistant Consensus from Reputation". In: *Pervasive and Mobile Computing* (2019). DOI: 10.1016/j.pmcj.2019.101109. URL: http://hdl.handle.net/10993/41325.

[38] Alex Biryukov and Sergei Tikhomirov. "Security and Privacy of Mobile Wallet Users in Bitcoin, Dash, Monero, and Zcash". In: *Pervasive and Mobile Computing* (2019). URL: http://hdl.handle.net/10993/39729.

[39] Gedare Bloom, Gianluca Cena, Ivan Cibrario Bertolotti, Tingting Hu, Nicolas Navet, and Adriano Valenzano. "Event Notification in CAN-based Sensor Networks". In: *IEEE Transactions on Industrial Informatics* 15 (2019), pp. 5613–5625. DOI: 10.1109/TII.2019.2904082. URL: http://hdl.handle.net/10993/40221.

[40] Nils Bulling, Wojciech Jamroga, and Matei Popovici. "Reasoning about Strategic Abilities: Agents with Truly Perfect Recall". In: *ACM Transactions on Computational Logic* 20 (2019), 10:1–10:46. DOI: 10.1145/3309761. URL: http://hdl.handle.net/10993/41799.

[41] Andrea Capponi, Claudio Fiandrino, Burak Kantarci, Luca Foschini, Dzmitry Kliazovich, and Pascal Bouvry. "A Survey on Mobile Crowdsensing Systems: Challenges, Solutions, and Opportunities". In: *IEEE Communications Surveys and Tutorials* 21 (2019), pp. 2419–2465. DOI: 10.1109/COMST.2019.2914030. URL: http://hdl.handle.net/10993/39438.

[42] Ilaria Castellani, Mariangiola Dezani-Ciancaglini, Paola Giannini, and Ross James Horne. "Global Types with Internal Delegation". In: *Theoretical Computer Science* (2019). DOI: 10.1016/j.tcs.2019.09.027. URL: http://hdl.handle.net/10993/41616.

[43] Gianluca Cena, Ivan Cibrario Bertolotti, Tingting Hu, and Adriano Valenzano. "On a Software-Defined CAN Controller for Embedded Systems". In: *Computer Standards & Interfaces* 63 (2019), pp. 43–51. DOI: 10.1016/j.csi.2018.11.007. URL: http://hdl.handle.net/10993/37376.

[44] Jérémy Henri J. Charlier, Radu State, and Jean Hilger. "PHom-GeM: Persistent Homology for Generative Models". In: *The 6th Swiss Conference on Data Science* (2019). URL: http://hdl.handle.net/10993/40108.

[45] Bo-Heng Chen, Cheng-Te Li, Kun-Ta Chuang, Jun Pang, and Yang Zhang. "An active learning-based approach for location-aware acquaintance inference". In: *Knowledge and Information Systems* 59 (2019), pp. 539–569. URL: http://hdl.handle.net/10993/39246.

[46] Benoît-Michel Cogliati and Titouan Tanguy. "Multi-user Security Bound for Filter Permutators in the Random Oracle Model". In: *Designs, Codes and Cryptography* (2019). URL: http://hdl.handle.net/10993/42327.

[47] Maxime Cordy and Axel Legay. "Verification and abstraction of real-time variability-intensive systems". In: *International Journal on Software Tools for Technology Transfer* 21 (2019), pp. 635–649. URL: http://hdl.handle.net/10993/42020.

[48] Jean-Sébastien Coron and Agnese Gini. "Improved Cryptanalysis of the AJPS Mersenne Based Cryptosystem". In: *Journal of Mathematical Cryptology* (2019). DOI: 10.1515/jmc-2019-0027. URL: http://hdl.handle.net/10993/42886.

[49] Marcos Cramer and Jérémie Dauphin. "A Structured Argumentation Framework for Modeling Debates in the Formal Sciences". In: *Journal for General Philosophy of Science* (2019), pp. 1–23. DOI: 10.1007/s10838-019-09443-z. URL: http://hdl.handle.net/10993/41181.

[50] Thierry Derrmann, Raphaël Frank, Francesco Viti, and Thomas Engel. "How Road and Mobile Networks Correlate: Estimating Urban Traffic Using Handovers". In: *IEEE Transactions on Intelligent Transportation Systems* (2019). URL: http://hdl.handle.net/10993/39292.

[51] Joseph Emeras, Sébastien Varrette, Valentin Plugaru, and Pascal Bouvry. "Amazon Elastic Compute Cloud (EC2) versus In-House HPC Platform: A Cost Analysis". In: *IEEE Transactions on Cloud Computing* 7 (2019), pp. 456–468. DOI: 10.1109/TCC.2016.2628371. URL: http://hdl.handle.net/10993/42068.

[52] Saharnaz Esmaeilzadeh Dilmaghani, Matthias R. Brust, Apivadee Piyatumrong, Grégoire Danoy, and Pascal Bouvry. "Link Definition ameliorating Community Detection in Collaboration Networks". In: *Frontiers in Big Data* 2 (2019), p. 22. URL: http://hdl.handle.net/10993/41511.

[53] Eric Falk, Vendel Toth, Alexandre Knaff, and Radu State. "A Tale of Location-Based User Authentication". In: *IEEE BigComp2019 - The 6th IEEE International Conference on Big Data and Smart Computing* (2019). URL: http://hdl.handle.net/10993/37862.

[54] Maria Fernandes, Jérémie Decouchant, Marcus Volp, Francisco Couto, and Paulo Verissimo. "DNA-SeAl: Sensitivity Levels to Optimize the Performance of Privacy-Preserving DNA Alignment". In: *IEEE Journal of Biomedical and Health Informatics* (2019). DOI: 10.1109/JBHI.2019.2914952. URL: http://hdl.handle.net/10993/40046.

[55] Claudio Fiandrino, Nicholas Allio, Dzmitry Kliazovich, Paolo Giaccone, and Pascal Bouvry. "Profiling Performance of Application Partitioning for Wearable Devices in Mobile Cloud and Fog Computing". In: *IEEE Access* 7 (2019), pp. 12156–12166. DOI: 10.1109/ACCESS.2019.2892508. URL: http://hdl.handle.net/10993/42077.

[56] Georgios Fotiadis and Elisavet Konstantinou. "TNFS Resistant Families of Pairing-Friendly Elliptic Curves". In: *Theoretical Computer Science* 800 (2019), pp. 73–89. URL: http://hdl.handle.net/10993/39265.

[57] Dov M. Gabbay, Uri Schild, and Esther David. "The Talmudic Logic Project, Ongoing Since 2008". In: *Logica Universalis* 13 (2019), pp. 425–442. URL: http://hdl.handle.net/10993/42682.

[58] Loïc Gammaitoni and Pierre Kelsen. "F-Alloy: a relational model transformation language based on Alloy". In: *Software & Systems Modeling* 18 (2019), pp. 213–247. URL: http://hdl.handle.net/10993/33261.

[59] Reynaldo Gil-Pons, Yunior Ramirez Cruz, Rolando Trujillo-Rasua, and Ismael G. Yero. "Distance-based vertex identification in graphs: The outer multiset dimension". In: *Applied Mathematics and Computation* 363 (2019), p. 124612. DOI: 10.1016/j.amc.2019.124612. URL: http://hdl.handle.net/10993/40570.

[60] Christian Grevisse, Steffen Rothkugel, and Robert Reuter. "Scaffolding support through integration of learning material". In: *Smart Learning Environments* 6 (2019). DOI: 10.1186/s40561-019-0107-0. URL: http://hdl.handle.net/10993/41409.

[61] Ross James Horne and Alwen Tiu. "Constructing weak simulations from linear implications for processes with private names". In: *Mathematical Structures in Computer Science* (2019). DOI: 10.1017/S0960129518000452. URL: http://hdl.handle.net/10993/41632.

[62] Ross James Horne, Alwen Tiu, Bogdan Aman, and Gabriel Ciobanu. "De Morgan Dual Nominal Quantifiers Modelling Private Names in Non-Commutative Logic". In: *ACM Transactions on Computational Logic* 20 (2019), 22:1–22:44. DOI: 10.1145/3325821. URL: http://hdl.handle.net/10993/41612.

[63] Wojciech Jamroga, Micha L Knapik, Damian Kurpiewski, and Lukasz Mikulski. “Approximate Verification of Strategic Abilities under Imperfect Information”. In: *Artificial Intelligence* 277 (2019). DOI: 10.1016/j.artint.2019.103172. URL: http://hdl.handle.net/10993/41791.

[64] Wojciech Jamroga, Vadim Malvone, and Aniello Murano. “Natural Strategic Ability”. In: *Artificial Intelligence* 277 (2019). DOI: 10.1016/j.artint.2019.103170. URL: http://hdl.handle.net/10993/41793.

[65] Georgios Kaiafas, Christian Hammerschmidt, Sofiane Lagraa, and Radu State. “Auto Semi-supervised Outlier Detection for Malicious Authentication Events”. In: *ECML PKDD 2019 Workshops* (2019). URL: http://hdl.handle.net/10993/39981.

[66] Emmanuel Kieffer, Grégoire Danoy, Pascal Bouvry, and Anass Nagih. “Tackling Large-Scale and Combinatorial Bi-level Problems with a Genetic Programming Hyper-heuristic”. In: *IEEE Transactions on Evolutionary Computation* (2019). URL: http://hdl.handle.net/10993/39737.

[67] Daniel Kirchner, Christoph Benzmüller, and Edward N. Zalta. “Computer Science and Metaphysics: A Cross-Fertilization”. In: *Open Philosophy* 2 (2019), pp. 230–251. DOI: 10.1515/opphil-2019-0015. URL: http://hdl.handle.net/10993/40546.

[68] Daniel Kirchner, Christoph Benzmüller, and Edward N. Zalta. “Mechanizing Principia Logico-Metaphysica in Functional Type Theory”. In: *Review of Symbolic Logic* (2019), pp. 1–13. DOI: 10.1017/S1755020319000297. URL: http://hdl.handle.net/10993/40542.

[69] Michal Knapik, Étienne André, Laure Petrucci, Wojciech Jamroga, and Wojciech Penczek. “Timed ATL: Forget Memory, Just Count”. In: *Journal of Artificial Intelligence Research* 66 (2019), pp. 197–223. DOI: 10.1613/jair.1.11612. URL: http://hdl.handle.net/10993/41794.

[70] Niklas Kolbe, Sylvain Kubler, Jérémy Robert, Yves Le Traon, and Arkady Zaslavsky. “Linked Vocabulary Recommendation Tools for Internet of Things: A Survey”. In: *ACM Computing Surveys* (2019). URL: http://hdl.handle.net/10993/37518.

[71] David Kozhaya, Jérémie Decouchant, and Paulo Verissimo. “RT-ByzCast: Byzantine-Resilient Real-Time Reliable Broadcast”. In: *IEEE Transactions on Computers* 68 (2019). DOI: 10.1109/TC.2018.2871443. URL: http://hdl.handle.net/10993/37812.

[72] Christiane Kuhn, Martin Beck, Stefan Schiffner, Eduard Jorswieck, and Thorsten Strufe. “On privacy notions in anonymous communication”. In: *Proceedings on Privacy Enhancing Technologies* 2019 (2019), pp. 105–125. DOI: 10.2478/popets-2019-0022. URL: http://hdl.handle.net/10993/40073.

[73] Daoyuan Li, Li Li, Dongsun Kim, Tegawendé François D Assise Bissyande, David Lo, and Yves Le Traon. “Watch out for This Commit! A Study of Influential Software Changes”. In: *Journal of Software: Evolution and Process* (2019). URL: http://hdl.handle.net/10993/27742.

[74] Li Li, Tegawendé François D Assise Bissyande, and Jacques Klein. "Rebooting Research on Detecting Repackaged Android Apps: Literature Review and Benchmark". In: *IEEE Transactions on Software Engineering* (2019). URL: http://hdl.handle.net/10993/41965.

[75] Li Li, Tegawendé François D Assise Bissyande, Haoyu Wang, and Jacques Klein. "On Identifying and Explaining Similarities in Android Apps". In: *Journal of Computer Science and Technology* 34 (2019), pp. 437–455. URL: http://hdl.handle.net/10993/41967.

[76] Li Li, Timothée Riom, Tegawendé François D Assise Bissyande, Haoyu Wang, Jacques Klein, and Yves Le Traon. "Revisiting the impact of common libraries for android-related investigations". In: *Journal of Systems and Software* 154 (2019), pp. 157–175. URL: http://hdl.handle.net/10993/42605.

[77] José Miguel Lopez Becerra, Vincenzo Iovino, Dimiter Ostrev, and Marjan Skrobot. "On the Relation Between SIM and IND-RoR Security Models for PAKEs with Forward Secrecy". In: *E-Business and Telecommunications - 2019* (2019), pp. 173–198. URL: http://hdl.handle.net/10993/38621.

[78] Rocio Lopez Perez, Florian Adamsky, Ridha Soua, and Thomas Engel. "Forget the Myth of the Air Gap: Machine Learningfor Reliable Intrusion Detection in SCADA Systems". In: *EAI Endorsed Transactions on Security and Safety* (2019). URL: http://hdl.handle.net/10993/40125.

[79] Hugues Mandon, Cui Su, Jun Pang, Soumya Paul, Stefan Haar, and Loic Pauleve. "Algorithms for the Sequential Reprogramming of Boolean Networks". In: *IEEE/ACM Transactions on Computational Biology and Bioinformatics* 16 (2019), pp. 1610–1619. DOI: 10.1109/TCBB.2019.2914383. URL: http://hdl.handle.net/10993/40672.

[80] Réka Markovich. ""Understanding Hohfeld and Formalizing Legal Rights: the Hohfeldian Conceptions and Their Conditional Consequences". In: *Studia Logica* (2019). URL: http://hdl.handle.net/10993/41665.

[81] Réka Markovich. "Rights and Punishment: The Hohfeldian Theory's Applicability and Morals in Understanding Criminal Law". In: *IfCoLog Journal of Logics and Their Applications* (2019). URL: http://hdl.handle.net/10993/41661.

[82] Réka Markovich. "Two Limitations in Legal Knowledge Base Constructing and Formalizing Law". In: *IfCoLog Journal of Logics and Their Applications* (2019). URL: http://hdl.handle.net/10993/41662.

[83] Sjouke Mauw, Yunior Ramirez Cruz, and Rolando Trujillo Rasua. "Robust active attacks on social graphs". In: *Data Mining and Knowledge Discovery* 33 (2019), pp. 1357–1392. DOI: 10.1007/s10618-019-00631-5. URL: http://hdl.handle.net/10993/40556.

[84] Andrzej Mizera, Jun Pang, Hongyang Qu, and Qixia Yuan. "Taming asynchrony for attractor detection in large Boolean networks". In: *IEEE/ACM Transactions on Computational Biology and Bioinformatics* 16 (2019), pp. 31–42. URL: http://hdl.handle.net/10993/38688.

[85] Andrzej Mizera, Jun Pang, and Qixia Yuan. “GPU-accelerated steady-state computation of large probabilistic Boolean networks”. In: *Formal Aspects of Computing* 31 (2019), pp. 27–46. DOI: 10.1007/s00165-018-0470-6. URL: http://hdl.handle.net/10993/39098.

[86] Jedrzej Musial, Emmanuel Kieffer, Mateusz Guzek, Grégoire Danoy, Shyam Sharan Wagle, Pascal Bouvry, et al. “Cloud Brokering with Bundles: Multi-objective Optimization of Services Selection”. In: *Foundations of Computing and Decision Sciences* (2019). DOI: 10.2478/fcds-2019-0020. URL: http://hdl.handle.net/10993/42578.

[87] Robert Norvill, Beltran Fiz Pontiveros, Radu State, and Andrea Cullen. “Standardising smart contracts: Automatically inferring ERC standards”. In: *Proceedings of 2019 IEEE International Conference on Blockchain and Cryptocurrency* (2019). DOI: 10.1109/BLOC.2019.8751350. URL: http://hdl.handle.net/10993/40024.

[88] Katerina Papaioannou, Martin Theobald, and Michael H. Böhlen. “Generalized Lineage-Aware Temporal Windows: Supporting Outer and Anti Joins in Temporal-Probabilistic Databases”. In: *CoRR* abs/1902.04379 (2019). URL: http://hdl.handle.net/10993/42586.

[89] Katerina Papaioannou, Martin Theobald, and Michael H. Böhlen. “Lineage-Aware Temporal Windows: Supporting Set Operations in Temporal-Probabilistic Databases”. In: *CoRR* abs/1910.00474 (2019). URL: http://hdl.handle.net/10993/42582.

[90] Andrew Paverd, Marcus Volp, Ferdinand Brasser, Matthias Schunter, N Asokan, Ahmad-Reza Sadeghi, et al. “Sustainable Security and Safety: Challenges and Opportunities”. In: *OpenAccess Series in Informatics (OASIcs)* 73 (2019). DOI: 10.4230. URL: http://hdl.handle.net/10993/41487.

[91] Alfredo Rial. “A conditional access system with revocation for mobile pay-TV systems revisited”. In: *Information Processing Letters* 147 (2019), pp. 6–9. DOI: 10.1016/j.ipl.2019.02.010. URL: http://hdl.handle.net/10993/39946.

[92] Livio Robaldo, Cesare Bartolini, Gabriele Lenzini, Arianna Rossi, Monica Palmirani, and Michele Martoni. “Formalizing GDPR provisions in reified I/O logic: the DAPRECO knowledge base”. In: *Journal of Logic, Language and Information* (2019). URL: http://hdl.handle.net/10993/42608.

[93] Martin Rosalie, Jean-Matthieu Etancelin, André Fabbri, and Frédéric Guinand. “DACYCLEM: A decentralized algorithm for maximizing coverage and lifetime in a mobile wireless sensor network”. In: *Ad Hoc Networks* 87 (2019). DOI: 10.1016/j.adhoc.2018.12.008. URL: http://hdl.handle.net/10993/39917.

[94] Arianna Rossi, Rossana Ducato, Helena Haapio, and Stefania Passera. “When Design Met Law: Design Patterns for Information Transparency”. In: *Droit de la Consommation* (2019). URL: http://hdl.handle.net/10993/40116.

[95] Izhak Rubin, Andrea Baiocchi, Yulia Sunyoto, and Ion Turcanu. "Traffic Management and Networking for Autonomous Vehicular Highway Systems". In: *Ad Hoc Networks* 83 (2019), pp. 125–148. DOI: 10.1016/j.adhoc.2018.08.018. URL: http://hdl.handle.net/10993/36497.

[96] Nader Samir Labib, Grégoire Danoy, Jedrzej Musial, Matthias R. Brust, and Pascal Bouvry. "Internet of Unmanned Aerial Vehicles—A Multilayer Low-Altitude Airspace Model for Distributed UAV Traffic Management". In: *Sensors* 19 (2019), p. 22. DOI: 10.3390/s19214779. URL: http://hdl.handle.net/10993/41481.

[97] Donghwan Shin, Shin Yoo, Mike Papadakis, and Doo-Hwan Bae. "Empirical Evaluation of Mutation-based Test Prioritization Techniques". In: *Software Testing, Verification and Reliability* 29 (2019). URL: http://hdl.handle.net/10993/37485.

[98] Alexander Steen. "Higher-Order Theorem Proving and its Applications". In: *IT-Information Technology* 61 (2019), pp. 187–191. DOI: 10.1515/itit-2019-0001. URL: http://hdl.handle.net/10993/40250.

[99] Andrei Tchernykh, Jorge M. Cortes-Mendoza, Igor Bychkov, Alexander Feoktistov, Loic Didelot, Pascal Bouvry, et al. "Configurable Cost-Quality Optimization of Cloud-based VoIP". In: *Journal of Parallel and Distributed Computing* 133 (2019), pp. 319–336. DOI: 10.1016/j.jpdc.2018.07.001. URL: http://hdl.handle.net/10993/42079.

[100] Thierry Titcheu Chekam, Mike Papadakis, Tegawendé François D Assise Bissyande, Yves Le Traon, and Koushik Sen. "Selecting fault revealing mutants". In: *Empirical Software Engineering* (2019), pp. 1–54. DOI: 10.1007/s10664-019-09778-7. URL: http://hdl.handle.net/10993/42520.

[101] Georgios Varisteas and Raphaël Frank. "JUNIOR, A Research Platform for Connected and Automated Driving". In: *Proceedings of 2019 IEEE Vehicular Networking Conference* (2019). URL: http://hdl.handle.net/10993/41214.

[102] Qingju Wang, Honglin Hao, Yosuke Todo, Chaoyun Li, Isobe Takanori, and Willi Meier. "Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly". In: *IEEE Transactions on Computers* 68 (2019), pp. 1470–1486. DOI: 10.1109/TC.2019.2909871. URL: http://hdl.handle.net/10993/41328.

[103] Peerasak Wangsom, Kittichai Lavagnananda, and Pascal Bouvry. "Multi-Objective Scientific-Workflow Scheduling With Data Movement Awareness in Cloud." In: *IEEE Access* 7 (2019), pp. 177063–177081. DOI: 10.1109/ACCESS.2019.2957998. URL: http://hdl.handle.net/10993/42078.

[104] Jiangshan Yu, David Kozhaya, Jérémie Decouchant, and Paulo Verissimo. "RepuCoin: Your Reputation is Your Power". In: *IEEE Transactions on Computers* (2019). URL: http://hdl.handle.net/10993/38630.

[105] Qixia Yuan, Andrzej Mizera, Jun Pang, and Hongyang Qu. "A new decomposition-based method for detecting attractors in synchronous Boolean networks". In: *Science of Computer Programming* 180 (2019), pp. 18–35. URL: http://hdl.handle.net/10993/39721.

A.4 Conference Papers

[106] Madhusudan Akash, Iraklis Symeonidis, Mustafa A. Mustafa, Bart Preneel, and Ren Zhang. "SC2Share: Smart Contract for Secure Car Sharing". In: *International Conference on Information Systems Security and Privacy (ICISSP)*. 2019. URL: http://hdl.handle.net/10993/38992.

[107] Benoit Amand, Maxime Cordy, Patrick Heymans, Mathieu Acher, Paul Temple, and Jean-Marc Jézéquel. "Towards Learning-Aided Configuration in 3D Printing: Feasibility Study and Application to Defect Prediction". In: *Proceedings of the 13th International Workshop on Variability Modelling of Software-Intensive Systems, VAMOS 2019, Leuven, Belgium, February 06-08, 2019*. 2019, 7:1–7:9. ISBN: 978-1-4503-6648-9. URL: http://hdl.handle.net/10993/42058.

[108] Faouzi Amrouche, Sofiane Lagraa, Georgios Kaiafas, and Radu State. "Graph-based malicious login events investigation". In: *16th IFIP/IEEE Symposium on Integrated Network and Service Management (IM 2019)*. 2019. URL: http://hdl.handle.net/10993/39937.

[109] Aryobarzan Atashpendar, Christian Grevisse, and Steffen Rothkugel. "Enhanced Sketchnoting through Semantic Integration of Learning Material". In: *Applied Informatics*. Springer International Publishing, 2019. ISBN: 978-3-030-32474-2. URL: http://hdl.handle.net/10993/40456.

[110] Chloe M. Barnes, Kirstie Bellman, Jean Botev, Ada Diaconescu, Lukas Esterle, Christian Gruhl, et al. "CHARIOT – Towards a Continuous High-level Adaptive Runtime Integration Testbed". In: *Proceedings of the 13th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO)*. 2019. DOI: 10.1109/FAS-W.2019.00026. URL: http://hdl.handle.net/10993/40095.

[111] Francesco Belardinelli, Wojciech Jamroga, Damian Kurpiewski, Vadim Malvone, and Aniello Murano. "Strategy Logic with Simple Goals: Tractable Reasoning about Strategies". In: *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence IJCAI*. 2019, pp. 88–94. DOI: 10.24963/ijcai.2019/13. URL: http://hdl.handle.net/10993/41789.

[112] Paul-Lou Benedick, Jérémy Robert, and Yves Le Traon. "TRIDENT: A Three-Steps Strategy to Digitise an Industrial System for Stepping into Industry 4.0". In: *Proceedings of 45th Annual Conference of the IEEE Industrial Electronics Society*. 2019. URL: http://hdl.handle.net/10993/41469.

[113] Christoph Benzmüller, Srecko Kovac, and Kordula Swietorzecka. "Computational Metaphysics: New Insights on Gödel's Ontological Argument and Modal Collapse". In: *Formal Methods and Science in Philosophy III, Informal Proceedings*. 2019. URL: http://hdl.handle.net/10993/41337.

[114] Nicolas Bernard, Franck Leprévost, and Thanaruk Theeramunkong. "How Evolutionary Algorithms and Information Hiding deceive machines and humans for image recognition: A research program". In: *Proceedings of the OLA'2019 International Conference on Optimization and Learning (Bangkok, Thailand, Jan 29-31, 2019)*. Ed. by Pascal Bouvry and Piyawut Srichaikul. Springer, 2019. URL: http://hdl.handle.net/10993/40853.

[115] Marc Beunardeau, Fatima Ezzahra El Orche, Diana Maimut, David Naccache, Peter Roenne, and Peter Ryan. "Authenticated Key Distribution: When the Coupon Collector is Your Enemy". In: *Innovative Security Solutions for Information Technology and Communications*. Springer, 2019. URL: http://hdl.handle.net/10993/42594.

[116] Alex Biryukov and Daniel Feher. "Portrait of a Miner in a Landscape". In: *IEEE INFOCOM 2019 Workshop Proceedings*. 2019. URL: http://hdl.handle.net/10993/39995.

[117] Alex Biryukov and Daniel Feher. "Privacy and Linkability of Mining in Zcash". In: *2019 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2019. ISBN: 978-1-5386-7117-7. DOI: 10.1109/CNS.2019.8802711. URL: http://hdl.handle.net/10993/39996.

[118] Alex Biryukov, Daniel Feher, and Giuseppe Vitto. "Privacy Aspects and Subliminal Channels in Zcash". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Securit*. 2019. DOI: 10.1145/3319535.3345663. URL: http://hdl.handle.net/10993/41278.

[119] Alex Biryukov and García-Alfaro. "Cryptocurrencies and Blockchain Technology". In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology - ESORICS 2019 International Workshops*. Springer, 2019, pp. 173–400. ISBN: 978-3-030-31499-6. URL: http://hdl.handle.net/10993/41275.

[120] Alex Biryukov and Sergei Tikhomirov. "Deanonymization and linkability of cryptocurrency transactions based on network analysis". In: *Proceedings of 2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. 2019. URL: http://hdl.handle.net/10993/39724.

[121] Alex Biryukov and Sergei Tikhomirov. "Transaction Clustering Using Network Traffic Analysis for Bitcoin and Derived Blockchains". In: *IEEE INFOCOM 2019 Workshop Proceedings*. 2019. URL: http://hdl.handle.net/10993/39728.

[122] Jean Botev, Joe Mayer, and Steffen Rothkugel. "Immersive Mixed Reality Object Interaction for Collaborative Context-Aware Mobile Training and Exploration". In: *Proceedings of the 10th ACM Multimedia Systems Conference (MMSys)*. 2019, pp. 4–9. DOI: 10.1145/3304113.3326117. URL: http://hdl.handle.net/10993/39785.

[123] Abdelwahab Boualouache, Ridha Soua, and Thomas Engel. "SDN-based Pseudonym-Changing Strategy for Privacy Preservation in Vehicular Networks". In: *15th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'19)*. 2019. URL: http://hdl.handle.net/10993/40163.

[124] Abdelwahab Boualouache, Ridha Soua, and Thomas Engel. "VPGA: an SDN-based Location Privacy Zones Placement Scheme for Vehicular Networks". In: *38th IEEE International Performance Computing and Communications Conference (IPCCC)*. 2019. URL: http://hdl.handle.net/10993/40220.

[125] Sergiu Bursuc, Constantin-Catalin Dragan, and Steve Kremer. “Private Votes on Untrusted Platforms: Models, Attacks and Provable Scheme”. In: *Private Votes on Untrusted Platforms: Models, Attacks and Provable Scheme*. IEEE, 2019. URL: http://hdl.handle.net/10993/41899.

[126] Sergiu Bursuc and Steve Kremer. “Contingent Payments on a Public Ledger: Models and Reductions for Automated Verification.” In: *Contingent Payments on a Public Ledger: Models and Reductions for Automated Verification.* Springer, 2019. URL: http://hdl.handle.net/10993/41900.

[127] 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, 2019, pp. 1–18. ISBN: 978-3-030-06018-3. DOI: 10.1007/978-3-030-06019-0. URL: http://hdl.handle.net/10993/37224.

[128] Andrea Capponi, Piergiorgio Vitello, Claudio Fiandrino, Guido Cantelmo, Dzmitry Kliazovich, Ulrich Sorger, et al. “Crowdsensed Data Learning-Driven Prediction of Local Businesses Attractiveness in Smart Cities”. In: *IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 2019*. 2019. URL: http://hdl.handle.net/10993/39439.

[129] Luan Cardoso Dos Santos, Johann Groszschädl, and Alex Biryukov. “FELICS-AEAD: Benchmarking of Lightweight Authenticated Encryption Algorithms”. In: *Smart Card Research and Advanced Applications, 18th International Conference*. 2019. URL: http://hdl.handle.net/10993/41537.

[130] Giovanni Casini, Michael Harrison, Thomas Meyer, and Reid Swan. “Arbitrary Ranking of Defeasible Subsumption”. In: *Proceedings of the 32nd International Workshop on Description Logics*. CEUR, 2019. URL: http://hdl.handle.net/10993/39647.

[131] Giovanni Casini, Thomas Meyer, and Ivan Varzinczak. “Simple Conditionals with Constrained Right Weakening”. In: *Proceedings of the 28th International Joint Conference on Artificial Intelligence (IJCAI 2019)*. 2019, pp. 1632–1638. ISBN: 978-0-9992411-4-1. DOI: 10.24963/ijcai.2019/226. URL: http://hdl.handle.net/10993/40324.

[132] Giovanni Casini, Thomas Meyer, and Ivan Varzinczak. “Taking Defeasible Entailment beyond Rational Closure”. In: *Proceedings of the 16th European Conference on Logics in Artificial Intelligence (JELIA-19)*. Springer, 2019. ISBN: 978-3-030-19570-0. DOI: 10.1007/978-3-030-19570-0. URL: http://hdl.handle.net/10993/39594.

[133] Boonyarit Changaival, Grégoire Danoy, Dzmitry Kliazovich, Frédéric Guinand, Matthias R. Brust, Jedrzej Musial, et al. “Toward Real-world Vehicle Placement Optimization in Round-trip Carsharing”. In: *Proceedings of the Genetic and Evolutionary Computation Conference*. ACM, 2019, pp. 1138–1146. ISBN: 978-1-4503-6111-8. DOI: 10.1145/3321707.3321825. URL: http://hdl.handle.net/10993/42479.

[134] Jérémy Henri J. Charlier, Gaston Ormazabal, Radu State, and Jean Hilger. "MQLV: Optimal Policy of Money Management in Retail Banking with Q-Learning". In: *Proceedings of the Fourth Workshop on MIning DAta for financial applicationS (MIDAS 2019) co-located with the 2019 European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD 2019)*. 2019. URL: http://hdl.handle.net/10993/40331.

[135] Jérémy Henri J. Charlier, François Petit, Gaston Ormazabal, Radu State, and Jean Hilger. "Visualization of AE's Training on Credit Card Transactions with Persistent Homology". In: *Proceedings of the International Workshop on Applications of Topological Data Analysis In conjunction with ECML PKDD 2019*. 2019. URL: http://hdl.handle.net/10993/40330.

[136] Jérémy Henri J. Charlier, Radu State, and Jean Hilger. "Predicting Sparse Clients' Actions with CPOPT-Net in the Banking Environment". In: *32nd Canadian Conference on Artificial Intelligence Proceedings*. 2019. URL: http://hdl.handle.net/10993/40107.

[137] Hao Cheng, Dumitru-Daniel Dinu, Johann Groszschädl, Peter Roenne, and Peter Ryan. "A Lightweight Implementation of NTRU Prime for the Post-Quantum Internet of Things". In: *Information Security Theory and Practice, 13th IFIP WG 11.2 International Conference, WISTP 2019, Paris, France, December 11–12, 2019, Proceedings*. Ed. by Maryline Laurent and Thanassis Giannetsos. Springer Verlag, 2019, pp. 103–119. ISBN: 978-3-030-41701-7. DOI: 10.1007/978-3-030-41702-4_7. URL: http://hdl.handle.net/10993/42985.

[138] Raluca Ioana Chitic, Nicolas Bernard, Franck Leprévost, and Iona Raluca Chitic. "A proof of concept to deceive humans and machines at image classification with evolutionary algorithms". In: *Proceedings of ACIIDS 2020*. 2019. URL: http://hdl.handle.net/10993/42259.

[139] Maxime Cordy, Xavier Devroey, Axel Legay, Gilles Perrouin, Andreas Classen, Patrick Heymans, et al. "A Decade of Featured Transition Systems". In: *From Software Engineering to Formal Methods and Tools, and Back - Essays Dedicated to Stefania Gnesi on the Occasion of Her 65th Birthday*. 2019, pp. 285–312. URL: http://hdl.handle.net/10993/42026.

[140] Maxime Cordy and Sami Lazreg. "Automated evaluation of embedded-system design alternatives". In: *Proceedings of the 23rd International Systems and Software Product Line Conference, SPLC 2019, Volume A, Paris, France, September 9-13, 2019*. 2019, 52:1. ISBN: 978-1-4503-7138-4. URL: http://hdl.handle.net/10993/42056.

[141] Maxime Cordy, Axel Legay, Sami Lazreg, and Philippe Collet. "Towards sampling and simulation-based analysis of featured weighted automata". In: *Proceedings of the 7th International Workshop on Formal Methods in Software Engineering*. 2019, pp. 61–64. URL: http://hdl.handle.net/10993/42031.

[142] Maxime Cordy, Steve Muller, Mike Papadakis, and Yves Le Traon. "Search-based Test and Improvement of Machine-Learning-Based Anomaly Detection Systems". In: *ACM SIGSOFT International Symposium on Software Testing and Analysis*. 2019. URL: http://hdl.handle.net/10993/40033.

[143] Jean-Sébastien Coron and Luca Notarnicola. “Cryptanalysis of CLT13 Multilinear Maps with Independent Slots”. In: *Advances in Cryptology – ASIACRYPT 2019, 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8–12, 2019, Proceedings, Part II*. Springer, 2019. URL: http://hdl.handle.net/10993/41392.

[144] Jean-Sébastien Coron and Vitor Pereira. “On Kilian’s Randomization of Multilinear Map Encodings”. In: *On Kilian’s Randomization of Multilinear Map Encodings*. 2019. URL: http://hdl.handle.net/10993/41687.

[145] Marcos Cramer and Leon van der Torre. “SCF2 - an Argumentation Semantics for Rational Human Judgments on Argument Acceptability”. In: *Proceedings of the 8th Workshop on Dynamics of Knowledge and Belief (DKB-2019) and the 7th Workshop KI \& Kognition (KIK-2019) co-located with 44nd German Conference on Artificial Intelligence (KI 2019), Kassel, Germany, September 23, 2019*. 2019, pp. 24–35. URL: http://hdl.handle.net/10993/42646.

[146] Aditya Shyam Shankar Damodaran, Maria Dubovitskaya, and Alfredo Rial. “UC Priced Oblivious Transfer with Purchase Statistics and Dynamic Pricing”. In: *Progress in Cryptology – INDOCRYPT 2019*. 2019, pp. 273–296. URL: http://hdl.handle.net/10993/39424.

[147] Jérémie Dauphin and Ken Satoh. “Explainable ASP”. In: *PRIMA 2019: Principles and Practice of Multi-Agent Systems - 22nd International Conference, Turin, Italy, October 28-31, 2019, Proceedings*. 2019, pp. 610–617. DOI: 10.1007/978-3-030-33792-6_47. URL: http://hdl.handle.net/10993/41121.

[148] Patrick Derbez, Virginie Lallemand, and Aleksei Udovenko. “Cryptanalysis of SKINNY in the Framework of the SKINNY 2018–2019 Cryptanalysis Competition”. In: *Selected Areas in Cryptography – SAC 2019*. Ed. by Kenneth G. Patterson and Douglas Stebila. Springer International Publishing, 2019, pp. 124–145. ISBN: 978-3-030-38471-5. DOI: 10.1007/978-3-030-38471-5_6. URL: http://hdl.handle.net/10993/41518.

[149] Antonio Di Maio, Maria Rita Palattella, and Thomas Engel. “Multi-flow congestion-aware routing in software-defined vehicular networks”. In: *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall) Proceedings*. 2019. DOI: 10.1109/VTCFall.2019.8891465. URL: http://hdl.handle.net/10993/41583.

[150] Antonio Di Maio, Maria Rita Palattella, and Thomas Engel. “Performance Analysis of MANET Routing Protocols in Urban VANETs”. In: *Lecture Notes in Computer Science (volume 11803)*. Springer, 2019. ISBN: 978-3-030-31831-4. DOI: 10.1007/978-3-030-31831-4_30. URL: http://hdl.handle.net/10993/41584.

[151] Verena Distler, Marie-Laure Zollinger, Carine Lallemand, Peter Roenne, Peter Ryan, and Vincent Koenig. “Security – Visible, Yet Unseen? How Displaying Security Mechanisms Impacts User Experience and Perceived Security”. In: *Proceedings of ACM CHI Conference on Human Factors in Computing Systems (CHI2019)*. 2019. URL: http://hdl.handle.net/10993/37704.

[152] Huimin Dong, Beishui Liao, Réka Markovich, and Leon van der Torre. "From Classical to Non-monotonic Deontic Logic Using ASPIC+". In: *Logic, Rationality, and Interaction - 7th International Workshop LORI 2019, Chongqing, China, October 18-21, 2019, Proceedings*. 2019, pp. 71–85. DOI: 10.1007/978-3-662-60292-8_6. URL: http://hdl.handle.net/10993/42519.

[153] Manxing Du, Alexander I. Cowen-Rivers, Ying Wen, Phu Sakulwongtana, Jun Wang, Mats Hakan Brorsson, et al. "Know Your Enemies and Know Yourself in the Real-Time Bidding Function Optimisation". In: *Proceedings of the 19th IEEE International Conference on Data Mining Workshops (ICDMW 2019)*. 2019. URL: http://hdl.handle.net/10993/41419.

[154] Manxing Du, Christian Hammerschmidt, Georgios Varisteas, Radu State, Mats Hakan Brorsson, and Zhu Zhang. "Time Series Modeling of Market Price in Real-Time Bidding". In: *27th European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning*. 2019. URL: http://hdl.handle.net/10993/39730.

[155] Gabriel Duflo, Emmanuel Kieffer, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. "A GP Hyper-Heuristic Approach for Generating TSP Heuristics". In: *33rd IEEE International Parallel & Distributed Processing Symposium (IPDPS 2019)*. 2019. URL: http://hdl.handle.net/10993/39841.

[156] Christof Ferreira Torres, Mathis Steichen, and Radu State. "The Art of The Scam: Demystifying Honeypots in Ethereum Smart Contracts". In: *USENIX Security Symposium, Santa Clara, 14-16 August 2019*. 2019. URL: http://hdl.handle.net/10993/39687.

[157] Antonio Maria Fiscarelli, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. "A Memory-Based Label Propagation Algorithm for Community Detection". In: *Complex Networks and Their Applications VII*. Springer International Publishing, 2019. ISBN: 978-3-030-05411-3. DOI: 10.1007/978-3-030-05411-3_14. URL: http://hdl.handle.net/10993/39867.

[158] David Fuenmayor and Christoph Benzmüller. "Automated Reasoning with Complex Ethical Theories–A Case Study Towards Responsible AI". In: *16th International Congress on Logic, Methodology and Philosophy of Science and Technology (CLMPST 2019) — Bridging across Academic Cultures, Book of Abstracts*. 2019. URL: http://hdl.handle.net/10993/41336.

[159] David Fuenmayor and Christoph Benzmüller. "Harnessing Higher-Order (Meta-)Logic to Represent and Reason with Complex Ethical Theories". In: *PRICAI 2019: Trends in Artificial Intelligence*. Ed. by A. Nayak and A. Sharma. Springer International Publishing, 2019, pp. 418–432. DOI: 10.1007/978-3-030-29908-8_34. URL: http://hdl.handle.net/10993/40906.

[160] Jun Gao, Pingfan Kong, Li Li, Tegawendé François D Assise Bissyande, and Jacques Klein. "Negative Results on Mining Crypto-API Usage Rules in Android Apps". In: *Proceedings of the 16th International Conference on Mining Software Repositories*. 2019. DOI: 10.1109/MSR.2019.00065. URL: http://hdl.handle.net/10993/42460.

[161] Jun Gao, Li Li, Pingfan Kong, Tegawendé François D Assise Bissyande, and Jacques Klein. "Should You Consider Adware as Malware in Your Study?" In: *26th edition of the IEEE International Conference on Software Analysis, Evolution and Reengineering*. 2019. URL: http://hdl.handle.net/10993/39008.

[162] Jun Gao, Li, Tegawendé François D Assise Bissyande, and Jacques Klein. "On the Evolution of Mobile App Complexity". In: *Proceedings of 2019 24th International Conference on Engineering of Complex Computer Systems*. 2019. URL: http://hdl.handle.net/10993/41510.

[163] Ziya Alper Genç, Gabriele Lenzini, and Peter Ryan. "NoCry: No More Secure Encryption Keys for Cryptographic Ransomware". In: *Proceedings of the Second International Workshop on Emerging Technologies for Authorization and Authentication*. Springer, 2019, pp. 69–85. ISBN: 978-3-030-39748-7. DOI: 10.1007/978-3-030-39749-4_5. URL: http://hdl.handle.net/10993/40578.

[164] Ziya Alper Genç, Gabriele Lenzini, Peter Ryan, and Itzel Vazquez Sandoval. "A Critical Security Analysis of the Password-Based Authentication Honeywords System Under Code-Corruption Attack". In: *Information Systems Security and Privacy*. Springer International Publishing, 2019, pp. 125–151. ISBN: 978-3-030-25109-3. DOI: 10.1007/978-3-030-25109-3_7. URL: http://hdl.handle.net/10993/40158.

[165] Ziya Alper Genç, Gabriele Lenzini, and Daniele Sgandurra. "A Game of "Cut and Mouse": Bypassing Antivirus by Simulating User Inputs". In: *Proceedings of the 35th Annual Computer Security Applications Conference*. ACM, 2019, pp. 456–465. ISBN: 978-1-4503-7628-0. DOI: 10.1145/3359789.3359844. URL: http://hdl.handle.net/10993/42162.

[166] Ziya Alper Genç, Gabriele Lenzini, and Daniele Sgandurra. "Case Study: Analysis and Mitigation of a Novel Sandbox-Evasion Technique". In: *Proceedings of the Third Central European Cybersecurity Conference*. ACM, 2019. ISBN: 978-1-4503-7296-1. DOI: 10.1145/3360664.3360673. URL: http://hdl.handle.net/10993/40577.

[167] Ziya Alper Genç, Gabriele Lenzini, and Daniele Sgandurra. "On Deception-Based Protection Against Cryptographic Ransomware". In: *Proceedings of the 16th Conference on Detection of Intrusions and Malware & Vulnerability Assessment*. Springer, 2019, pp. 219–239. ISBN: 978-3-030-22037-2. DOI: 10.1007/978-3-030-22038-9_11. URL: http://hdl.handle.net/10993/40579.

[168] Salah Ghamizi, Maxime Cordy, Mike Papadakis, and Yves Le Traon. "Automated Search for Configurations of Deep Neural Network Architectures". In: *Automated Search for Configurations of Convolutional Neural Network Architectures*. 2019. URL: http://hdl.handle.net/10993/39320.

[169] Sigmund Albert Gorski III, Benjamin Andow, Adwait Nadkarni, Sunil Manandhar, William Enck, Eric Bodden, et al. "ACMiner: Extraction and Analysis of Authorization Checks inAndroid's Middleware". In: ACM, 2019. URL: http://hdl.handle.net/10993/41782.

[170] Siwen Guo, Sviatlana Höhn, and Christoph Schommer. “A Personalized Sentiment Model with Textual and Contextual Information”. In: *The SIGNLL Conference on Computational Natural Language Learning, Hong Kong 3-4 November 2019*. 2019. URL: http://hdl.handle.net/10993/40963.

[171] Siwen Guo, Sviatlana Höhn, and Christoph Schommer. “Looking into the Past: Evaluating the Effect of Time Gaps in a Personalized Sentiment Model”. In: *ACM/SIGAPP Symposium On Applied Computing, Limassol 8-12 April 2019*. 2019. URL: http://hdl.handle.net/10993/38468.

[172] Siwen Guo, Sviatlana Höhn, and Christoph Schommer. “Topic-based Historical Information Selection for Personalized Sentiment Analysis”. In: *European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, Bruges 24-26 April 2019*. 2019. URL: http://hdl.handle.net/10993/39490.

[173] Siwen Guo, Sviatlana Höhn, Feiyu Xu, and Christoph Schommer. “Personalized Sentiment Analysis and a Framework with Attention-Based Hawkes Process Model”. In: *Agents and Artificial Intelligence*. Springer, 2019. ISBN: 978-3-030-05453-3. DOI: 10.1007/978-3-030-05453-3_10. URL: http://hdl.handle.net/10993/38467.

[174] Ross James Horne. “The Sub-Additives: A Proof Theory for Probabilistic Choice extending Linear Logic”. In: *4th International Conference on Formal Structures for Computation and Deduction (FSCD 2019)*. LIPIcs, 2019, 23:1–23:16. DOI: 10.4230/LIPIcs.FSCD.2019.23. URL: http://hdl.handle.net/10993/41614.

[175] Ross James Horne, Sjouke Mauw, and Zachary Daniel Smith. “Breaking Unlinkability of the ICAO 9303 Standard for e-Passports using Bisimilarity”. In: *Breaking Unlinkability of the ICAO 9303 Standard for e-Passports using Bisimilarity*. 2019, p. 18. URL: http://hdl.handle.net/10993/41606.

[176] Antonio Ken Iannillo and Radu State. “A Proposal for Security Assessment of Trustzone-M based Software”. In: *2019 IEEE 30th International Symposium on Software Reliability Engineering (ISSRE)*. 2019. URL: http://hdl.handle.net/10993/40975.

[177] Vincenzo Iovino and Ivan Visconti. “Non-interactive Zero Knowledge Proofs in the Random Oracle Model”. In: *Codes, Cryptology and Information Security*. Springer, Cham, 2019, pp. 118–141. ISBN: 978-3-030-16457-7. DOI: 10.1007/978-3-030-16458-4. URL: http://hdl.handle.net/10993/39427.

[178] Wojciech Jamroga and Michal Knapik. “Some Things are Easier for the Dumb and the Bright Ones (Beware the Average!)” In: *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence IJCAI*. 2019, pp. 1734–1740. DOI: 10.24963/ijcai.2019/240. URL: http://hdl.handle.net/10993/41790.

[179] Wojciech Jamroga, Vadim Malvone, and Aniello Murano. “Natural Strategic Ability under Imperfect Information”. In: *Proceedings of the 18th International Conference on Autonomous Agents and Multiagent Systems AAMAS 2019*. IFAAMAS, 2019, pp. 962–970. URL: http://hdl.handle.net/10993/41795.

[180] Wojciech Jamroga, Peter Roenne, Peter Ryan, and Philip B. Stark. "Risk-Limiting Tallies". In: *Electronic Voting: Proceedings of E-Vote-ID*. 2019, pp. 183–199. DOI: 10.1007/978-3-030-30625-0_12. URL: http://hdl.handle.net/10993/41801.

[181] Asad Javed, Narges Yousefnezhad, Jérémy Robert, Keijo Heljanko, and Kary Främling. "Access Time Improvement Framework for Standardized IoT Gateways". In: *Proceedings of IEEE International Conference on Pervasive Computing and Communications*. 2019. URL: http://hdl.handle.net/10993/41187.

[182] Sophie Jenzsch, Sviatlana Höhn, and Nico Hochgeschwender. "Conversational Interfaces for Explainable AI: A Human-Centered Approach". In: *Proceedings of EXTRAAMAS 2019*. 2019, pp. 1–14. URL: http://hdl.handle.net/10993/39940.

[183] Matthieu Jimenez, Renaud Rwemalika, Mike Papadakis, Federica Sarro, Yves Le Traon, and Mark Harman. "An Empirical Study on Vulnerability Prediction of Open-Source Software Releases". In: *Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE)*. 2019. URL: http://hdl.handle.net/10993/40031.

[184] Matthieu Jimenez, Renaud Rwemalika, Mike Papadakis, Federica Sarro, Yves Le Traon, and Mark Harman. "The Importance of Accounting for Real-World Labelling When Predicting Software Vulnerabilities". In: *Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE)*. 2019. URL: http://hdl.handle.net/10993/40076.

[185] Georgios Kaiafas, Christian Hammerschmidt, Sofiane Lagraa, and Radu State. "An Experimental Analysis of Fraud Detection Methods in Enterprise Telecommunication Data using Unsupervised Outlier Ensembles". In: *16th IFIP/IEEE Symposium on Integrated Network and Service Management (IM 2019)*. Institute of Electrical and Electronics Engineers, 2019. URL: http://hdl.handle.net/10993/39936.

[186] Hong Jin Kang, Tegawendé François D Assise Bissyande, and Lo David. "Assessing the Generalizability of code2vec Token Embeddings". In: *Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering*. 2019, pp. 1–12. URL: http://hdl.handle.net/10993/41962.

[187] Oguz Özgür Karadeniz and Stefan Schiffner. "Get to know your geek: towards a sociological understanding". In: *Data for Better Living: AI and Privacy*. 2019. URL: http://hdl.handle.net/10993/41707.

[188] Nida Khan, Tabrez Ahmad, and Radu State. "Blockchain-based Micropayment Systems: Economic Impact". In: *ACM IDEAS '19 Proceedings of the 23rd International Database Engineering & Applications Symposium*. ACM, 2019. DOI: 10.1145/3331076.3331096. URL: http://hdl.handle.net/10993/39491.

[189] Nida Khan, Tabrez Ahmad, and Radu State. “Feasibility of Stellar as a Blockchain-based Micropayment System”. In: *Springer SmartBlock 2019 - 2nd International Conference on Smart Blockchain*. Springer, 2019. ISBN: 978-3-030-34083-4. DOI: 10.1007/978-3-030-34083-4_6. URL: http://hdl.handle.net/10993/40105.

[190] Nida Khan and Radu State. “Lightning Network: A Comparative Review of Transaction Fees and Data Analysis”. In: *Springer Blockchain and Applications*. Springer, 2019, pp. 11–18. DOI: 10.1007/978-3-030-23813-1_2. URL: http://hdl.handle.net/10993/39399.

[191] Sybren de Kinderen, Monika Kaczmarek-Heß, Ivan Razo-Zapata, and Qin Ma. “Strategic Analysis in the Realm of Enterprise Modeling – On the Example of Blockchain-Based Initiatives for the Electricity Sector”. In: *WIRTSCHAFTSINFORMATIK 2019 PROCEEDINGS*. AIS, 2019. URL: http://hdl.handle.net/10993/41513.

[192] Niklas Kolbe, Sylvain Kubler, and Yves Le Traon. “Popularity-driven Ontology Ranking using Qualitative Features”. In: *The Semantic Web - ISWC 2019*. 2019. DOI: 10.1007/978-3-030-30793-6_19. URL: http://hdl.handle.net/10993/40972.

[193] Anil Koyuncu, Kui Liu, Tegawendé François D Assise Bissyande, Dongsun Kim, Martin Monperrus, Jacques Klein, et al. “iFixR: bug report driven program repair”. In: *ESEC/FSE 2019 Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 2019. DOI: 10.1145/3338906.3338935. URL: http://hdl.handle.net/10993/40434.

[194] Damian Kurpiewski, Wojciech Jamroga, and Micha L Knapik. “STV: Model Checking for Strategies under Imperfect Information”. In: *Proceedings of the 18th International Conference on Autonomous Agents and Multiagent Systems AAMAS 2019*. IFAAMAS, 2019, pp. 2372–2374. URL: http://hdl.handle.net/10993/41797.

[195] Damian Kurpiewski, Micha L Knapik, and Wojciech Jamroga. “On Domination and Control in Strategic Ability”. In: *Proceedings of the 18th International Conference on Autonomous Agents and Multiagent Systems AAMAS 2019*. IFAAMAS, 2019, pp. 197–205. URL: http://hdl.handle.net/10993/41796.

[196] Damian Kurpiewski, Michal Knapik, and Wojciech Jamroga. “On Domination and Control in Strategic Ability (Extended Abstract)”. In: *Proceedings of the 31st Benelux Conference on Artificial Intelligence (BNAIC)*. 2019. URL: http://hdl.handle.net/10993/41800.

[197] Augusto Wladimir de La Cadena Ramos, Daniel Kaiser, Asya Mitseva, Andriy Panchenko, and Thomas Engel. “Analysis of Multi-path Onion Routing-based Anonymization Networks”. In: *Data and Applications Security and Privacy XXXIII, 2019*. 2019. URL: http://hdl.handle.net/10993/39409.

[198] Sofiane Lagraa, Maxime Cailac, Sean Rivera, Frédéric Beck, and Radu State. “Real-time attack detection on robot cameras: A self-driving car application”. In: *International Conference on Robotic Computing*. 2019. URL: http://hdl.handle.net/10993/38960.

[199] Sami Lazreg, Maxime Cordy, Philippe Collet, Patrick Heymans, and Sébastien Mosser. “Multifaceted automated analyses for variability-intensive embedded systems”. In: *Proceedings of the 41st International Conference on Software Engineering, ICSE 2019, Montreal, QC, Canada, May 25-31, 2019*. 2019, pp. 854–865. URL: http://hdl.handle.net/10993/42032.

[200] Claire Leong, Singh Abhayendra, Mike Papadakis, Yves Le Traon, and John Micco. “Assessing Transition-based Test Selection Algorithms at Google”. In: *International Conference on Software Engineering (ICSE)*. 2019. URL: http://hdl.handle.net/10993/39793.

[201] Tomer Libal and Alexander Steen. “NAI: The Normative Reasoner”. In: *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law*. Ed. by Floris Bex. ACM, 2019, pp. 262–263. ISBN: 978-1-4503-6754-7. URL: http://hdl.handle.net/10993/40369.

[202] Tomer Libal and Alexander Steen. “The NAI Suite - Drafting and Reasoning over Legal Texts”. In: *Legal Knowledge and Information Systems - JURIX2019: The Thirty-second Annual Conference, Madrid, Spain, December 11-13, 2019*. Ed. by Michal Araszkiewicz and Victor Rodriguez-Doncel. IOS, 2019, pp. 243–246. DOI: 10.3233/FAIA190333. URL: http://hdl.handle.net/10993/42334.

[203] Kui Liu, Dongsun Kim, Tegawendé François D Assise Bissyande, Taeyoung Kim, Kisub Kim, Anil Koyuncu, et al. “Learning to Spot and Refactor Inconsistent Method Names”. In: *41st ACM/IEEE International Conference on Software Engineering (ICSE)*. IEEE, 2019. URL: http://hdl.handle.net/10993/39016.

[204] Kui Liu, Anil Koyuncu, Tegawendé François D Assise Bissyande, Dongsun Kim, Jacques Klein, and Yves Le Traon. “You Cannot Fix What You Cannot Find! An Investigation of Fault Localization Bias in Benchmarking Automated Program Repair Systems”. In: *The 12th IEEE International Conference on Software Testing, Verification and Validation (ICST-2019)*. IEEE, 2019. URL: http://hdl.handle.net/10993/38442.

[205] Kui Liu, Anil Koyuncu, Kim Dongsun, and Tegawendé François D Assise Bissyande. “AVATAR: Fixing Semantic Bugs with Fix Patterns of Static Analysis Violations”. In: *The 26th IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER-2019)*. IEEE, 2019. URL: http://hdl.handle.net/10993/37864.

[206] Kui Liu, Anil Koyuncu, Dongsun Kim, and Tegawendé François D Assise Bissyande. “TBar: Revisiting Template-based Automated Program Repair”. In: *28th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)*. 2019. URL: http://hdl.handle.net/10993/39778.

[207] José Miguel Lopez Becerra, Peter Ryan, Petra Sala, and Marjan Skrobot. “An offline dictionary attack against zkPAKE protocol”. In: *An offline dictionary attack against zkPAKE protocol*. Springer, 2019. URL: http://hdl.handle.net/10993/39540.

[208] Tieu Long Mai, Nicolas Navet, and Jörn Migge. “A Hybrid Machine Learning and Schedulability Method for the Verification of TSN Networks”. In: *15th IEEE International Workshop on Factory Communication Systems (WFCS2019)*. IEEE, 2019. DOI: 10.1109/WFCS.2019.8757948. URL: http://hdl.handle.net/10993/38990.

[209] Tieu Long Mai, Nicolas Navet, and Jörn Migge. “On the use of supervised machine learning for assessing schedulability: application to Ethernet TSN”. In: *27th International Conference on Real-Time Networks and Systems (RTNS 2019)*. 2019. DOI: 10.1145/3356401.3356409. URL: http://hdl.handle.net/10993/40154.

[210] Hugues Mandon, Cui Su, Stefan Haar, Jun Pang, and Loic Paulevé. “Sequential reprogramming of Boolean networks made practical”. In: *Proceedings of 17th International Conference on Computational Methods in Systems Biology (CMSB’19)*. Springer, 2019, pp. 3–19. URL: http://hdl.handle.net/10993/40458.

[211] Cátia Mano Ferreira and Sviatlana Höhn. “Crafting Conversational Agents’ Personality in a User-Centric Context”. In: *Proceedings of the 31st Benelux Conference on Artificial Intelligence (BNAIC 2019) and the 28th Belgian Dutch Conference on Machine Learning (Benelearn 2019)*. 2019, pp. 1–2. URL: http://hdl.handle.net/10993/42861.

[212] Réka Markovich. “On the Formal Structure of Rules in Conflict of Laws”. In: *Legal Knowledge and Information Systems 2019 (proceedings)*. IOS Press, 2019. ISBN: 978-1-64368-048-4. DOI: 10.3233/FAIA190325. URL: http://hdl.handle.net/10993/41318.

[213] Karola Marky, Marie-Laure Zollinger, Markus Funk, Peter Ryan, and Max Mühlhäuser. “How to Assess the Usability Metrics of E-Voting Schemes”. In: *Lecture Notes in Computer Science*. Springer, 2019. URL: http://hdl.handle.net/10993/38498.

[214] Sjouke Mauw and Olga Gadyatskaya. “Attack-Tree Series: A Case for Dynamic Attack Tree Analysis”. In: *Proc. 6th International Workshop on Graphical Models for Security (GraMSec’19)*. Springer, 2019, pp. 7–19. URL: http://hdl.handle.net/10993/41698.

[215] Sjouke Mauw, Zachary Daniel Smith, Rolando Trujillo Rasua, and Jorge Luis Toro Pozo. “Post-collusion security and distance bounding”. In: *Post-collusion security and distance bounding*. 2019. URL: http://hdl.handle.net/10993/41607.

[216] David Mestel. “Quantifying information flow in interactive systems”. In: *2019 IEEE 32nd Computer Security Foundations Symposium (CSF)*. 2019. URL: http://hdl.handle.net/10993/39496.

[217] Federico Montori, Emanuele Cortesi, Luca Bedogni, Andrea Capponi, Claudio Fiandrino, and Luciano Bononi. “CrowdSenSim 2.0: a Stateful Simulation Platform for Mobile Crowdsensing in Smart Cities”. In: *MSWIM ’19: Proceedings of the 22nd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, Miami Beach, FL, USA, 2019*. Association for Computing Machinery, 2019. ISBN: 978-1-4503-6904-6. DOI: 10.1145/3345768.3355929. URL: http://hdl.handle.net/10993/41599.

[218] Mohamed Nizar Msadek, Ridha Soua, and Thomas Engel. “IoT Device Fingerprinting: Machine Learning based Encrypted Traffic Analysis”. In: *The IEEE Wireless Communications and Networking Conference (WCNC)*. 2019. URL: http://hdl.handle.net/10993/39318.

[219] Gilles Neyens and Denis Zampunieris. “Proactive Middleware for Fault Detection and Advanced Conflict Handling in Sensor Fusion”. In: *Proceedings of the 18th International Conference, ICAISC 2019 Zakopane, Poland, June 16–20, 2019, Part I & II*. Springer, 2019, pp. 643–653. ISBN: 978-3-030-20915-5. DOI: 10.1007/978-3-030-20915-5_57. URL: http://hdl.handle.net/10993/39711.

[220] Gilles Neyens and Denis Zampunieris. “Proactive Model for Handling Conflicts in Sensor Data Fusion Applied to Robotic Systems”. In: *Proceedings of the 14th International Conference on Software Technologies (ICSOFT), 2019 Prague, Czech Republic, 26 - 28 July, 2019*. SCITEPRESS, 2019, pp. 468–474. ISBN: 978-989-758-379-7. DOI: 10.5220/0007835504680474. URL: http://hdl.handle.net/10993/40433.

[221] Robert Norvill, Mathis Steichen, Wazen Shbair, and Radu State. “Demo: Blockchain for the Simplification and Automation of KYC Result Sharing”. In: *IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2019)*. IEEE Xplore, 2019. URL: http://hdl.handle.net/10993/39662.

[222] Dimiter Ostrev. “Composable, Unconditionally Secure Message Authentication without any Secret Key”. In: *2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, 2019*. IEEE, 2019. ISBN: 978-1-5386-9291-2. DOI: 10.1109/ISIT.2019.8849510. URL: http://hdl.handle.net/10993/37480.

[223] Mohamed Oumaziz, Jean-Rémy Falleri, Xavier Blanc, Tegawendé François D Assise Bissyande, and Jacques Klein. “Handling duplicates in Dockerfiles families: Learning from experts”. In: *35th IEEE International Conference on Software Maintenance and Evolution (ICSME)*. IEEE, 2019, pp. 524–535. URL: http://hdl.handle.net/10993/41956.

[224] Rohan Padhye, Caroline Lemieux, Koushik Sen, Mike Papadakis, and Yves Le Traon. “Semantic Fuzzing with Zest”. In: *ACM SIGSOFT International Symposium on Software Testing and Analysis*. 2019. URL: http://hdl.handle.net/10993/40030.

[225] Maria Rita Palattella, Ridha Soua, Khelil Abdelmajid, and Thomas Engel. “Fog Computing as the Key for Seamless Connectivity Handover in Future Vehicular Networks”. In: *The 34th ACM Symposium On Applied Computing (SAC*. 2019. URL: http://hdl.handle.net/10993/38380.

[226] Maria Rita Palattella, Ridha Soua, André Stemper, and Thomas Engel. “Aggregation of MQTT Topics over Integrated Satellite Terrestrial Networks”. In: *ACM SIGMETRICS Performance Evaluation Review*. ACM SIGMETRICS, 2019. DOI: 10.1145/3308897.3308942. URL: http://hdl.handle.net/10993/42378.

[227] Katerina Papaioannou, Martin Theobald, and Michael H. Böhlen. "Outer and Anti Joins in Temporal-Probabilistic Databases". In: *35th IEEE International Conference on Data Engineering, ICDE 2019, Macao, China, April 8-11, 2019*. IEEE, 2019. ISBN: 978-1-5386-7474-1. URL: http://hdl.handle.net/10993/41787.

[228] Pierre-André Patout and Maxime Cordy. "Towards context-aware automated writing evaluation systems". In: *Proceedings of the 1st ACM SIGSOFT International Workshop on Education through Advanced Software Engineering and Artificial Intelligence, EASEAI@ESEC/SIGSOFT FSE 2019, Tallinn, Estonia, August 26, 2019*. 2019, pp. 17–20. URL: http://hdl.handle.net/10993/42055.

[229] Balazs Pejo, Qiang Tang, and Gergely Biczók. "Together or Alone: The Price of Privacy in Collaborative Learinig". In: *Proceedings on Privacy Enhancing Technologies*. De Gruyter group, 2019. URL: http://hdl.handle.net/10993/38399.

[230] Quentin Plazar, Mathieu Acher, Gilless Perrouin, Xavier Devroey, and Maxime Cordy. "Uniform Sampling of SAT Solutions for Configurable Systems: Are We There Yet?" In: *12th IEEE Conference on Software Testing, Validation and Verification, ICST 2019, Xi'an, China, April 22-27, 2019*. 2019, pp. 240–251. URL: http://hdl.handle.net/10993/42033.

[231] Julien Polge, Jérémy Robert, and Yves Le Traon. "Assessing the impact of attacks on OPC-UA applications in the Industry 4.0 era". In: *16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, 11-14 January 2019*. 2019. ISBN: 978-1-5386-5553-5. URL: http://hdl.handle.net/10993/38972.

[232] Giulia Rinaldi, Florian Adamsky, Ridha Soua, Andrea Baiocchi, and Thomas Engel. "Softwarization of SCADA: Lightweight Statistical SDN-Agents for Anomaly Detection". In: *10th International Conference on Networks of the Future (NoF)*. 2019. URL: http://hdl.handle.net/10993/40162.

[233] Sean Rivera, Sofiane Lagraa, Antonio Ken Iannillo, and Radu State. "Auto-encoding Robot State against Sensor Spoofing Attacks". In: *International Symposium on Software Reliability Engineering*. 2019. URL: http://hdl.handle.net/10993/41349.

[234] Sean Rivera, Sofiane Lagraa, and Radu State. "ROSploit: Cybersecurity tool for ROS". In: *International Conference on Robotic Computing*. 2019. URL: http://hdl.handle.net/10993/39278.

[235] Sean Rivera, Sofiane Lagraa, Radu State, Cristina Nita-Rotaru, and Sheila Becker. "ROS-Defender: SDN-based Security Policy Enforcement for Robotic Applications". In: *IEEE Workshop on the Internet of Safe Things, Co-located with IEEE Security and Privacy 2019*. 2019. URL: http://hdl.handle.net/10993/39887.

[236] Arianna Rossi, Rossana Ducato, Helena Haapio, and Stefania Passera. "Legal Design Patterns: Towards A New Language for Legal Information Design". In: *22nd International Legal Infomatics Symposium IRIS 2019*. Ed. by Erich Schweighofer, Franz Kummer, and Ahti Saarenpää. 2019. ISBN: 978-3-96443-724-2. URL: http://hdl.handle.net/10993/39921.

[237] Arianna Rossi and Helena Haapio. “Proactive Legal Design: Embedding Values in the Design of Legal Artefacts”. In: *International Legal Infomatics Symposium IRIS 2019*. Ed. by Erich Schweighofer, Franz Kummer, and Ahti Saarenpää. 2019, pp. 537–544. ISBN: 978-3-96443-724-2. URL: http://hdl.handle.net/10993/39919.

[238] Renaud Rwemalika, Marinos Kintis, Mike Papadakis, Yves Le Traon, and Pierre Lorrach. “An industrial study on the differences between pre-release and post-release bugs”. In: *Proceedings of 35th IEEE International Conference on Software Maintenance and Evolution*. IEEE, 2019, p. 11. URL: http://hdl.handle.net/10993/41416.

[239] Renaud Rwemalika, Marinos Kintis, Mike Papadakis, Yves Le Traon, and Pierre Lorrach. “On the Evolution of Keyword-Driven Test Suites”. In: *12th IEEE International Conference on Software Testing, Verification and Validation*. 2019. URL: http://hdl.handle.net/10993/38894.

[240] Nader Samir Labib, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. “Trustworthiness in IoT - A Standards Gap Analysis on Security, Data Protection and Privacy”. In: *Trustworthiness in IoT - A Standards Gap Analysis on Security, Data Protection and Privacy*. IEEE, 2019, pp. 1–7. ISBN: 978-1-7281-0864-3. DOI: 10.1109/CSCN.2019.8931393. URL: http://hdl.handle.net/10993/40502.

[241] Nader Samir Labib, Grégoire Danoy, Jedrzej Musial, Matthias R. Brust, and Pascal Bouvry. “A Multilayer Low-Altitude Airspace Model for UAV Traffic Management”. In: *9th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (DIVANet ’19)*. ACM, 2019, pp. 57–63. ISBN: 978-1-4503-6907-7. DOI: 10.1145/3345838.3355998. URL: http://hdl.handle.net/10993/40536.

[242] Xavier Schmitt, Sylvain Kubler, Jérémy Robert, Mike Papadakis, and Yves Le Traon. “A Replicable Comparison Study of NER Software: StanfordNLP, NLTK, OpenNLP, SpaCy, Gate”. In: *International Conference on Social Networks Analysis, Management and Security*. 2019. URL: http://hdl.handle.net/10993/41853.

[243] Wazen Shbair, Mathis Steichen, Jerome Francois, and Radu State. “BlockZoom: Large-Scale Blockchain Testbed”. In: *IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2019)*. IEEE Xplore, 2019. URL: http://hdl.handle.net/10993/39669.

[244] Joshgun Sirajzade and Christoph Schommer. “The LuNa Open Toolbox for the Luxembourgish Language”. In: *Advances in Data Mining, Applications and Theoretical Aspects, Poster Proceedings 2019*. Ed. by Petra Perner. ibai publishing, 2019. ISBN: 978-3-942952-61-3. URL: http://hdl.handle.net/10993/40407.

[245] Alexander Steen and Christoph Benzmüller. “The Higher-Order Prover Leo-III (Extended Abstract)”. In: *{KI} 2019: Advances in Artificial Intelligence - 42nd German Conference on AI, Kassel, Germany, September 23-26, 2019, Proceedings*. Ed. by Christoph Benzmüller and Heiner Stuckenschmidt. Springer, 2019, pp. 333–337. DOI: 10.1007/978-3-030-30179-8_30. URL: http://hdl.handle.net/10993/40370.

[246] Mathis Steichen, Christof Ferreira Torres, Beltran Fiz Pontiveros, and Radu State. “Whispering Botnet Command and Control Instructions”. In: *2nd Crypto Valley Conference on Blockchain Technology, Zug 24-26 June 2019*. 2019. URL: http://hdl.handle.net/10993/39744.

[247] Borce Stojkovski, Itzel Vazquez Sandoval, and Gabriele Lenzini. “Detecting misalignments between system security and user perceptions: a preliminary socio-technical analysis of an E2E email encryption system”. In: *4th European Workshop on Usable Security - 2019 IEEE European Symposium on Security and Privacy Workshops*. 2019. URL: http://hdl.handle.net/10993/39726.

[248] Cui Su, Soumya Paul, and Jun Pang. “Controlling large Boolean networks with temporary and permanent perturbations”. In: *Proceedings of the 23rd International Symposium on Formal Methods (FM’19)*. Springer, 2019, pp. 707–724. URL: http://hdl.handle.net/10993/40491.

[249] Cui Su, Soumya Paul, and Jun Pang. “Scalable control of asynchronous Boolean networks”. In: *Proceedings of 17th International Conference on Computational Methods in Systems Biology (CMSB’19)*. Springer, 2019, pp. 362–367. URL: http://hdl.handle.net/10993/40459.

[250] Iraklis Symeonidis, Jessica Schroers, Mustafa A. Mustafa A. Mustafa, and Gergely Biczok. “Towards Systematic Specification of Non-Functional Requirements for Sharing Economy Services”. In: *Towards Systematic Specification of Non-Functional Requirements for Sharing Economy Services*. 2019. URL: http://hdl.handle.net/10993/39416.

[251] Bastian Tenbergen and Benoît Ries. “Methodological Aspects of Software Engineering, Assurance, Quality, and Reliability Engineering (MAS/AQR) 2019 Welcome from the Minitrack Co-Chairs”. In: *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS)*. 2019. URL: http://hdl.handle.net/10993/37371.

[252] Thierry Titcheu Chekam, Mike Papadakis, and Yves Le Traon. “Mart: A Mutant Generation Tool for LLVM”. In: *Mart: A Mutant Generation Tool for LLVM*. 2019. DOI: https://doi.org/10.1145/3338906.3341180. URL: http://hdl.handle.net/10993/39780.

[253] Ion Turcanu, Florian Adamsky, and Thomas Engel. “Experimental Evaluation of Floating Car Data Collection Protocols in Vehicular Networks”. In: *IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. 2019. DOI: 10.1109/VTCFall.2019.8891115. URL: http://hdl.handle.net/10993/40056.

[254] Ion Turcanu, Thomas Engel, and Christoph Sommer. “Fog Seeding Strategies for Information-Centric Heterogeneous Vehicular Networks”. In: *11th IEEE Vehicular Networking Conference (VNC 2019)*. IEEE, 2019. DOI: 10.1109/VNC48660.2019.9062816. URL: http://hdl.handle.net/10993/40872.

[255] Maarten Van den Heuvel, Peter Ivanov, Wolfgang Gatterbauer, Floris Geerts, and Martin Theobald. “Anytime Approximation in Probabilistic Databases via Scaled Dissociations”. In: *Proceedings of the 2019 International Conference on Management of Data, SIGMOD Conference 2019,*

Amsterdam, The Netherlands, June 30 - July 5, 2019. ACM, 2019. ISBN: 978-1-4503-5643-5. URL: http://hdl.handle.net/10993/41785.

[256] Georgios Varisteas, Raphaël Frank, Seyed Amin Sajadi Alamdari, Holger Voos, and Radu State. "Evaluation of End-To-End Learning for Autonomous Driving: The Good, the Bad and the Ugly". In: *2nd International Conference on Intelligent Autonomous Systems, Singapore, Feb. 28 to Mar. 2, 2019*. IEEE, 2019. URL: http://hdl.handle.net/10993/38967.

[257] Sébastien Varrette, Frédéric Pinel, Emmanuel Kieffer, Grégoire Danoy, and Pascal Bouvry. "Automatic Software Tuning of Parallel Programs for Energy-Aware Executions". In: *Proc. of 13th Intl. Conf. on Parallel Processing and Applied Mathematics (PPAM 2019)*. Springer Verlag, 2019. URL: http://hdl.handle.net/10993/42069.

[258] Itzel Vazquez Sandoval and Gabriele Lenzini. "A Formal Security Analysis of the pEp Authentication Protocol for Decentralized Key Distribution and End-to-End Encrypted Email". In: *Emerging Technologies for Authorization and Authentication*. Springer, 2019. URL: http://hdl.handle.net/10993/40580.

[259] Piergiorgio Vitello, Andrea Capponi, Claudio Fiandrino, Guido Cantelmo, and Dzmitry Kliazovich. "The Impact of Human Mobility on Edge Data Center Deployment in Urban Environments". In: *IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019*. 2019. URL: http://hdl.handle.net/10993/40457.

[260] Ivana Vukotic, Vincent Rahli, and Paulo Verissimo. "Asphalion: Trustworthy Shielding Against Byzantine Faults". In: *Asphalion: Trustworthy Shielding Against Byzantine Faults*. 2019. URL: http://hdl.handle.net/10993/40472.

[261] Vahid Yazdanpanah, Mehdi Dastani, Natasha Alechina, Brian Logan, and Wojciech Jamroga. "Strategic Responsibility Under Imperfect Information". In: *Proceedings of the 18th International Conference on Autonomous Agents and Multiagent Systems AAMAS 2019*. IFAAMAS, 2019, pp. 592–600. URL: http://hdl.handle.net/10993/41798.

[262] Zhiqiang Zhong, Yang Zhang, and Jun Pang. "A graph-based approach to explore relationship between hashtags and images". In: *Proceedings of the 20th International Conference on Web Information System Engineering*. springer, 2019, pp. 473–488. URL: http://hdl.handle.net/10993/40995.

[263] Marie-Laure Zollinger, Verena Distler, Peter Roenne, Peter Ryan, Carine Lallemand, and Vincent Koenig. "User Experience Design for E-Voting: How mental models align with security mechanisms". In: *Electronic Voting*. 2019. URL: http://hdl.handle.net/10993/40486.

A.5 Theses

[264] Arash Atashpendar. "From Information Theory Puzzles in Deletion Channels to Deniability in Quantum Cryptography". PhD thesis. University

of Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/38825.

[265] Boonyarit Changaival. "Graph-based Algorithms for Smart Mobility Planning and Large-scale Network Discovery". PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2019. URL: http://hdl.handle.net/10993/41593.

[266] Jérémy Henri J. Charlier. "From Persistent Homology to Reinforcement Learning with Applications for Retail Banking". PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/40891.

[267] Manxing Du. "Towards Optimal Real-Time Bidding Strategies for Display Advertising". PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/41311.

[268] Beltran Fiz Pontiveros. "A Transaction's Journey: Transactional Enhancements for Public Blockchain-based Distributed Ledgers". PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/39254.

[269] Patrick Oliver Glauner. "Artificial Intelligence for the Detection of Electricity Theft and Irregular Power Usage in Emerging Markets". PhD thesis. University of Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/38544.

[270] Siwen Guo. "Deep Neural Networks for Personalized Sentiment Analysis with Information Decay". PhD thesis. University of Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/41205.

[271] Thomas Harzheim. "Mixed Frequency Single Receiver Architectures and Calibration Procedures for Linear and Non-Linear Vector Network Analysis". PhD thesis. University of Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/39176.

[272] Médéric Hurier. "Creating better ground truth to further understand Android malware: A large scale mining approach based on antivirus labels and malicious artifacts". PhD thesis. University of Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/39903.

[273] Emmanuel Kieffer. "Co-evolutionary Hybrid Bi-level Optimization". PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2019. URL: http://hdl.handle.net/10993/38566.

[274] Sophie Klecker. "Robotic Trajectory Tracking: Position- and Force-Control". PhD thesis. University of Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/39865.

[275] Kui Liu. "Deep Pattern Mining for Program Repair". PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/41348.

[276] José Miguel Lopez Becerra. "PROVABLE SECURITY ANALYSIS FOR THE PASSWORD AUTHENTICATED KEY EXCHANGE PROBLEM". PhD thesis. University of Luxembourg, Esch-Uelzecht, Luxembourg, 2019. URL: http://hdl.handle.net/10993/39511.

[277] Ludovic Mouline. “TOWARDS A MODELLING FRAMEWORK WITH TEMPORAL AND UNCERTAIN DATA FOR ADAPTIVE SYSTEMS”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/41258.

[278] Rohan Nanda. “Automated Identification of National Implementations of European Union Directives With Multilingual Information Retrieval Based On Semantic Textual Similarity”. PhD thesis. University of Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/40257.

[279] Gilles Neyens. “CONFIDENCE-BASED DECISION-MAKING SUPPORT FOR MULTI-SENSOR SYSTEMS”. PhD thesis. University of Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/41506.

[280] Balazs Pejo. “Integrity and Confidentiality Problems of Outsourcing”. PhD thesis. University of Luxembourg, Esch/Alzette, Luxembourg, 2019. URL: http://hdl.handle.net/10993/40333.

[281] Arianna Rossi. “Legal Design for the General Data Protection Regulation. A Methodology for the Visualization and Communication of Legal Concepts”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg and Università di Bologna, Bologna, Italy, 2019. URL: http://hdl.handle.net/10993/39925.

[282] Mathis Steichen. “Access Control Mechanisms Reconsidered with Blockchain Technologies”. PhD thesis. University of Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/41053.

[283] Sakthivel Manikandan Sundharam. “Timing-aware Model Based Design with Application to Automotive Embedded Systems”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/40501.

[284] Thierry Titcheu Chekam. “Assessment and Improvement of the Practical Use of Mutation for Automated Software Testing”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/40442.

[285] Bogdan Toader. “MOBILITY ANALYSIS AND PROFILING FOR SMART MOBILITY SERVICES: A BIG DATA DRIVEN APPROACH. An Integration of Data Science and Travel Behaviour Analytics”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2019. URL: http://hdl.handle.net/10993/40724.

[286] Jorge Luis Toro Pozo. “Computational and symbolic analysis of distance-bounding protocols”. PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2019. URL: http://hdl.handle.net/10993/39506.

[287] Aleksei Nikolaevich Udovenko. “Design and Cryptanalysis of Symmetric-Key Algorithms in Black and White-box Models”. PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2019. URL: http://hdl.handle.net/10993/39350.

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 (Luxembourg)/NCBiR (Poland)
- FNR - POC
- FNR - PRIDE
- ONRG - NICOP
- SnT partnership with pEp security
- UL
- UL and External Organisation Funding
- 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

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

HiEdTec project has successfully finished the first year. During the year 2019, HiEdTec project consortium members developed first version of the Concepts of adaptation of the education system to the digital generation with regard to the specific conditions of each of the involved countries. Recommendations for adapting the Central Asian Higher Education System to the needs of the digital learners was proposed. Each country developed national concept of digital

transformation. Syllabus of a Training Course for Improving Lecturers' Skills in Innovative Educational Technologies and Didactic Models have been created and the corresponding Training courses for Lecturers from the Central Asian Countries took place. The Quality assurance of the projects is in hand of the Uni.Lu and a Quality plan as well as an evaluation strategy has been produced.

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 work carried out in 2019 focused on two aspects:

The first aspect focused on the identification of potential security vulnerabilities in vehicle-to-everything communications (V2X) and the delivery of a detailed description of the penetration tests. To this end, a plan for assessing the resiliency of connected vehicles to a set of attacks (jamming, tracking, misbehaving nodes) and intentional and non-intentional interferences was proposed. Dr. Ridha Soua and Dr. Abdelwahab Boualouache have defined a set of user stories for an urban scenario (intelligent intersection and Green Light Optimal Speed Advisory use cases) to test the performances of ITS-G5 and Cellular-V2X under attacks. Moreover, given that the two technologies for connected vehicles (ITS-G5 and Cellular-V2X) will co-exist in the future deployment, we defined a set of test to analyse the levels of potential interferences in the 5.9

GHz.

In the second aspect, SECAN-lab team investigated 5G key technologies (software defined networking and multi-access edge computing) and their contribution to the security and privacy of connected vehicles. On the first hand, given that the pseudonym-changing approach is the de-facto location privacy solution proposed by security standards to ensure that drivers are not tracked during their journey, we proposed a pseudonym changing strategy between connected vehicles that exploit the Software Defined Network (SDN) paradigm. The proposed approach is context-aware in which connected vehicles assisted by SDN controllers, decide whether and when to change their pseudonyms based on their context (density of the network, vehicle privacy level, attacker power, etc.). On the second hand, the Secan-lab proposed a placement strategy of the vehicular Location Privacy Zones (VLPZs) which is a promising approach to ensure unlinkability. These logical zones can be easily deployed over roadside infrastructures (RIs) such as gas station or electric charging stations. However, the placement optimization problem of VLPZs is NP-hard and thus an efficient allocation of VLPZs to these RIs is needed to avoid their overload and the degradation of the QoS provided within theses RIs. The optimal placement of the VLPZs is genetic-based algorithm that ensures minimized trajectory cost of involved vehicles and hence less consumption of their pseudonyms.

In terms of standardisation, Secan-lab team contributed to an ETSI paper related to IPv6 based vehicular-to-everything (V2X) communication.

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 NATUUR-WETENSCHAPPELIJK 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

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. In 2019, Secan-Lab continued its active contribution to this project. In particular, we participated in dissemination activities through several keynotes and speeches at international conferences/events and lead the international cooperation activities. We contributed to the evaluation methodology of the business impact assessment and cost/benefit analysis.

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

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

Acronym:	ATENA
Reference:	R-AGR-3026
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	6,889,925.00 €
Duration:	1 May 2016 – 30 Apr 2019
Members:	• Thomas ENGEL (Principal Investigator) • 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

ATENA project finished in 2019. It produced a set of tools that, implementing innovative models, methodologies and algorithms for security assurance, and interacting with the available smart components of a critical infrastructure. Increasing the level of cyber-physical security and resilience of underpinning CI & IACS is result of the project proved by End Users that operate a critical infrastructure.

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 Jan 2019
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

EXCITING partners have cooperated effectively, accomplished tasks aligned with the work plan in the DoA and have submitted the planned deliverables.

The Report on Future Internet research and innovation policies and ecosystems in China has provided a detailed analysis of China's innovation ecosystem and identified specific innovation support mechanisms. It details existing policies promoting innovation; existing capacity building on innovation; China's research and innovation capacity; existing support schemes and initiatives for science, technology and innovation collaboration; regulations and financial incentives that support innovation and internationalisation; and opportunities and obstacles related to the innovation ecosystem.

The Harmonisation of standards for IoT technologies, version 1 and the Harmonisation of standards for 5G technologies, version 1 have addressed the situation of global standardisation of IoT and 5G Technologies, with a focus on Europe and China. In addition, Interop guidelines for IoT, version 1 and Interop guidelines for 5G, version 1) have included existing interoperability activities concerning the IoT and 5G, as well as analysing the requirements for the possible alignment of - and recommendation for – interoperability testing between China and Europe in these two fields.

Outline of the Pilot concept and Identification of Ongoing IoT and 5G Large Scale Pilots between Europe and China introduced the primary goal and the methodology used in WP4. First, our studies of the IoT-LSP Programme and testbeds of IoT in both Europe and China were listed. Then, the current ongoing pre-pilots and large scale testbeds of 5G have been studied. The achievement of WP4 in year 1 presented in D4.1 will serve as part of the input for Task 4.2 which focuses on a set of practices and recommendation to be considered in future cooperation opportunities on LSPs for IoT and 5G.

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 an H2020 project of a three year duration that focuses on the development of a quantum-resistant Trusted Platform Module (TPM). It consists of 15 European partners and by the end of 2019 it completed the second year. The main progress is related to work packages 2 and 3. The aim of work package 2 is to identify, or create new, quantum-resistant cryptographic primitives to be integrated in a TPM. A first list of recommendations for such symmetric and asymmetric primitives was reported by the end of 2019. In work package 3, the project started the development of security models for the TPM, in order to perform a formal security analysis of the TPM. In September 2019 it has successfully passed the first EC review process, where the project received a very positive evaluation and comments.

Mining and Reasoning with Legal Texts

http://www.mirelproject.eu/

Acronym:	MIREL
PI:	Leon VAN DER TORRE
Funding:	European Commission - Horizon 2020
Budget:	464,486,400,000.00 €
Duration:	1 Jan 2016 – 31 Dec 2019
Members:	• Leon VAN DER TORRE (Principal Investigator) • Giovanni CASINI (Researcher) • Réka MARKOVICH (Researcher) • Amro NAJJAR (Researcher) • Xavier PARENT (Researcher) • Alexander STEEN (Researcher) • Livio ROBALDO (Project Coordinator) • Jérémie DAUPHIN (Doctoral Candidate) • Shohreh HADDADAN (Doctoral Candidate)
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

With his research background in automated and interactive reasoning, in particular higher-order reasoning technology, Alexander Steen planned to contribute to the objectives related to reasoning in normative and/or regulative systems in WP3. Earlier work includes the application of reasoning technology to theoretical philosophy and meta-physics, as well as non-classical logics in general.

During his secondment at U Stanford, he exchanged research ideas and prospective collaboration possibilities with relevant local actors; in particular with Cleo Condoravdi (NLP) but also further key figures for interdisciplinary research relevant to MIREL's goals such as Ed Zalta (CSLI), Thomas Icard (Stanford Philosophy), Richard Waldinger (SRI), John Rushby (CSLI), Susanne Riehemann (Google), Valeria de Pavia (Nuance/Samsung Research) and further.
These contacts and the knowledge transfer during his secondment enables

subsequent collaborative and interdisciplinary research on novel reasoning technology for normative knowledge (see objects of WP3, D3.4).

Livio Robaldo was the main guest editor of these two special issues:

- Robaldo, L. and and van der Torre, L.: Introduction to legal AI, Journal of Applied Logics, special issue "reasoning on legal texts", Vol. 6, Issue 5.
- Robaldo, L. and Villata, S. and Wyner, A. and Grabmair, M.: Introduction for artificial intelligence and law: special issue "natural language processing for legal texts", Artificial Intelligence and Law, Vol. 27, Issue 2.

He published the paper describing the DAPRECO knowledge base, built also in light of feedback collected during his MIREL secondment at Stanford University:

- Robaldo, L. and Bartolini, C. and Palmirani, M. and Rossi, A. and Martoni, M. and Lenzini, G.: Formalizing GDPR provisions in reified I/O logic: the DAPRECO knowledge base, The Journal of Logic, Language, and Information (to appear).

The DAPRECO knowledge base is currently the biggest public knowledge base in LegalRuleML and Input/Output logic.

In the last year of the MIREL project, Giovanni Casini has visited The University of Cape Town for 3 months and Stanford University for 1 month. In such a visit he has mainly worked in the development of appropriate formalisms for modelling defeasible forms of reasoning, with particular focus on normative reasoning.

Papers published in 2019 and associated to the MIREL project:

- Booth R., Casini G., Meyer T., Varzinczack I. (in Press) 'On Rational Entailment for Propositional Typicality Logic' in Artificial Intelligence Journal, https://doi.org/10.1016/j.artint.2019.103178.
- Casini G., Meyer T., Varzinczack I. (2019), 'Simple Conditionals with Constrained Right Weakening' in Proceedings of the 28th International Joint Conference on Artificial Intelligence (IJCAI-19), pp. 1632-1638.
- Casini G., Harrison M., Meyer T., Swan R. (2019), 'Arbitrary Ranking of Defeasible Subsumption' in Proceedings of the 32nd International Workshop on Description Logics (DL-2019), CEUR Workshops Proceedings.
- Britz A., Casini G., Meyer T., Varzinczack I. (2019), 'A KLM Perspective on Defeasible Reasoning for Description Logics' in Lutz C., Tinelli C., Sattler U., Turhan A-Y., Wolter F. (eds.), 'Description Logic, Theory Combination, and All That - Essays Dedicated to Franz Baader on the Occasion of His 60th Birthday', Springer.
- Casini G., Meyer T., Varzinczack I. (2019) 'Taking Defeasible Entailment beyond Rational Closure' in Proceedings of the 16th Edition of the European Conference on Logics in Artificial Intelligence (JELIA-19), LNAI 11468, pp. 182-197, Springer.
- Casini G., Straccia U., Meyer T. (2019), 'A polynomial Time Subsumption Algorithm for Nominal Safe ELO under Rational Closure', Information Sciences, vol. 501, pp. 588-620.

PRACE Sixth Implementation Phase

Acronym:	PRACE-6IP
PI:	Pascal BOUVRY
Funding:	European Commission - Horizon 2020
Budget:	21,305,000.00 €
Duration:	1 Apr 2019 – 30 Sep 2021
Members:	• Pascal BOUVRY (Principal Investigator) • Sébastien VARRETTE (Researcher) • Valentin PLUGARU (Collaborator)
Areas:	• Computational Sciences • Security, Reliability and Trust in Information Technology • Sustainable Development
Partner:	Forschungszentrum Jülich

Description

This proposal addresses the continuation of support for the world-class pan-European HPC infrastructure PRACE. This includes its further expansion for both academia and industry, while providing state-of-the-art services that can be accessed by users regardless of their location. A unique catalogue of services is provided by PRACE 2 and complemented by the services provided by the PRACE-6IP project. Pooling, integration and rationalisation of European HPC resources will contribute to the EU strategy, and complement the activities of the Public-Private Partnership (PPP) in order to implement the HPC strategy. The Research Infrastructures Work Programme 2018-2020 lists the following key components that PRACE-6IP aims to address: 1. Provide a seamless and efficient Europe-wide Tier-0 service to users; 2. Support software implementations, helping Tier-0 users and communities in adapting and adopting novel software solutions; 3. Collaborate with Centres of Excellence on HPC and other national and EU funded activities that focus on similar or complementary activities for HPC codes and applications; 4. Identify and support new user needs and ensure openness to new user communities and new applications; reach out to scientific and industrial communities, promoting industrial take-up of HPC services in particular by SMEs; 5. Carry out activities that build on national HPC capabilities (Tier-1) and are necessary to support Tier-0 services and a functional European HPC ecosystem; 6. Run training and skills development programmes tailored to the research needs of academia and industry and relevant public services and transfer of know-how for the use of HPC; Coordinate at European level such programmes in cooperation with the Centres of Excellence on HPC; 7. Implement inclusive and equitable governance and a flexible business model to ensure long term financial sustainability; 8. Support the development of the strategy for the deployment of a rich HPC environment of world-class systems with different machine architectures; 9. Coordinate activities with the European Technology Platform for HPC (ETP4HPC) and the Centres of Excellence

in HPC applications in support of the European HPC strategy towards the next generation of computing systems, technologies and applications. 10. Develop an international cooperation policy and associated activities in the area of HPC.

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 ap-

propriate 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 was successfully finalised in 2019. It examined the problem of failures in cyber-security using a multidisciplinary approach that goes beyond the purely technical viewpoint. The project consortium combined the insights gained by economic, behavioural, societal and institutional views. UL's contributions were both practical and theoretical. SECAN-Lab developed a prototype of a tool that can be used by any citizen or organization to evaluate the level of their privacy when using privacy preserving communication systems. The output of the tool is a privacy score that depends on the current state of Internet and user's geographical position. UL also developed privacy models for anonymous communication networks. The efforts for the latter contributed to a publication in PETs that was awarded the best student paper award [1]. Lastly, the project was finalised and reviewed by the EU and considered a success.

[1] On privacy notions in anonymous communication. Kuhn, Christiane; Beck, Martin; Schiffner, Stefan; Jorswieck, Eduard; Strufe, Thorsten in Proceedings on Privacy Enhancing Technologies (2019)

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
Member:	Dzmitry KLIAZOVICH (Principal Investigator)
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.

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 Dec 2019
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) • Luca LAMORTE (Research Associate)
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

The secan-lab team within the M2MSAT project, which was closed in December 2019, succeeded to develop and assess the performances of two proposed optimization for both MQTT and CoAP protocols.

For MQTT, Dr. Ridha Soua design an advanced filter namely MQTT-MFA that performs MQTT topics aggregation in close proximity of MQTT Publishers before data is sent over the satellite link. The developed MQTT-MFA implementation is compliant with Mosquitto, an open source MQTT broker.

On the other hand, to reduce network traffic overhead in group communication and improve the network responsiveness when CoAP is used, Secan-lab team proposed an aggregation scheme for the CoAP group communication in combination with Observer pattern and proxying. Results obtained by using the openSAND emulator and CoAPthon library corroborate the merit of the proposed optimization in terms of overhead reduction and delay.

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

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

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

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

Results

The project has finished in March 2019. The Prime Investigator Dr. Olga Gadyatskaya has joined Leiden University, the Netherlands as a lecturer.

- A research paper about Android miners has been accepted to ACM CODASPY 2020.
- A journal paper about ACVTool has been prepared as major revision.

B.6 FNR and UL Projects

Approaching Indigenous Australian History With Text Mining Methods

https://www.c2dh.uni.lu/people/ekaterina-kamlovskaya

Acronym:	AIAHTMM
PI:	Christoph SCHOMMER
Funding:	Fonds National de la Recherche, University of Luxembourg
Duration:	1 Jan 2017 – 15 May 2021
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

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 reso-

lution 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

The PhD defence took place on January 18, 2019.

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.

Privacy Attacks and Protection in Machine Learning as a Service

Acronym:	PriML
PI:	Jun PANG
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD
Duration:	1 Dec 2019 – 30 Nov 2023
Members:	• Jun PANG (Principal Investigator) • Hailong HU (Doctoral Candidate)

Description

Machine learning (ML) techniques have gained widespread adoption in a large number of real- world applications. Following the trend, machine learning as a service (MLaaS) is provided by leading Internet companies to broaden and simplify ML model deployment. Although MLaaS only provides black-box access to its customers, recent research has identified several attacks to reveal confidential information about model itself and training data. Along this line, this project's goal is to further investigate new attacks in terms of ML models and training data and develop a systematic, practical and general defense mechanism to enhance the security of ML models. The project team including SaToSS and CISPA will also make source codes publicly available and use them in their own courses. This project will provide a deeper understanding of machine learning privacy, thereby increasing the safety of machine learning-based systems such as authentication system and malware detection, helping protect the nation and its citizens from cyber harm. This project PriML combines multiple novel ideas synergistically, organized into three inter-related research thrusts. The first thrust aims to explore potential attacks from the perspective of ML models via black-box explainable machine learning techniques. The second thrust focuses on investigating new attacks from the perspective of training datasets through DeepSets technique which can mitigate the complexity of deep neural networks and facilitate our attacks. Both thrusts include considering different types of neural networks and identifying inherently distinct properties of these types of attacks respectively. The third thrust involves un- derstanding and finding out a set of invariant properties underlying these attacks and developing defense mechanisms that exploit these properties to provide better protection of ML privacy.

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

- Trustworthiness in IoT - A Standards Gap Analysis on Security, Data Protection and Privacy, 2019. IEEE Conference on Standards for Communications and Networking (CSCN 2019) N. S. Labib, M. R. Brust, G. Danoy, P. Bouvry. [240]
- A Multilayer Low-Altitude Airspace Model for UAV Traffic Management. *9th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (DIVANet '19), 2019.* N. S. Labib, G. Danoy, J. Musial, M. R. Brust, P. Bouvry. [241]
- Internet of Unmanned Aerial Vehicles—A Multilayer Low-Altitude Airspace Model for Distributed UAV Traffic Management. Sensors, 2019. N. S. Labib, G. Danoy, J. Musial, M. R. Brust, P. Bouvry. [96]
- White Paper: Data Protection and Privacy in Smart ICT - Scientific Research and Technical Standardization, 2018 [10993/37276]
- On Standardised UAV Localisation and Tracking Systems in Smart Cities - N. Labib, M.R. Brust, G. Danoy, P. Bouvry, Book of abstracts of the 17th Annual STS Conference (Graz), 2018 [10993/37265]
- A Standardized Broker Model in Smart Cities, C. Liu, S. Varrette, G. Danoy, M.R. Brust, P. Bouvry, Book of abstracts of the 17th Annual STS Conference

(Graz), 2018 [10993/37479]
- Maya Olszewski, Jeff Meder, Emmanuel Kieffer, Raphaël Bleuse, Martin Rosalie, Grégoire Danoy, and Pascal Bouvry. Template of a Chaotic Attractor . Graph Drawing. 2018 [10993/37764]
- 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 [10993/38402]
- C. Liu, P. Bouvry. Optimal Pricing for Socially-aware Usage of Cloud Services. International Conference on Optimization and Learning, OLA 2019
- 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
- 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 [10993/38696]

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

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 Investiga-

tor)

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)

- Maria Rita PALATTELLA (Post-Doc)
- 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

In 2019, Secan-Lab continued its active contribution to the CONTACT project, focusing on several aspects:

One aspect is related to the benefits of using a centralized SDN-controller to support the content retrieval in Information-Centric Heterogeneous Vehicular Networks. Nowadays, content downloading of mobile broadband users routinely causes network load to exceed what the Radio Access Network (RAN) can sustain without degrading user experience. Many works are therefore considering edge or fog computing paradigms and Device to Device (D2D) communication using 4G/5G C-V2X or IEEE 802.11p/bd links to obtain content. When content originates (or is maintained) at a central location, however, this requires expensive seeding of the content into the mobile network. In this context, we studied different seeding strategies assuming a centralized instance (e.g., an operator or a content provider) for decision making and basing the decision of when and where to perform fog seeding on a network graph that respects connectivity metrics while performing community detection and exploiting node centrality. We investigated their relative benefits and their benefits with respect to the baseline of traditional information-centric networking. We demonstrated that choosing sub-optimal metrics for connectivity, community detection, or node centrality can yield substantial loss of performance, whereas following a strategy adapted for the described use case can yield substantial benefits. We also showed that the global network-status knowledge offered by the SDN controller can be leveraged to design a centralized congestion-aware routing algorithm to improve QoS in vehicular networks.

Within CONTACT project, SECAN-Lab team was engaged in outreach activities to show the benefits of the carried out research to a larger public and to interact with distinguished researchers working on smart mobility. In this vein, the team organized the second edition of the international workshop on 5G and autonomous driving (https://icc2019.ieee-icc.org/workshop/w12-2nd-international-workshop-5g-and-cooperative-autonomous-driving-5g-auto) in conjunction with the IEEE International Conference on Communications (ICC) 2019 that was held in Shanghai, China.

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.

EnCaViBS

Acronym:	EnCaViBS
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - CORE
Budget:	969,000.00 €
Duration:	1 Sep 2019 – 31 Aug 2022
Members:	• Thomas ENGEL (Principal Investigator) • Aamir FARAH (Research assistant) • Stefan SCHIFFNER (Post-Doc)
Area:	Communicative Systems
Partner:	Mark Cole (University of Luxembourg, Faculty of Law, Economics and Finance)

Description

Today's economy and citizens of the EU by proxy, depend on reliable network and information services. Despite a wide selection of technical protection measures being available, attacks on electronic services are on the rise in number and impact. The EU's response under its Cybersecurity Strategy has been the NIS Directive as a legal instrument aiming to ensure that critical information technology systems in central sectors of the economy are secure. The analysis whether and how the legal requirements under the new framework match software requirements and vice versa, calls for a joint effort of legal and technical experts. The abstract notions of the NIS Directive requirements are in need of clarification so that compliant products can to be derived and developers can be equipped with guidelines how to meet the legal requirements with the currently

available technologies. However, technology and the law evolve with different speeds hence these interpretations and guidelines need to be dynamic.

Objective of EnCaViBS is the creation of a living commentary to the NIS Directive that is accompanied with a methodology to select the appropriate technological and organisational measures for NIS Directive compliant IT products.

Privacy Enhancing Techniques for Future Internet

Acronym:	PETIT
Reference:	R-AGR-0665
PI:	Thomas ENGEL, Andriy PANCHENKO
Funding:	Fonds National de la Recherche - CORE
Budget:	654,000.00 €
Duration:	1 Sep 2016 – 31 Aug 2020
Members:	• Thomas ENGEL (Principal Investigator) • 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 core project PETIT is in designing and evaluating privacy-enhancing techniques for the future Internet. Within the scope of the project in 2019, the SECAN-Lab team made advances in (1) multipath routing, (2) website fingerprinting, (3) DHT simulation for testing security/privacy extensions and (4) analysis of guard selection algorithms for Tor. In the following, we briefly summarize our achievements.

During the reported period, we continued our research of anonymity and performance analysis of multipath onion routing anonymization systems, which resulted in a paper presented at the IFIP DBSEC conference. After this, we proceeded with the development of a defence mechanism to counter website fingerprinting attacks based on dynamically distributed traffic via multiple paths in Tor. In a poster presented at the IEEE ICNP conference in October, we addressed system design and performance of multipath data transmission. Then, we investigated and proposed a traffic distribution mechanism that obfuscates the patterns that a malicious entry node can see to perform a website fingerprinting attack. The developed splitting strategy reduces the effectiveness of an attack from more than 95% to around 35%. The comprehensive evaluation of this traffic distribution mechanism was presented as a poster at the ACM CCS conference in November. Currently, we continue evaluating our splitting traffic defence mechanism within a multipath Tor prototype developed by our team.

Further, we investigated Distributed Hash Table (DHT) security/privacy. Tor's directory service does not scale, and using a DHT to make the directory service

scale is a promising approach. However, current DHT security/privacy mechanisms do not meet the requirements a Tor directory has to fulfill. While we investigated novel DHT security/privacy extensions during this reported period, we mainly focused on building an efficient highly parallel DHT simulator which allows us both practically evaluating novel approaches and testing the accuracy of the underlying mathematical models.

Finally, we finished analysing some novel guard selection algorithms for Tor. This work resulted in a publication that is now under review at the IFIP SEC conference. In this paper, we quantify privacy leaks and performance deterioration of such algorithms as Counter-RAPTOR and DPSelect, which were previously considered comparable to Vanilla Tor.

Privacy-preserving Publication of Dynamic Social Network Data in the Presence of Active Adversaries

Acronym:	PrivDA
PI:	Yunior RAMIREZ CRUZ
Funding:	Fonds National de la Recherche - CORE
Duration:	1 Jun 2018 – 31 May 2021
Members:	• Yunior RAMIREZ CRUZ (Principal Investigator) • Sjouke MAUW (Supervisor / Scientific Advisor) • Xihui CHEN (Research Associate)
Areas:	• Computer Science & ICT Security • Security, Reliability and Trust in Information Technology

Description

Over the last decade, online social networks (OSNs) have become one of the most popular online services. The analysis of social network data allows social scientists, market analysts, economists, among others, to understand societal phenomena, detect consumption patterns, assess the effect of policies, etc. Likewise, companies and public agencies can benefit from these studies to improve their decision-making processes and social outreach. In order to enable such studies, it is necessary that OSN owners release the necessary information about the network structure. However, given the personal and sensitive nature of the information contained in the network, it is necessary to sanitise the released information, to ensure that the privacy of the individual users is protected.

Adversaries seek to re-identify users and learn sensitive private information about them from the sanitised information releases, such as the existence of relations between users, political affiliation, religious beliefs, etc. To that end, the adversary collects pieces of information that identifies each victim in a unique manner, so when the information is released the victims can be re-

identified by matching the adversary knowledge to the released information. So-called active adversaries have the capacity of enrolling sybil nodes in the network, which engage in interactions with the targeted victims in order to create unique structural patterns that can later be used as fingerprints to re-identify the victims and infer private information about them.

In this project, we will focus on providing methods for safely releasing structural information about the social network, accounting for, and counteracting, the presence of active adversaries. Given that social networks are inherently dynamic, and numerous analysis tasks require information on the evolution of the social graph over time, we will focus on techniques allowing to release updates on the structural information as the network evolves. We will first study how the dynamic nature of the networks and the release process can be exploited by active adversaries to strengthen their attacks. Then, considering the new vulnerabilities detected, we will define novel ways to quantify privacy in the dynamic scenario. The new privacy properties will be the basis for new models and algorithms allowing OSN owners to safely release information in two manners: (1) periodically publishing anonymised versions of the dynamic social graph, and (2) answering structural queries about the network. The proposed methods will be incremental, in the sense that as the network evolves and new information is released, each new piece of information will integrate with the previously released ones in such a manner that the privacy properties are globally satisfied.

Results

- Dr. Xihui Chen joined the project in January 2019 as a Research Associate.
- Ema Këpuska developed her master's thesis "Active re-identification attacks on periodically released social graphs" within the project. She successfully defended her thesis in September 2019 (grade 18=20).

Publications and conference presentations:

1. S. Mauw, Y. Ramírez-Cruz, R. Trujillo-Rasua. Conditional adjacency anonymity in social graphs under active attacks. Knowledge and Information Systems 61(1):485-511, 2019.

2. S. Mauw, Y. Ramírez-Cruz, R. Trujillo-Rasua. Robust active attacks on social graphs. Data Mining and Knowledge Discovery 33(5):1357-1392, 2019. Presented in ECMLPKDD 2019, Würzburg, Germany, September 2019.

3. R. Gil-Pons, Y. Ramírez-Cruz, R. Trujillo-Rasua and I.G. Yero. Distance-based vertex identification in graphs: the outer multiset dimension. Applied Mathematics and Computation 363:124612, 2019.

4. The talk "Constrained incremental resolvability in dynamic graphs": a case study in active re-identificaton attacks on social networks was delivered at the 9th Slovenian International Conference on Graph Theory, Bled, Slovenia, June 2019 (abstract published).

Submissions:

1. X. Chen, S. Mauw and Y. Ramírez-Cruz. Publishing Community-Preserving Attributed Social Graphs with a Differential Privacy Guarantee. Submitted to PoPETs, major revision requested, due in March 2020.
2. X. Chen, E. Këpuska, S. Mauw and Y. Ramírez-Cruz. Active Re-identification Attacks on Periodically Released Dynamic Social Graphs. Submitted to Euro S&P 2020, notification expected by February 2020.

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) • Jeroen VAN WIER (Doctoral Candidate) • Arash ATASHPENDAR (PhD student) • Dimiter OSTREV (Research Associate) • Peter Browne Roenne (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

The FNR CORE project Q-CoDe aims to explore whether quantum information processing can help to achieve the cryptographic property of deniability. In 2019, we focused on completing work package 1, a literature review of deniability in classical cryptography. We also worked on developing deniable public key-based Key Exchange protocols via strong designated verifier signatures both in the classical case and for Quantum Key Distribution. Further, we performed work on malleability in the quantum setting, presented at Qcrypt 2019.

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:	• Jan LAGERWALL (Principal Investigator) • 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 research activities in 2019 focused on some relevant topics in privacy-preserving cryptocurrencies and, more generally, in the blockchain world: succinct and efficient zero-knowledge proof protocols (zkSNARKs), memory-efficient KYC implementations (accumulators), cryptanalysis of cryptographic primitives. In particular, the project team showed the presence of subliminal channels in J. Groth's zkSNARK proof protocol (EUROCRYPT 2016) and in the Pedersen's commitment scheme, which are both currently used in Zcash: these results and how these can be used to actively tag Zcash shielded transactions were presented at ACM CCS'19. The project team also studied cryptographic accumulators and their relevance for (distributed) anonymous credentials. They

also cryptanalyzed the Legendre PRF, a MPC-friendly PRF proposed as a building block for a proof-of-custody mechanism in Ethereum 2.0: these results will be presented at FSE ToSC'20. Furthermore, the team worked on various privacy aspects in privacy-preserving cryptocurrencies (transaction privacy and network privacy).

teSTing sELf-LeARning systems

Acronym:	STELLAR
PI:	Yves LE TRAON
Funding:	Fonds National de la Recherche - CORE
Duration:	1 Sep 2019 – 31 Aug 2022
Members:	• Yves LE TRAON (Principal Investigator) • Maxime CORDY (Researcher) • Mike PAPADAKIS (Researcher)

Description

Self-learning software systems (SLS) are integrated into a variety of domains ranging from safety-critical applications (autonomous cars and healthcare) to business-critical applications (finance, smart factories). Engineering such systems, however, is still a new practice, often not well-understood by engineers, and thus errorprone. It is therefore essential to provide engineers with means to assess that the SLS they build work reliably and as expected. In this project, we aim at complementing state-of-the-art machine-learning evaluation processes with testing techniques specifically adapted to the peculiarities of SLS. Indeed, although a plethora of techniques exists for testing traditional software, these are heavily challenged by SLS, their intrinsic probabilistic nature, their vast number of parameters, and their use cases too numerous to be elicited. More precisely, we focus on testing their underlying learning models and target three objectives: (1) measuring the adequacy of existing test cases with criteria that indicate how well the test cases cover the learning model; (2) defining model transformations (mutations) to modify the models, and estimating their sensitivity; (3) designing differential testing methods to discover disagreements between models, thereby obtaining new test cases that reveal errors in the models. Our three objectives are certainly not independent as fulfilling one will help achieve the others. Thus, altogether they will form a triangular chain of techniques to generate a high-quality test suite for learning models.

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

The POLLUX CORE project VoteVerif (Verification of Voter-Verifiable Voting Protocols) has finished. Despite numerous problems with human resources, both with respect to the PhD candidate and the postdoc positions, we achieved most of the project objectives. In particular, we developed a number of algorithms for verification of human aspects of voting protocols, and implemented them in a prototype verification tool.

VoteVerif was a joint project with the Polish Academy of Sciences in Warsaw, Poland and the Polish-Japanese IT Academy in Gdansk, Poland. The collaboration went very well. Besides research outcomes, it resulted in a follow-up POLLUX CORE project STV, which began in September 2019.

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
Funding:	Fonds National de la Recherche - CORE - Core Junior
Duration:	1 Mar 2018 – 28 Feb 2021
Members:	• Alfredo RIAL (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 2019, given our basic security definition for SZK protocols, we have defined security for variants and extensions of SZK protocols, which give support for non-interactive proofs, for unlinkability between proofs, and for the case in which the verifier of proofs is also able to modify the state. We have also provided constructions of SZK protocols that fulfill those definitions. We have used SZK protocols for the construction of privacy-preserving protocols for different applications, such as oblivious transfer with access control, loyalty programs, auctions and billing.

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

PhD student Ahmad Tawakuli has completed the first work package of the project and has already initiated the second work package in Q4 2019. Details of the progress were presented in the Successful CET Panel meeting together with the industry partner Goodyear S.A. An investigation of the technical background of the project, which is mainly related to Near Field Communications (NFC) for automotive applications has been completed, and a better understanding of the research challenges and the different concepts has been estab-

lished. The literature review went on to cover aspects related to the second work package, mainly related to simulation of model analysis. A number of fruitful meeting with the industry partner supporting the project took place during the year.

The PhD student has established contact with advisors of Association of the Automotive Industry VDA, Researchers from other Universities and representatives of various trailer manufacturers for support on the project.

B.14 FNR - INTER Projects

INTER/CNRS/14/10367986 Algorithmic Decision Theory

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

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

Description

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

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

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

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

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

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

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

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

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

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) • Peter Browne Roenne (Research Associate)

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

First, we have worked on a collaboration with Karola Marky (TU Darmstadt). We did a literature review of Usability studies in the field of voting and we published a paper at the Voting Workshop (at Financial Crypto).

We continued analyzing the data collected in 2018 in a collaboration with Verena Distler (University of Luxembourg). The experiment was about testing a voting application we developed for the protocol Selene. A first paper has been published in 2019 at the CHI Conference, analyzing the results of the questionnaires given to participants. A deeper analysis of interviews resulted in a paper submitted and published at E-Vote-ID 2019 (TalTech Proceedings).

Regarding the results and the feedback obtained from users, the application has been modified and also translated into German to make a new user study with Karola Marky (TU Darmstadt). The user study has been done and one paper is under submission. In early 2020, other elements from the study will be analyzed.

We also studied formal verification and in particular the formal verification tool Tamarin. We worked on new definitions of privacy and a model has been developed for the protocol Selene. A paper will be submitted in early 2020. Another model for the protocol Electryo has been developed and a paper about the first results has been published and accepted in 2019 for the Voting Workshop at Financial Crypto (early 2020).

Finally, a new user study to evaluate the understanding of coercion-resistance in voting has started. The planning and the design of the study have been discussed in collaboration with Steve Schneider (University of Surrey) and Wojtek Jamroga (University of Luxembourg) and the experiment will start in early 2020.

Secure, Usable and Robust Cryptographic Voting Systems

Acronym:	SURCVS
PI:	Peter Y A RYAN
Funding:	Fonds National de la Recherche - INTER
Duration:	1 Nov 2018 – 31 Oct 2022
Members:	• Peter Y A RYAN (Principal Investigator) • Sjouke MAUW (Collaborator) • Jun PANG (Collaborator)
Areas:	• Computer Science & ICT Security • Security, Reliability and Trust in Information Technology
Partner:	Norwegian University of Science and Technology

Description

This project will investigate the security of voting systems and increase our assurance in state-of-the-art voting systems. We have
identified three specific areas which are critical in progressing towards adoption of modern voting systems to the benefit of society.

User confidence: Most users are not interested in the cryptographic details, but user acceptance relies on an understanding of the processes involved. Voting systems must be designed so that voters believe in their security and integrity.

Security proofs: In the cryptographic community it is now routine to provide a mathematical security proof for algorithms and protocols. This is not typically the case for electronic voting systems deployed today. Obtaining such proofs for typical complex voting systems will require innovative proof methods.

Long-term security: Electronic records will be protected by cryptography, but they will be public and must remain secure into the future. A specific long-term threat against most existing voting system is quantum computers. This project will address each of these areas. We will contribute to increased confidence in our voting systems, and thereby also in the integrity of the electoral process.

Our emphasis on security proofs for voting systems will improve the overall assurance of voting systems, both directly and by establishing a scientific standard in the field of voting systems.

This project will also generate new knowledge with regard to cryptographic protocols, in particular about protocols involving humans and the practicability of automatic verification for complicated, real-world protocols.

Results

In collaboration with NTNU Norway, several new e-voting protocols have been developed and presented in 2019, especially for coercion-resistant voting, quantum-safe voting and schemes providing everlasting privacy.

Work was performed on designing and formally analyzing post-quantum secure e-voting systems [2, 3], and on systematically analyzing techniques for verifiable mix nets which are important building blocks for many secure e-voting systems [1].

[1] SoK: Techniques for Verifiable Mix Nets. Thomas Haines and Johannes Mueller. Under submission at IEEE CSF 2020.

[2] A Practical Lattice-Based E-Voting Scheme with End-to-End Verifiability. Xavier Boyen and Thomas Haines and Johannes Mueller. Under submission at IEEE S&P 2020.

[3] A Verifiable and Practical Lattice-Based Decryption Mix Net with External Auditing. Xavier Boyen and Thomas Haines and Johannes Mueller. Under submission at ACNS 2020.

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.

B.15 FNR - JUMP Projects

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)

B.16 FNR (Luxembourg)/NCBiR (Poland) Projects

Socio-Technical Verification of Information Security and Trust in Voting Systems

Acronym:	STV
PI:	Peter Y A RYAN
Funding:	FNR (Luxembourg)/NCBiR (Poland)
Duration:	1 Sep 2019 – 31 Aug 2022
Members:	• Peter Y A RYAN (Principal Investigator) • Wojciech JAMROGA (Research Associate) • Gabriele LENZINI (Senior Researcher)

B.17 FNR - POC Projects

Swarm Intelligent Mission systeMS

http://simms.lu

Acronym:	SIMMS
PI:	Grégoire DANOY
Funding:	Fonds National de la Recherche - POC
Budget:	338,860.00 €
Duration:	1 Feb 2019 – 31 Oct 2020
Members:	• Grégoire DANOY (Principal Investigator) • Pascal BOUVRY (Scientific and Technology Mentoring) • Pierre-Yves HOUITTE (Research and Development Specialist)
Area:	Intelligent and Adaptive Systems

Description

SIMMS brings a set of innovative algorithms to create a distributed (swarm) intelligence that allows autonomous, highly effective, cost efficient, and coordinated undertaking of missions by mobile vehicles, principally drones. This plug-and-play A.I. (Artificial Intelligence) technology, in the form of a ‘smart

box', can be used and tailored to all sorts of monitoring, securitisation, rescue or tracking missions. The smart box is compatible with major brands of mobile robots and drones, such as Parrot, DJI, etc.

The integration of SIMMS' proprietary A.I. technology with off-the-shelf sensorial and visualisation technology results in the fully autonomous and coordinated execution of swarm missions The use of swarms of from two to tens of autonomous robots, results in the opportunity to cover greater areas, achieve missions in a fast and efficient way, a higher accuracy and reliability and above all a much more cost effective deployment of technology.

Results

A first prototype of the SIMMS product is currently implemented. Initial tests with a flying swarm of three professional drones have been successfully conducted in real conditions (http://simms.lu/gallery).

SIMMS has gained visibility thanks to its new website (http://simms.lu/) and to its participation to events like the SnT Partnership Day in Luxembourg and the 3rd Digital Construction Show in Brussels. We had many opportunities to demonstrate how swarming can open new business perspectives.

B.18 FNR - PRIDE Projects

Security and Privacy for System Protection

Acronym:	PRIDE: SPsquared
Reference:	R-AGR-3125
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - PRIDE
Budget:	3,037,120.00 €
Duration:	1 Oct 2016 – 30 Jun 2023
Members:	• Sjouke MAUW (Principal Investigator) • Alexei BIRYUKOV (Collaborator) • Jean-Sébastien CORON (Collaborator) • Thomas ENGEL (Collaborator) • Jacques KLEIN (Collaborator) • Gabriele LENZINI (Collaborator) • Christian MULLER (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

Partner: David Naccache (Université de Paris - II)

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

SaToSS has made the following progress for the project:

- The paper "A graph-based approach to explore relationship between hashtags and images" has been published in the Proceedings of the 20th International Conference on Web Information System Engineering (2019).
- Dr. Jun Pang taught the course "Social Network Analysis" as a part of the DTU training program, granting 1 ECTS.
- Semen Yukov joined as a PhD student in April 2019.
- Husam al-Jawaheri joined as a PhD student in July 2019

B.19 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) • Daniel STOLFI ROSSO (Post-Doc)
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.

Results

Our research on the optimisation of the chaotic parameters of our Unmanned Aerial Vehicles (UAVs) swarming mobility model using a surrogate-based approach has been published in the Journal of Computational Science (Elsevier) [10993/35500].

Our follow-up work on the optimisation of the CACOC mobility model for UAV swarms using (co-)evolutionary genetic algorithms has been accepted as a conference paper in the 2020 17th IEEE Annual Consumer Communications & Networking Conference (CCNC) in Las Vegas, NV, USA.

B.20 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)

B.21 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 pro-

vide user-sensitive predictions. Aspects of sentiment analysis in chatbots are analysed.

Decentralized global decision-making over dynamic networks of proactive engines

Acronym:	Proactive PhD 4
PI:	Denis ZAMPUNIERIS
Funding:	University of Luxembourg
Duration:	1 Nov 2019 – 1 Nov 2022
Members:	• Denis ZAMPUNIERIS (Principal Investigator) • Parisa MAHYA (Doctoral Candidate) • Sandro REIS (Research assistant)

Description

Proactive Computing is a recent research field, which aims at the development of new IT systems and software applications that work in a more autonomic way for the user's interests. Based on predefined scenarios, the system decides alone about its actions for reacting in a swift and best appropriate way to the changes in its environment, without the command of human beings. Implementing such complex systems into large and/or complex real-world environments often requires one to connect several proactive engines over a dynamic network, for multiple reasons such as geographic proximity of the engines with sensors or actuators, specific computing capacities in engines, redundancy of engines for safer robustness, etc. Each proactive engine taking its decisions locally and acting on its immediate surrounding only, it becomes necessary to add on top of this architecture, a distributed logic for decision-making based on the communication possibilities offered by the network and the computation power embedded in each node. This logic should allow the system of systems to apply uniform management rules and strategies to achieve its global objectives, to deal with potential conflicts between local decisions or their effects, and to pursue goals dedicated to some global optimization purposes.

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 aforementioned 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 continued contributing to the cryptanalysis methods based on the division property, which is commonly believed to be one of the most powerful tools for the cryptanalysis of symmetric-key ciphers. One result is that the project team further optimized their work at CRYPTO 2018 and applied it to attack more ciphers, which was published in the IEEE Transactions on Computers. The second result is a proposal for a new method to model the division property propagations through a linear layer with a complex matrix. This result will appear at IACR Transactions on Symmetric Cryptology and will be presented at FSE 2020.

Regarding the design context of WP1, the project team contributed to the design, analysis and implementation of SPARKLE, SCHWAEMM and ESCH. The outputs are a specification of an AEAD algorithm and hash function that were submitted to the NIST LWC competition and some source code of reference and optimized implementations.

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) • Frederic PINEL (Researcher) • Emmanuel KIEFFER (Post-Doc) • Hyacinthe CARTIAUX (Technical support) • Clément PARISOT (Research and Development Specialist) • Valentin PLUGARU (Research and Development Specialist)

Description

With the advent of the technological revolution and the digital transformation that made all scientific disciplines becoming computational nowadays, High Performance Computing (HPC) is increasingly identified as a strategic asset and enabler to accelerate the research performed in all areas requiring intensive computing and large-scale Big Data analytic capabilities.

Therefore since 2007, the University of Luxembourg (UL) has invested tens of millions of euro into its own HPC facilities to responds to the growing needs for increased computing and storage. This enabled its researchers to go beyond the limits of traditional simulation. Furthermore, special focus was laid on the development of large computing power combined with huge data storage capacity to accelerate the research performed in intensive computing and large-scale data analytic (Big Data). This characteristic distinguishes the HPC center at the university from many other HPC facilities, which often concentrate on only one of these two pillars. This makes the UL HPC facility the reference implementation within the country, offering a cutting-edge research infrastructure to Luxembourg public research while serving as edge access to the upcoming Euro-HPC Luxembourg supercomputer.

Nowadays, people from the three faculties and the three Interdisciplinary centres within the UL, are users of this facility. 2019 has seen also the first HPC service contracts signed with industrial partners (Arcelor-Mittal, Ceratizit etc.) and more generally, the University extends access to its HPC resources (i.e., facility and expert HPC consultants) to scientific staff of national public organizations and external partners.

The HPC facility is managed by an expert team under the responsibility of

Prof. Pascal Bouvry (Head) and Dr. Sebastien Varrette (Deputy Head), PC for research. The UL HPC platform has kept growing over time thanks to the continuous efforts of the core HPC team (Dr. S. Varrette, V. Plugaru, S. Peter, H. Cartiaux, C. Parisot, Dr. F. Pinel, Dr. E. Kieffer and E. Krishnasamy - contact: hpc-team@uni.lu). Installed in the premises of the University's Centre de Calcul (CDC), it provides in 2019 a total computing capacity of 1,26 PetaFlops (1 PetaFlops = 10^{15} floating point operations per second) across several clusters of compute nodes, and around 10 PetaByte of shared data storage. A total of 756 servers are operated by the team to pilot the HPC platform and the other deployed services for research such as Gforge and GitLab used by hundreds of researchers. 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. It also consolidates the University's ambition to offer a cutting-edge research infrastructure to Luxembourg public research while serving as edge access to the upcoming Luxembourg MeluXina supercomputer in the EuroHPC context.

From its reputation and national expertise in the HPC and Big Data domains, the University of Luxembourg through its Delegate (Prof. Pascal Bouvry) and Advisor (Dr. Sebastien Varrette), has been chosen by the ministry to represent the country within PRACE (Partnership for Advanced Computing in Europe). The UL is also member of ETP4HPC - European Technology Platform (ETP) in the area of High-Performance Computing (HPC) and involved to support the EuroHPC development in the country, in particular with regards the upcoming Luxembourg MeluXina supercomputer or the implementation of the HPC Competence Center, both scheduled for 2020.

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.

Proactive computing paradigm applied to the programming of robotic systems

Acronym:	Proactive PhD 3
PI:	Denis ZAMPUNIERIS
Funding:	University of Luxembourg
Duration:	1 Oct 2019 – 1 Oct 2022
Members:	• Denis ZAMPUNIERIS (Principal Investigator) • Samira CHAYCHI (Doctoral Candidate) • Sandro REIS (Research assistant)

Description

Proactive Computing is a recent research field which aims at the development of new IT systems and software applications that work in a more autonomic way for the user's interests. Based on predefined scenarios, the system decides alone about its actions for reacting in a the swift and best appropriate way to the changes in its environment, without the command of human beings. The user is no more involved in a continuous interactive loop with the system but is now placed on top of it: he/she is solicited by the system only if the system cannot act by itself.

Nowadays most of the robotic systems are programmed using traditional imperative or object-oriented languages, possibly augmented with real-time, sensor-based and event-based frameworks. This approach leads to intricate code where the pursue of objectives and needs for system management is mixed.

We propose to oppose to this approach, by programming a robotic system with a set of proactive scenarios running in parallel, each one devoted either to a part of the objectives or to some specific system control. This would lead to a better separation of concerns in the code, and consequently to easier development and maintenance. The challenges are numerous and the thesis will concentrate on a few of them, to be decided with the candidate.

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
Members:	• Jun PANG (Principal Investigator) • Thomas SAUTER (Co-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 ”Controlling large Boolean networks with temporary and permanent perturbations” has been published in the Proceedings of the 23rd International Symposium on Formal Methods (2019).
- The paper ”Sequential reprogramming of Boolean networks made practical” has been published in the Proceedings of the 17th International Conference on Computational Methods in Systems Biology (2019).
- The poster ”Scalable control of asynchronous Boolean networks” has been published in the Proceedings of the 17th International Conference on Computational Methods in Systems Biology (2018).
- The paper ”Algorithms for the sequential reprogramming of Boolean networks” has been published in IEEE/ACM Transactions on Computational Biology and Bioinformatics (2019).
- The paper ”Controlling large Boolean networks with single-step perturbations” has been published in Bioinformatics (2019).
- The paper ”A new decomposition-based method for detecting attractors in synchronous Boolean networks” has been published in Science of Computer Programming (2019).

- The paper ”GPU-accelerated steady-state computation of large probabilistic Boolean networks” has been published in Formal Aspects of Computing (2019).
- The paper ”Taming asynchrony for attractor detection in large Boolean networks” has been published in IEEE/ACM Transactions on Computational Biology and Bioinformatics (2019).

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
Members:	• Nicolas NAVET (Principal Investigator) • Sebastian ALTMEYER (Co-Supervisor)
Area:	Security, Reliability and Trust in Information Technology

Description

Despite a lot of R&D efforts, the productivity in the development of CPS remains limited. This can be largely explained by the lack of automation in the design, implementation and verification of these systems. At best, today's development framework hides away from the designer platform specific implementation details and configuration issues, but the design and coding work is mainly done manually.

The aim of this Phd thesis is to explore the use of machine learning and optimization techniques to generate solutions that meet high-level design requirements under some hypotheses on the environment (possible faults happening at runtime, processing capacities, etc). We believe that significant progresses can be made by further automating the design process using techniques blending both the best practices in the field (e.g. proofs from the literature, coding standards, safety standards, etc) and machine learning. The aim is to help designers optimize their solution and allow them consider novel alternatives identified leveraging on AI techniques and today's computing power.

One promising technique to master the complexity of designing and configuring complex embedded systems, like the Electrical and Electronic (E/E) architecture of a vehicle platform, is Design-Space Exploration (DSE) algorithms, that is design decisions based on the systematic exploration of the search space. DSE algorithms typically consist of three distinct steps: creating candidate solutions, configuring these solutions and evaluating their performance. This

last step, performed by simulation or mathematical analysis, is compute intensive and drastically limits the size of the search space that can be explored. In this project, we ask if Machine Learning (ML) can provide a viable alternative to mathematical analysis or simulation to determine whether an embedded systems meets a set of performance constraints. The approach is applied to the design of Ethernet TSN based communication architectures as used in the automotive or industrial domains.

B.22 UL and External Organisation Funding Projects

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

http://acc.uni.lu/strips

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 like names or 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.

Project Members:

- Prof Dr Peter Gilles
- Prof Dr Christoph Schommer
- Dr Joshgun Sirajzade
- Dr Christoph Purschke
- MSc. Daniela Gierschek
- Thanks to the students from the 1GSO-Abschlussklasse des Lycée Nic-Biever, Dudelange.
- Thanks to the students from the école privée Sainte-Sophie, Luxembourg-Kirchberg.

Prospective students: Anna Felix (Master), Rosito Gerbo (Erasmus Mundus, Torino, Italy).

Former participants: Elisabeth Joy (Department of Computer Science), Elida van Nierop (Department of Mathematics), Rik Lamesch (Department of Mathematics)

Publications:

- Joshgun Sirajzyade, C. Schommer The LuNa Open Toolbox for the Luxembourgish Language. In Conference Proceedings Advances in Data Mining, Applications and Theoretical Aspects. New York (2019).
- Joshgun Sirajzade, Daniela Gierschek, Christoph Schommer and Peter Gilles. Component analysis of adjectives in Luxembourgish for detecting sentiments. Computational Linguistics in the Netherlands (CLIN 29) (2019).
- Daniela Gierschek. Automatic Detection of Sentiment in Luxembourgish User Comments. CL-Postersession at the 41st Annual Conference of the German Linguistic Society (2019).
- Daniela Gierschek, Peter Gilles, Christoph Purschke, Christoph Schommer, Joshgun Sirajzade. A Temporal Warehouse for Modern Luxembourgish Text Collections. DH Benelux (2019).
- Elida van Nierop. Improving LDA Topic Modelling using word embeddings. Master Thesis (2018).
- Joshgun Sirajzade, Christoph Schommer. Mind and Language. AI in an Example of Similar Patterns of Luxembourgish Language. Proceedings International Conference on Artificial Intelligence and Humanities. Seoul, Korea (2018).
- Daniela Gierschek. Automatic Detection of Emotions in Luxembourgish User Comments. PhD Forum at the European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD) 2018.
- Ekaterina Kamlovskaya, Christoph Schommer, Joshgun Sirajzade. A Dynamic Associative Memory for Distant Reading. Proceedings International Conference on Artificial Intelligence and Humanities. Seoul, Korea (2018).
- Joshgun Sirajzade. Korpusbasierte Untersuchung der Wortbildungsaffixe im Luxemburgischen. Technische Herausforderungen und linguistische Analyse am Beispiel der Produktivität. Zeitschrift für Wortbildung = Journal of Word Formation (2018), 2(1).

In the press:

- Wéi si se geduecht: Positiv? Negativ? Neutral? RTL Kultur news (16 December 2019). Luxemburger Wort. 24 April 2019: Luxemburgish ganz Digital: Schnëssen und Strips: So funktioniert moderne Sprachforschung an der Universität Luxemburg. von Birgit Pfaus-Ravida

B.23 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

In 2019, Secan-Lab continued its work on this project, funded by 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 AVB-capable switches, 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 results showed that AVB/TSN can fulfil the latency requirements of Automotive Ethernet while keeping a constant latency variation under different network traffic loads and various network topologies. The results have been presented to Honda R&D Europe in a final report, and in the Master's Thesis of Sofia Morseletto.

Model Based Design for Real Time Multicore Embedded Platforms in Industrial Motion Control System

PI:	Tingting HU
Funding:	External Organisation Funding
Budget:	28,000.00 €
Duration:	15 Feb 2019 – 15 Feb 2020
Members:	• Tingting HU (Principal Investigator) • Nicolas NAVET (Supervisor / Scientific Advisor)
Areas:	• Computational Sciences • Software and Systems

Description

The research activity focuses on the redesign of the firmware architecture of the existing Robox-designed R execution environment. The innovative aspects of the project are the use of a model-based design language (MBD) from the early design stages and support of multi-core processors. The MBD will not be used as an implementation language due to real-time performance considerations. Instead, its main application areas will be:

- Test different design choices before their implementation.
- Perform timing analysis of the new firmware architecture.
- Provide a formal architectural reference for the implementation.

The design activity can be divided into two parts:

1. Analysis of existing system and new user requirement

- Thorough analysis of the existing design, focusing on components essential for the new design, and identification of critical points in the existing design that may have negative impacts on the performance.
- Gathering and discussion of new and changed user requirements, with respect to the existing design.

2. Design of the new firmware architecture and validation by simulation

- Re-design of the Robox firmware architecture for multi-core platforms, based on the analysis of the existing system and the new user requirements. The new design will be formally specified with the CPAL model-based design language.
- Exploration and comparison of different design alternatives by means of the simulation capability provided by the CPAL execution engine, with key timing information (such as task cycle time, deadline, execution time, etc) provided by Robox.
- Analysis and confirmation of design scalability, especially task scheduling and synchronization, to 2-, 4-, and 8-core processors by means of the multi-interpreter feature of CPAL, exploiting our past experience with multisource software on multicore ECUs. This activity will be carried out based on the information of selected candidate scheduling policies and synchronization mechanisms.

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)
- Raimondas SASNAUSKAS (Post-Doc)
- Ridha SOUA (Post-Doc)
- Emilia TANTAR (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

Secan-lab team focused on the early anomaly detection in Supervisory Control And Data Acquisition (SCADA) systems using Intrusion detection systems (IDS). However, IDSs are facing unprecedented challenges due to the escalation in the number, scale and diversity of attacks. Software-Defined Network (SDN) then comes into play and can provide the required flexibility and scalability. Building on that, we introduced Traffic Agent Controllers that monitor SDN-enabled switches via Open-Flow. By using lightweight statistical metrics such as Kullback-Leibler Divergence, we were able to detect the slightest anomalies, such as stealth port scans, even in the presence of background traffic. The obtained metrics can also be used to locate the anomalies with precision over 90% inside a hierarchical network topology.

Appendix C

Representational Activities

C.1 Conference Committee Memberships

10th ACM Multimedia Systems Conference (MMSys 2019)

Location: Amherst, MA, United States of America, 18 Jun 2019 – 21 Jun 2019.

Participating Members:

- Jean BOTEV (Program Committee Member)

10th International Conference on Ambient Systems Networks and Technologies

http://cs-conferences.acadiau.ca/ant-19/

Location: Leuven, Belgium, 29 Apr 2019 – 2 May 2019.

Description: The 10th International Conference on Ambient Systems, Networks and Technologies (ANT-2019) is a leading international conference for researchers and industry practitioners to share their new ideas, original research results and practical development experiences from all Ambient Systems, Networks and Technologies related areas. ANT 2019 will be held in conjunction with the 2nd International Conference on Emerging Data and Industry 4.0 (EDI40).

Participating Members:

- Ridha SOUA (Track / Working Group Chair)

11th International Workshop on Immersive Mixed and Virtual Environment Systems (MMVE 2019)

Location: Amherst, MA, United States of America, 18 Jun 2019.

Participating Members:

- Jean BOTEV (Steering Committee Member)

12th International Conference of Education Research and Innovation (ICERI 2019)

https://iated.org/iceri/

Location: Seville, Spain, 11 Nov 2019 – 13 Nov 2019.

Participating Members:

- Christian GREVISSE (Program Committee Member)

12th International Conference on Security of Information and Networks (SIN 2019)

https://www.sinconf.org/sin2019/Committee/program.html

Location: Sochi, Russia, 12 Sep 2019 – 15 Sep 2019.

Participating Members:

- Johann GROSZSCHÄDL (PC Member)

13e Université des DPO

Location: Paris, France, 16 Jan 2019.

Participating Members:

- Arianna ROSSI (Invited Speaker)

13th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO 2019)

https://saso2019.cs.umu.se

Location: Umeå, Sweden, 16 Jun 2019 – 20 Jun 2019.

Participating Members:

- Jean BOTEV (Program Committee Member)

13th International Conference on Information Security Theory and Practice (WISTP 2019)

http://www.wistp.org/wistp2019/

Location: Paris, France, 11 Dec 2019 – 12 Dec 2019.

Participating Members:

- Johann GROSZSCHÄDL (PC Member)

13th International Symposium on Theoretical Aspects of Software Engineering

http://www.se.gxnu.edu.cn/tase2019/

Location: Guilin, China, 29 Jul 2019 – 1 Aug 2019.

Description: TASE is an international symposium that aims to bring together researchers and developers from academia and industry with interest in the theoretical aspects of software engineering. Modern society is increasingly dependent on software systems that are becoming larger and more complex. This poses new challenges to current software engineering methodologies that need to be enhanced using modern results from theoretical computer science. We invite submission of research papers on topics covering all theoretical aspects of software engineering, including those describing applications of theoretical computer science in industrial applications and software engineering methodologies.

Participating Members:

- Pierre KELSEN (Program Committee Member)

14th International Conference on Parallel Problem Solving from Nature (PPSN 2016)

http://www.ppsn2016.org/conference/

Location: Edinburgh, United Kingdom, 17 Sep 2019 – 21 Sep 2019.

Participating Members:

- Pascal BOUVRY (Program Committee Member)

14th International Workshop on Security and High Performance Computing Systems (SHPCS 2019)

http://hpcs2019.cisedu.info/2-conference/workshops/workshop10-shpcs

Location: Dublin, Ireland, 15 Jul 2019 – 19 Jul 2019.

Participating Members:

- Johann GROSZSCHÄDL (PC Member)

15th International Conference on Information Security and Cryptology (INSCRYPT 2019)

http://asclab.nuaa.edu.cn/inscrypt2019/

Location: Nanjing, China, 6 Dec 2019 – 8 Dec 2019.

Participating Members:

- Johann GROSZSCHÄDL (PC Member)

16th International Joint Conference on Computer Science and Software Engineering (JCSSE)

https://jcsse.informatics.buu.ac.th/2019/

Location: Chonburi, Thailand, 10 Jul 2019 – 12 Jul 2019.

Participating Members:

- Pascal BOUVRY (Keynote speaker)

17th International Conference on Applied Cryptography and Network Security (ACNS 2019)

http://www.acns19.com/

Location: Bogota, Colombia, 5 Jun 2019 – 7 Jun 2019.

Participating Members:

- Alexei BIRYUKOV (PC Member)

18th Smart Card Research and Advanced Application Conference (CARDIS 2019)

http://cardis2019.fit.cvut.cz/

Location: Prague, Czechia, 11 Nov 2019 – 13 Nov 2019.

Participating Members:

- Luan CARDOSO DOS SANTOS (Paper presentation)

19th Cryptographers' Track at the RSA Conference (CT_RSA 2019)

http://www.venus.dti.ne.jp/matsui/index.html

Location: San Francisco, CA, United States of America, 4 Mar 2019 – 8 Mar 2019.

Participating Members:

- Alexei BIRYUKOV (PC Member)

19th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP 2019)

http://nsclab.org/ica3pp2019/

Location: Melbourne, Australia, 9 Dec 2019 – 11 Dec 2019.

Description: ICA3PP 2019 is the 19th in this series of conferences started in 1995 that are devoted to algorithms and architectures for parallel processing.

Participating Members:

- Grégoire DANOY (Program Committee Member)

1st Annual Zcon Privacy Conference (ZCON 2019)

http://www.zfnd.org/zcon/1/

Location: Split, Croatia, 22 Jun 2019 – 24 Jun 2019.

Participating Members:

- Daniel FEHER (Invited Speaker)

1st Workshop on Verification of Voter-Verifiable Voting Protocols

Location: Luxembourg, Belval, Luxembourg, 20 Nov 2019 – 22 Nov 2019.

Participating Members:

- Wojciech JAMROGA (Main organizer)

20th International Conference on Cryptology in India (INDOCRYPT 2019)

https://www.isical.ac.in/~indocrypt2019/

Location: Hyderabad, India, 15 Dec 2019 – 18 Dec 2019.

Participating Members:

- Qingju WANG (PC Member)

22nd International Conference on the Applications of Evolutionary Computation (Evostar 2019)

http://www.evostar.org/2019/cfp_evoapps.php

Location: Leipzig, Germany, 24 Apr 2019 – 26 Apr 2019.

Description: EvoApplications, the International Conference on the Applications of Evolutionary Computation -formerly known as EvoWorkshops- brings together researchers in a variety of areas of application of Evolutionary Computation and other Nature-inspired techniques.

Participating Members:

- Grégoire DANOY (Program Committee Member)
- Sébastien VARRETTE (Program Committee Member)

22nd International Symposium on Wireless Personal Multimedia Communications (WPMC)

https://wpmc-international-symposium.org/

Location: Lisboa, Portugal, 24 Nov 2019 – 27 Nov 2019.

Description: The 22nd International Symposium on Wireless Personal Multimedia Communications (WPMC - 2019) will be held in Lisbon, Portugal, on November 24-27, 2019. The theme of this year's event is "**DIGITAL TECHNOLOGIES AND BUSINESS TRANSFORMATION**", hosted by Instituto de Telecomunicações (IT) / Instituto Universitário de Lisboa (ISCTE-IUL).

The WPMC symposia series were inaugurated in 1998, as a global platform to enable collaboration in the field of wireless information. Held in Asia, Europe and America, WPMC has established itself as a unique global conference dedicated to wireless multimedia convergence, which over the last half-decade has been jointly held with the Global Wireless Summit (GWS) - the world's largest annual international conference on wireless techno-business modelling. To respond to the trend of rapid digital transformation its acceleration of business activities, processes, competencies, and models, the 22nd WPMC has merged with GWS and its related topics in a common platform for academia, industries and standardization bodies to present and discuss the various opportunities and open challenges to fully leverage the changes and promises of digital technologies and their impact in a strategic and prioritized way.

A key emphasis of this year's conferences is the borderless smart society - bridging across industries, public and private companies, universities, research labs,

and other knowledge societies in exploration of the newest digital technologies and pursuing innovative ways of living, conducting business, travelling, and so forth, towards sustainable solutions for the future.

IT / ISCTE-IUL is actively involved in fundamental and applied research in telecommunications and its supporting sciences, including wireless communications, optical communications, networks and multimedia, at national/international levels. IT also fosters higher education and training, by hosting and tutoring graduate/postgraduate students.

Participating Members:

- Abdelwahab BOUALOUACHE (Technical Program Committee Member)

23rd International Conference on Financial Cryptography and Data Security (FC 2019)

http://fc19.ifca.ai/index.html

Location: Saint Kitts, Saint Kitts and Nevis, 18 Feb 2019 – 22 Feb 2019.

Participating Members:

- Alexei BIRYUKOV (PC Member)

24th European Symposium on Research in Computer Security (ESORICS 2019)

http://esorics2019.uni.lu

Location: Luxembourg, Luxembourg, 23 Sep 2019 – 27 Sep 2019.

Participating Members:

- Alexei BIRYUKOV (Attendant)
- Luan CARDOSO DOS SANTOS (Attendant)
- Daniel FEHER (Attendant)
- Johann GROSZSCHÄDL (Attendant)
- Aleksei UDOVENKO (Attendant)
- Giuseppe VITTO (Attendant)
- Qingju WANG (Attendant)

26th ACM Conference on Computer and Communications Security (CCS 2019)

http://www.sigsac.org/ccs/2019/

Location: London, United Kingdom, 11 Nov 2019 – 15 Nov 2019.

Participating Members:

- Daniel FEHER (Paper presentation)
- Giuseppe VITTO (Paper presentation)
- Alexei BIRYUKOV (Attendant)

26TH IEEE INTERNATIONAL CONFERENCE ON HIGH PERFORMANCE COMPUTING,DATA,AND ANALYTICS (HiPC 2019)

https://hipc.org/

Location: Hyderabad, India, 21 Jun 2019 – 28 Jun 2019.

Participating Members:

- Grégoire DANOY (Program Committee Member)

28th International Joint Conference on Artificial Intelligence IJCAI-19

Location: Macao, China, 10 Aug 2019 – 16 Aug 2019.

Participating Members:

- Giovanni CASINI (Program Committee Member)
- Wojciech JAMROGA (Program Committee Member)
- Emil WEYDERT (Program Committee Member)

2nd Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock 2019)

http://www.cryblock.org

Location: Paris, France, 29 Apr 2019.

Participating Members:

- Daniel FEHER (Paper presentation)
- Sergei TIKHOMIROV (Attendant)

2nd Workshop on Information Management in Human-Centric Systems (IMHCS'19)

Location: Shenyang, China, 21 Oct 2019 – 23 Oct 2019.

Participating Members:

- Alfredo CAPOZUCCA (Program Committee Member)

35th IEEE International Conference on Data Engineering (ICDE 2019)

Location: Macao, Macao, 8 Apr 2019 – 11 Apr 2019.

Participating Members:

- Martin THEOBALD (Paper presentation)

38th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2019)

http://eurocrypt.iacr.org/2019/

Location: Darmstadt, Germany, 19 May 2019 – 23 May 2019.

Participating Members:

- Alexei BIRYUKOV (PC Member, Attendant)

3rd International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2019)

http://deic.uab.cat/conferences/cbt/cbt2019/

Location: Luxembourg, Luxembourg, 26 Sep 2019 – 27 Sep 2019.

Participating Members:

- Alexei BIRYUKOV (Program Committee Co-Chair)
- Daniel FEHER (Attendant)

- Giuseppe VITTO (Attendant)

3rd NIST Lightweight Cryptography Workshop (LWC 2019)

http://csrc.nist.gov/Events/2019/lightweight-cryptography-workshop-2019

Location: Washington, D.C., United States of America, 4 Nov 2019 – 6 Nov 2019.

Participating Members:

- Luan CARDOSO DOS SANTOS (Paper presentation)

40th IEEE Real-Time System Symposium (RTSS 2019)

http://2019.rtss.org/

Location: Hong Kong, China, 3 Dec 2019 – 6 Dec 2019.

Participating Members:

- Tingting HU (Sub-reviewer)

41st Cognitive Science Conference

https://cognitivesciencesociety.org/cogsci-2019/

Location: Montreal, Canada, 24 Jul 2019 – 27 Jul 2019.

Description: 41st CogSci - Annual Conference of the Cognitive Science Society

Participating Members:

- Christoph SCHOMMER (Attendant)

48th Argentine Symposium of Education in Informatics

Location: Salta, Argentina, 16 Sep 2019 – 20 Sep 2019.

Participating Members:

- Alfredo CAPOZUCCA (Program Committee Member)

4th IEEE European Symposium on Security and Privacy (EUROSP 2019)

http://www.ieee-security.org/TC/EuroSP2019/

Location: Stockholm, Sweden, 17 Jun 2019 – 19 Jun 2019.

Participating Members:

- Sergei TIKHOMIROV (Paper presentation)

4th Workshop on Advances in Secure Electronic Voting (VOTING 2019)

Location: St. Kitts Marriott Resort, Saint Kitts and Nevis, 22 Feb 2019.

Participating Members:

- Peter ROENNE (Co-Chair)
- Peter Y A RYAN (Program Committee Member)

5th IEEE Conference on Standards for Communications and Networking

https://cscn2019.ieee-cscn.org/about/

Location: Granada, Spain, 28 Oct 2019 – 30 Oct 2019.

Participating Members:

- Nader SAMIR LABIB (Paper presentation)

5th Workshop on Critical Automotive applications: Robustness & Safety (CARS)

http://conf.laas.fr/cars/CARS2019/

Location: Napoli, Italy, 17 Oct 2019.

Description: The CARS workshop is a forum focusing on architecture, methods and development techniques for safety-related automotive embedded systems and applications.

Participating Members:

- Nicolas NAVET (Program Committee Member)

6th International Workshop on Secure Internet of Things (SIOT 2019)

http://siot-workshop.org/2019/

Location: Luxembourg, Luxembourg, 26 Sep 2019.

Participating Members:

- Luan CARDOSO DOS SANTOS (Attendant)
- Johann GROSZSCHÄDL (Attendant)

6th International Workshop on Self-Improving System Integration (SISSY 2019)

Location: Umeå, Sweden, 16 Jun 2019.

Participating Members:

- Jean BOTEV (Program Committee Member)

7th IEEE Conference on Communications and Network Security (CNS 2019)

http://cns2019.ieee-cns.org

Location: Washington, D.C., United States of America, 10 Jun 2019 – 12 Jun 2019.

Participating Members:

- Daniel FEHER (Paper presentation)

7th International Conference on Future Internet of Things and Cloud

http://www.ficloud.org/2019/

Location: Istanbul, Turkey, 26 Aug 2019 – 28 Aug 2019.

Description: The theme of this conference is to promote the state of the art in scientific and practical research of the IoT and cloud computing. It provides a forum for bringing together researchers and practitioners from academia, industry, and public sector in an effort to present their research work and share research and development ideas in the area of IoT and cloud computing.

Participating Members:

- Qin MA (Program Committee Member)

7th International Workshop on Self-Optimisation in Autonomic & Organic Computing Systems (SAOS 2019)

Location: Copenhagen, Denmark, 20 May 2019.

Participating Members:

- Jean BOTEV (Co-Chair)

7th International Workshop on Strategic Reasoning SR 2019

Location: Macao, China, 10 Aug 2019.

Participating Members:

- Wojciech JAMROGA (Program Committee Member, Keynote speaker)

9th ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (DIVANet'19)

http://symposium.nsercdiva.com/2019/index.html

Location: Miami Beach, Florida, United States of America, 25 Nov 2019 – 29 Nov 2019.

Participating Members:

- Nader SAMIR LABIB (Paper presentation)

9th IEEE Workshop Parallel / Distributed Combinatorics and Optimization (PDCO 2019)

https://pdco2019.sciencesconf.org

Location: Rio de Janeiro, Brazil, 20 May 2019 – 24 May 2019.

Description: The IEEE Workshop on Parallel / Distributed Combinatorics and Optimization aims at providing a forum for scientific researchers and engineers on recent advances in the field of parallel or distributed computing for difficult combinatorial optimization problems, like 0-1 multidimensional knapsack problems, cutting stock problems, scheduling problems, large scale linear programming problems, nonlinear optimization problems and global optimization problems. Emphasis is placed on new techniques for the solution of these difficult problems like cooperative methods for integer programming problems. Techniques based on metaheuristics and nature-inspired paradigms are considered. Aspects related to Combinatorial Scientific Computing (CSC) are considered. In particular, we solicit submissions of original manuscripts on sparse matrix computations, graph algorithm and original parallel or distributed algorithms. The use of new approaches in parallel and distributed computing like GPU, MIC, FPGA, volunteer computing are considered. Application to cloud computing, planning, logistics, manufacturing, finance, telecommunications and computational biology are considered.

Participating Members:

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

9th International Workshop on Socio-technical Aspects in Security

Location: Luxembourg, Luxembourg, 26 Sep 2019.

Participating Members:

- Peter Y A RYAN (Program Committee Member)
- Itzel VAZQUEZ SANDOVAL (Website Chair)

ACM International Conference on Research in Adaptive and Convergent Systems (RACS 2019)

Location: Chongqing, China, 24 Sep 2019 – 27 Sep 2019.

Description: RACS provides an excellent forum for addressing research issues of concern within the adaptive and convergent computing area. Adaptive and convergent computing concentrates on innovative solutions to complex prob-

lems in all areas of industry and sciences using adaptive and convergent techniques in computer science and engineering. It involves programming, software engineering, graphics, databases, wireless networks, security, distributed systems, operating systems and so on.

Participating Members:

- Nicolas NAVET (Program Committee Member)

ACM SIGMOD/PODS International Conference on Management of Data (SIGMOD 2019)

Location: Amsterdam, Netherlands, 30 Jun 2019 – 5 Jul 2019.

Participating Members:

- Martin THEOBALD (Paper presentation)

Benelux Conference on Artificial Intelligence and Machine Learning Conference of Belgium and the Netherlands (BNAIC 2019)

https://bnaic19.brussels

Location: Brussels, Belgium, 6 Nov 2019 – 8 Nov 2019.

Participating Members:

- Grégoire DANOY (Program Committee Member)
- Leon VAN DER TORRE (Program Committee Member)

Central European Cybersecurity Conference (CECC2019)

Location: Munich, Germany, 14 Nov 2019 – 15 Nov 2019.

Participating Members:

- Peter Y A RYAN (Program Committee Member)

Computer Privacy and Data Protection Conference

Location: Brussels, Belgium, 30 Jan 2019 – 1 Feb 2019.

Participating Members:

- Arianna ROSSI (Invited panelist)

Cryptographic Integrated Circuits Conference 2019 (CryptoIC 2019)

http://easychair.org/cfp/CryptoIC2019

Location: Nanjing, China, 9 Aug 2019 – 11 Aug 2019.

Participating Members:

- Johann GROSZSCHÄDL (Invited Speaker)

CYSARM 2019: Workshop on Cyber-Security Arms Race 2019

Location: London, United Kingdom, 15 Nov 2019.

Participating Members:

- Peter Y A RYAN (Program Committee Member)

Deduktionstreffen 2019

https://fg-dedsys.gi.de/veranstaltung/deduktionstreffen-2019

Location: Kassel, Germany, 23 Sep 2019.

Description: The annual meeting **Deduktionstreffen** is the prime activity of the Special Interest Group on Deduction Systems (FG DedSys) of the AI Section of the German Society for Informatics (GI-FBKI). 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 (PC Chair)

DEVOPS 19: Second international workshop on software engineering for continuous development and new paradigms of software production and deployment

Location: Villebrumier, France, 6 May 2019 – 8 May 2019.

Participating Members:

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

Embedded Operating Systems Workshop (EWiLi 2019)

https://sites.google.com/view/ewili2019/home?authuser=0

Location: New York, United States of America, 17 Oct 2019.

Description: The Embedded Operating Systems Workshop (2019) is co-located with Embedded Systems Week.

Participating Members:

- Tingting HU (Program Committee Member)

EMSICC 2019 : The 6th International Workshop on Energy Management for Sustainable Internet-of-Things and Cloud Computing

http://cedric.cnam.fr/workshops/emsicc19/index.html

Location: Istanbul, Turkey, 26 Aug 2019 – 28 Aug 2019.

Participating Members:

- Christian FRANCK (Co-Chair)

ESSLLI 2019 student session

https://esslli2019.folli.info/programme/student-session/

Location: Riga, Latvia, 5 Aug 2019 – 16 Aug 2019.

Description: The **ESSLLI 2019 Student Session** will be held during ESSLLI 2019 at **University of Latvia,** Riga, Latvia, between the dates of August 5 – 16, 2019.

The Student Session is a forum for PhD and Master students to present their research at the interfaces of logic, language and computation. It features three

tracks: Logic & Computation (LoCo), Logic & Language (LoLa), and Language & Computation (LaCo).´

Participating Members:

- Jérémie DAUPHIN (Track / Working Group Chair)
- Alexander STEEN (Program Committee Member)
- Leon VAN DER TORRE (Program Committee Member)
- Emil WEYDERT (Program Committee Member)

EUROPEAN CONFERENCE ON LOGICS IN ARTIFICIAL INTELLIGENCE

https://jelia2019.mat.unical.it/

Location: Rende, Italy, 8 May 2019 – 10 May 2019.

Description: The 16th edition of the European Conference on Logics in Artificial Intelligence will take place in Cosenza, organised by the Department of Mathematics and Computer Science of University of Calabria.

Logics have, for many years, laid claim to providing a formal basis for the study and development of applications and systems in Artificial Intelligence. With the depth and maturity of formalisms, methodologies, and logic-based systems today, this claim is stronger than ever.

The European Conference on Logics in Artificial Intelligence (or Journées Européennes sur la Logique en Intelligence Artificielle - JELIA) began back in 1988, as a workshop, in response to the need for a European forum for the discussion of emerging work in this field. Since then, JELIA has been organised biennially, with proceedings published in the Springer-Verlag series Lecture Notes in Artificial Intelligence. Previous meetings took place in Roscoff, France (1988), Amsterdam, Netherlands (1990), Berlin, Germany (1992), York, UK (1994), Évora, Portugal (1996), Dagstuhl, Germany (1998), Málaga, Spain (2000), Cosenza, Italy (2002), Lisbon, Portugal (2004), Liverpool, UK (2006), Dresden, Germany (2008), Helsinki, Finland (2010), Toulouse, France (2012), Madeira, Portugal (2014), Cyprus, Greece (2016).

The increasing interest in this forum, its international level with growing participation from researchers outside Europe, and the overall technical quality, has turned JELIA into a major biennial forum for the discussion of logic-based approaches to artificial intelligence.

Participating Members:

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

EUROPEAN CONFERENCE ON SYMBOLIC AND QUANTITATIVE APPROACHES TO REASONING WITH UNCERTAINTY (ECSQARU 2019)

http://www.mi.sanu.ac.rs/~ecsqaru2019/

Location: Belgrade, Serbia, 18 Sep 2019 – 20 Sep 2019.

Description: The biennial ECSQARU conferences constitute a major forum for advances in the theory and practice of reasoning under uncertainty, with a focus on bringing symbolic and quantitative aspects together. Contributions come from researchers interested in advancing the scientific knowledge and from practitioners using uncertainty techniques in real-world applications. The scope of the ECSQARU conferences encompasses fundamental issues, representation, inference, learning, and decision making in qualitative and numeric uncertainty paradigms.

Previous ECSQARU events have been held in Lugano (2017), Compiegne (2015), Utrecht (2013), Belfast (2011), Verona (2009), Hammamet (2007), Barcelona (2005), Aalborg (2003), Toulouse (2001), London (1999), Bonn (1997), Fribourg (1995), Granada (1993), and Marseille (1991).

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

EXTRAAMAS@AAMAS 2019

http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=84208&copyownerid=97632

Location: Montreal, Canada, 13 May 2019 – 14 May 2019.

Description: Human decisions are increasingly relying on Artificial Intelligence (AI) techniques implementing autonomous decision making and distributed problem-solving. However, reasoning and dynamics powering such systems are becoming increasingly opaque. Therefore, the societal awareness about the lack of transparency and the need for explainability is rising. As a consequence, new legal constraints and grant solicitations have been defined to enforce transparency and explainability in IT systems. An example is the new General Data Protection Regulation (GDPR) which became effective in Europe in May 2018. Emphasizing the need for transparency in AI systems, recent studies pointed out that equipping intelligent systems with explanative abilities has a positive impact on users, (e.g., contributing to overcome discomfort, confusion, and self-deception due to the lack of understanding). For all these reasons, Explainable Artificial Intelligence (XAI) has recently re-emerged and is considered to be a hot topic in AI, attracting research from domains such as machine learn-

ing, robot planning, and multi-agent systems.

Agents and Multi-Agent Systems (MAS) can have two core contributions for XAI. The first is in the context of personal intelligent systems providing tailored and personalized feedback (e.g., recommendations and coaching systems). Autonomous agent and multi-agent approaches have recently gained noticeable results and scientific relevance in different research domains (e.g., e-health, UAVs,, smart environments). However, despite possibly being correct, the outcomes of such agent-based systems, as well as their impact and effect on users, can be negatively affected by the lack of clarity and explainability of their dynamics and rationality. Nevertheless, if explainable, their understanding, reliability, and acceptance can be enhanced. In particular, user personal features (e.g., user context, expertise, age, and cognitive abilities), which are already used to compute the outcome, can be employed in the explanation process providing a user-tailored solution.
The second axis is agent/robot teams or mixed human-agent teams. In this context, succeeding in collaboration necessitates a mutual understanding of the status of other agents/users/ their capacities and limitations. This ensures efficient teamwork and avoids potential dangers caused by misunderstandings. In such a scenario, explainability goes beyond single human-agent settings into agent-agent or even mixed agent-human team explainability.

The main aim of this first "International workshop on Explainable Transparent Agent and Multi-Agent Systems" (EXTRAAMAS) is four-folded:
(i) to establish a common ground for the study and development of explainable and understandable autonomous agents, robots and MAS,
(ii) to investigate the potential of agent-based systems in the development of personalized user-aware explainable AI,
(iii) to assess the impact of transparent and explained solutions on the user/agents behaviors, and
(iv) to discuss motivating examples and concrete applications in which the lack of explainability leads to problems, which would be resolved by explainability.
Contributions are encouraged in both theoretical and practical applications for transparent and explainable intelligence in agents and MAS. Papers presenting theoretical contributions, designs, prototypes, tools, subjective user tests, assessment, new or improved techniques, and general survey papers tracking current evolutions and future directions are welcome.

Participating Members:

- Amro NAJJAR (Chair)

FISEE 19: First international workshop on frontiers in software engineering education

Location: Villebrumier, France, 11 Nov 2019 – 13 Nov 2019.

Participating Members:

- Alfredo CAPOZUCCA (Programme Chair)

- Nicolas GUELFI (Programme Chair)
- Alfredo CAPOZUCCA (Organizing Chair, Organizing Chair)

Fourth International Joint Conference on Electronic Voting (E-VOTE-ID 2019)

Location: Bregenz, Austria, 1 Oct 2019 – 4 Oct 2019.

Participating Members:

- Peter Y A RYAN (Program Committee Member)
- Peter ROENNE (Chair of Communication and Demos)

Grande Region Security and Reliability Day 2019 (GRSRD 2019)

Location: Nancy, France, 26 Mar 2019.

Participating Members:

- Peter ROENNE (Co-Chair)
- Peter Y A RYAN (Program Committee Member)

Hawaii International Conference on System Sciences

Location: Hawaii, United States of America, 8 Jan 2019 – 11 Jan 2019.

Participating Members:

- Benoit RIES (Minitrack co-chair)

HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES

http://hicss.hawaii.edu/tracks-52/software-engineering-education/

Location: Maui, United States of America, 8 Jan 2019 – 11 Jan 2019.

Description:

For the past 30 years, software engineering education has changed a great deal. In 1986, software engineering education was largely undertaken by industry, with just a few academic software engineering programs in place. The Master of Software Engineering (MSE) reference curriculum changed the landscape of software engineering, resulting in many MSE programs worldwide, not to mention software engineering tracks within Computer Science (CS) masters' programs. In the years that followed, software engineering education emerged at the undergraduate level, with a documented reference curriculum. Software

engineering professionalism initiatives resulted in the certification and licensing of software engineers in a number of countries worldwide. We are seeing increased attention to software engineering specialty areas, and many software engineering degree programs have tracks to support these specialties.

On the industry side we are seeing an upheaval in software engineering as we know it. Software engineering is pervasive. Innovations such as Cloud Computing, autonomous vehicles, drones, bioengineering, and other initiatives have made for a rapidly changing landscape. Topics such as software assurance, safety, and reliability have become increasingly important knowledge areas. As educators we are challenged to keep up with the emerging trends, to identify suitable software engineering techniques, and to incorporate them into our class offerings. We are in a global economy with a software supply chain that can extend across many countries and regions. Each one has their own regulations and laws about safety, security, and privacy. Practicing software engineers change jobs frequently, so the value of in-house training is not as clear as it once was.

Quality submissions covering curriculum development, empirical studies, personal or institutional experience, conceptual or theoretical work are particularly invited. The list below indicates areas in the focus of this HICSS-52 special track. Submissions on additional topics consistent with the central themes of this track are also welcome.

- Revolutionizing Computer Science and Software Engineering Education: Perspectives and Progress
- Teaching Conceptual Modeling
- Team Development and Project Management
- Assessment
- Measuring Education and Training Results
- Communication With Clients, Peers, Etc.
- Degree Specializations
- Software Assurance, Quality, and Reliability Education
- Cloud Computing Education
- Methodological Aspects of Software Engineering Education
- Global and Distributed Software Development
- Social and Cultural Issues
- Novel Delivery Methods
- Open Source in Education
- Cooperation Between industry and Academia
- Continuous Education to Cope With Technological Change
- Vision For Software Engineering Education in the Future
- E-Learning, Online Training, and Education

Participating Members:

- Benoit RIES (Program Committee Member, Minitrack Chair)

HPC School 2019 - Summer School

https://hpc.uni.lu/hpc-school/2019/06/index.html

Location: Belval, Luxembourg, 20 Jun 2019 – 21 Jun 2019.

Description: The UL HPC team, together with leading computational scientists of the UL and HPC technologists will offer will offer **instructions, hands-on and guided sessions** (including several new ones) on a variety of topics representative of research activities and domains present at the university, including:

- Access to and interaction with the UL HPC infrastructures
- Monitoring, Debugging & Profiling
- 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 Scalable Science (OpenMP/MPI, Computational Physics, Chemistry & Engineering apps, GPU programming), MATLAB/Mathematica, R, Python, Big Data analytics, Bioinformatic workflows, Deep and Machine learning, Mixed-Integer Programming (MIP) optimization with CPLEX and Gurobi etc.
- Virtualisation with Singularity 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)

IEEE CLOUDCOM 2019

http://2019.cloudcom.org/

Location: Sydney, Australia, 11 Dec 2019 – 13 Jan 2020.

Description: CloudCom is the premier conference on Cloud Computing worldwide, attracting researchers, developers, users, students and practitioners from the fields of big data, systems architecture, services research, virtualization, security and privacy, high performance computing, always with an emphasis on how to build cloud computing platforms with real impact. The conference is co-sponsored by the Institute of Electrical and Electronics Engineers (IEEE), is steered by the Cloud Computing Association, and draws on the excellence of its world-class Program Committee and its participants.

The 11th IEEE International Conference on Cloud Computing Technology and

Science (CloudCom 2019) will be held in Sydney, Australia on 11-13 December 2019.

Participating Members:

- Valentin PLUGARU (Program Committee Member)

IEEE Congress on Evolutionary Computation (CEC 2019)

Location: Wellington, New Zealand, 10 Jun 2019 – 13 Jun 2019.

Participating Members:

- Grégoire DANOY (Program Committee Member)

IEEE Global Communications Conference (GLOBECOM)

https://globecom2019.ieee-globecom.org/

Location: Waikoloa, HI, United States of America, 9 Dec 2019 – 13 Dec 2019.

Participating Members:

- Abdelwahab BOUALOUACHE (Technical Program Committee Member)

IEEE ICC 2019,2nd International Workshop on 5G and Cooperative Autonomous Driving (5G Auto)

https://icc2019.ieee-icc.org/workshop/w12-2nd-international-workshop-5g-and-cooperative-autonomous-driving-5g-auto

Location: Shanghai, China, 24 May 2019.

Description: With the emergence of highly automated and autonomous driving vehicles, rigorous requirements in terms of responsiveness, security, resiliency and scalability are needed to enable new services that improve efficiency and safety on the road.

The recent progress on 5G ultra reliable and low latency communications is paving the way to novel solutions that address these challenging requirements. To this end, a plethora of paradigms, (such as Fog/Multi-Access Edge computing, Software Defined Networking, Network Function Virtualization); emerging protocols for V2X communication (LTE-V, C-V2X, etc.) and advanced localisation/navigation systems (3D High Definition maps, Advanced Driver Assistance Systems) have been proposed or are still under development to support future 5G road safety use cases.

Therefore, in the path towards fully autonomous and safe coordinated driving, 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 behaviours 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)

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

https://infocom2019.ieee-infocom.org/workshop-integrating-edge-computing-caching-and-offloading-next-generation-networks

Location: Paris, France, 29 Apr 2019 – 2 May 2019.

Description: Cloud computing has been widely adopted to enable convenient access to a shared pool of computing resources. Nevertheless, as the distance between the cloud and the edge device is usually large, cloud computing services may not provide guarantees to low latency applications, and transmitting a large amount of data (e.g., in big data analytics) from the device to the cloud may not be feasible or economical. To address these issues, edge (fog) computing has been proposed to deploy computing resources closer to end users. Edge computing allows edge devices to perform computation offloading to offload their computational tasks to the edge server, which executes the computational tasks on behalf of the edge devices. Another new technology called information-centric networking (ICN) has been extensively studied in recent years. In-network caching is used in ICN to reduce the duplicate content transmission in networks. ICN-based caching has been recognized as one of the promising techniques for future wireless/wired networks.

Recently, there is a phenomenal burst of research activities in integrating edge computing, caching, and offloading in next generation networks. From the perspective of applications (e.g., video), network, cache and compute are underlying resources enabling these applications. How to manage, control and optimize these resources can have significant impacts on the performance of applications.

The Workshop on ”Integrating Edge Computing, Caching, and Offloading in Next Generation Networks” provides a forum that brings together industry and academia, engineers and researchers to discuss up-to-date developments in integrating edge computing, caching, and offloading in next generation net-

works.

Participating Members:

- Matthias R. BRUST (Program Committee Member)

Intelligent Networking and Collaborative Systems (INCoS-2019)

http://voyager.ce.fit.ac.jp/conf/incos/2019/information.php

Location: Oita, Japan, 5 Sep 2019 – 7 Sep 2019.

Participating Members:

- Grégoire DANOY (Program Committee Member)

International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2019)

http://aamas2019.encs.concordia.ca/

Location: Montreal, Canada, 13 May 2019 – 17 May 2019.

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).

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), São Paulo (2017) and Stockholm, Sweden (2018).

Participating Members:

- Grégoire DANOY (Program Committee Member)

International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2019)

http://aamas2019.encs.concordia.ca/

Location: Montreal, Canada, 13 May 2019 – 17 May 2019.

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).

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), São Paulo (2017) and Stockholm, Sweden (2018).

Participating Members:

- Giovanni CASINI (Program Committee Member)
- Réka MARKOVICH (Program Committee Member)
- Alexander STEEN (Program Committee Member)

International Confernce on Optimization and Learning (OLA)

https://ola2019.sciencesconf.org/

Location: Bangkok, Thailand, 29 Jan 2019 – 31 Jan 2019.

Description: OLA is a conference focusing on the future challenges of optimization and learning methods and their applications.

The conference OLA'2019 will provide an opportunity to the international research community in optimization and learning to discuss recent research results and to develop new ideas and collaborations in a friendly and relaxed atmosphere. OLA'2019 welcomes presentations that cover any aspects of optimization and learning research such as new high-impact applications, parameter tuning, 4th industrial revolution, new research challenges, hybridization issues, optimization-simulation, meta-modeling, high-performance and exascale computing, surrogate modeling, multi-objective optimization, optimization for machine learning, machine learning for optimization, optimization and learning under uncertainty.

Accepted papers will be published in the proceedings that will be available at the conference. In addition, a post-conference indexed Springer book will be published. Participants will be invited to submit extended versions of their work for consideration. A special issue in the indexed journal ITOR (International Transactions in Operational Research) is organized (impact factor 2.4).

Participating Members:

- Jean BOTEV (Programme Chair)
- Grégoire DANOY (Programme Chair)
- Matthias R. BRUST (Program Committee Member)
- Gabriel DUFLO (Paper presentation)

International Workshop on Historicity of the Visuality and Image History: New Forms of Digital and Visual History/Humanities

http://www.lvivcenter.org/en/conferences/conferences/3148-19-11-15-dhs/

Location: Lviv, Ukraine, 14 Nov 2019 – 15 Nov 2019.

Participating Members:

- Jean BOTEV (Invited Speaker)

International Workshop on Secure Internet of Things

Location: Luxembourg, Luxembourg, 23 Sep 2019 – 26 Sep 2019.

Participating Members:

- Alfredo RIAL (Program Committee Member)

Internet of Things at IEEE Global Communications Conference 2019

https://globecom2019.ieee-globecom.org/

Location: Waikoloa, HI, United States of America, 9 Dec 2019 – 13 Dec 2019.

Participating Members:

- Ridha SOUA (Track / Working Group Chair)

IoT Week 2019 Aarhus

https://iotweek.org/iot-week-2019-aarhus/

Location: Aarhus, Denmark, 17 Jun 2019 – 21 Jun 2019.

Participating Members:

- Latif LADID (Invited Speaker)
- Ridha SOUA (Invited Speaker)

JELIA 2019

https://jelia2019.mat.unical.it/

Location: Rende, Italy, 7 May 2019 – 11 May 2019.

Description: JELIA 2019, the 16th edition of the European Conference on Logics in Artificial Intelligence, is to be held in Cosenza by the Department of Mathematics and Computer Science, University of Calabria.

Logics have, for many years, laid claim to providing a formal basis for the study and development of applications and systems in Artificial Intelligence. With the depth and maturity of formalisms, methodologies, and logic-based systems today, this claim is stronger than ever.

The European Conference on Logics in Artificial Intelligence (or Journées Européennes sur la Logique en Intelligence Artificielle - JELIA) began back in 1988, as a workshop, in response to the need for a European forum for the discussion of emerging work in this field. Since then, JELIA has been organised biennially, with proceedings published in the Springer-Verlag series Lecture Notes in Artificial Intelligence. Previous meetings took place in Roscoff, France (1988), Am-

sterdam, Netherlands (1990), Berlin, Germany (1992), York, UK (1994), Évora, Portugal (1996), Dagstuhl, Germany (1998), Málaga, Spain (2000), Cosenza, Italy (2002), Lisbon, Portugal (2004), Liverpool, UK (2006), Dresden, Germany (2008), Helsinki, Finland (2010), Toulouse, France (2012), Madeira, Portugal (2014), Larnaca, Cyprus (2016).

The increasing interest in this forum, its international level with growing participation from researchers outside Europe, and the overall technical quality, has turned JELIA into a major biennial forum for the discussion of logic-based approaches to artificial intelligence.

Participating Members:

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

JURIX 2019

https://jurix2019.oeg-upm.net/index.html

Location: Madrid, Spain, 11 Dec 2019 – 13 Dec 2019.

Description: JURIX 2019 is the 32nd International Conference on Legal Knowledge and Information Systems organised by the Foundation for Legal Knowledge Based Systems (JURIX) since 1988. JURIX 2019 is hosted by the Ontology Engineering Group (Artificial Intelligence Department, Universidad Politécnica de Madrid).

Participating Members:

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

KI 2019: Doctoral Consortium

https://www.ki2019.de/dc/

Location: Kassel, Germany, 23 Sep 2019 – 26 Sep 2019.

Description: The doctoral consortium provides an opportunity for PhD students to discuss their research interests and career objectives with established researchers in AI and network with other participants. The doctoral consortium will expose students to different areas of research within AI and help build professional connections within the international community of AI researchers.

The technical program of presentations, workshops, and tutorials is comple-

mented by a doctoral consortium that invites PhD students at a stage in which critique can still be integrated and from any subject area within AI. Each presented topic will be mentored by a senior researcher. This provides the opportunity for a private discussion of the PhD topic. The goals of the doctoral consortium are:

- to provide PhD students with the opportunity to present their ongoing research and receive feedback from established researchers;
- to promote networking among PhD students and AI researchers in general, both on a national and an international level;
- to support students with advice on academic, research, and industrial careers.

Participating Members:

- Alexander STEEN (Program Committee Member)

KI-Camp 2019

https://www.wissenschaftsjahr.de/2019/ki-camp/

Location: Berlin, Germany, 5 Dec 2019.

Description: In interaktiven Workshops, offenen Fishbowl-Diskussionen und spontanen Barcamp-Sessions widmeten sich die Teilnehmenden dabei drängenden Zukunftsfragen aus den Themenfeldern Gesellschaft, Wissenschaft, Gesundheit, Mobilität, Produktion und Nachhaltigkeit. Das Event bot jungen Forscherinnen und Forschern die Möglichkeit, sich über Disziplingrenzen hinweg zu vernetzen und zusammen mit Expertinnen und Experten aus Wirtschaft, Wissenschaft und Politik aktuelle Herausforderungen des KI-Forschungsstandorts Deutschland zu diskutieren.

In Kooperation mit dem Projekt #KI50: Künstliche Intelligenz in Deutschland – gestern, heute, morgen wurden darüber hinaus in einer abendlichen Ehrungsfeier 10 KI-Newcomerinnen und -Newcomer unter 30 gekürt.

Participating Members:

- Alexander STEEN (Panelist)

Kunstliche Intelligenz (KI 2019)

https://www.ki2019.de/

Location: Kassel, Germany, 23 Sep 2019 – 26 Sep 2019.

Description: KI 2019 is the 42nd edition of the German Conference on Artificial

Intelligence organized in cooperation with the AI Chapter of the German Society for Informatics (GI-FBKI).

KI traditionally brings together academic and industrial researchers from all areas of AI, providing an ideal place for exchanging news and research results of intelligent system technology.

Participating Members:

- Alexander STEEN (Workshop Organiser / Co-Organiser)

LegalDesign & LegalTech seminars

Location: Milan, Italy, 18 Dec 2019 – 19 Dec 2019.

Participating Members:

- Arianna ROSSI (Invited Speaker)

Malware Day

Location: Rennes, France, 23 May 2019.

Participating Members:

- Ziya Alper GENÇ (Invited Speaker)

Microservices DevOps and Service-Oriented Architecture at the 34th ACM/SIGAPP Symposium On Applied Computing (SAC-MiDOS 2019)

https://midos2019.sdu.dk/

Location: Limassol, Cyprus, 8 Apr 2019 – 12 Apr 2019.

Participating Members:

- Ross James HORNE (Program Committee Member)

MIREL-19

https://sites.google.com/view/mirelworkshop2019

Location: Madrid, Spain, 11 Dec 2019.

Description: MIREL-2019 workshop aims at **bridging 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 (http://www.mirelproject.eu).

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:

- Réka MARKOVICH (Programme Chair)
- Livio ROBALDO (Program Committee Member)
- Leon VAN DER TORRE (Program Committee Member)
- Giovanni CASINI (Workshop Organiser / Co-Organiser)
- Réka MARKOVICH (Workshop Organiser / Co-Organiser)

Optimization and Simulation (PaCOS 2019,International Workshop on the Synergy of Parallel Computing

http://hpcs2019.cisedu.info/2-conference/workshops/workshop07-pacos

Location: Dublin, Ireland, 15 Jul 2019 – 19 Jul 2019.

Participating Members:

- Grégoire DANOY (Program Committee Member)

PANELFIT workshop on Data Protection in ICT Research and Innovation

Location: Bilbao, Spain, 5 Jun 2019.

Participating Members:

- Arianna ROSSI (Invited Speaker)

Principles of Security and Trust (POST 2019)

Location: Prague, Czechia, 8 Apr 2019 – 11 Apr 2019.

Participating Members:

- Peter Y A RYAN (Program Committee Member)

Privacy Icons Expert Workshop

Location: Berlin, Germany, 27 Feb 2019.

Participating Members:

- Arianna ROSSI (Invited Speaker)

Proceedings on Privacy Enhancing Technologies

Location: Stockholm, Sweden, 16 Jul 2019 – 20 Jul 2019.

Participating Members:

- Alfredo RIAL (Program Committee Member)

RuleML+RR 2019

https://rulemlrr19.inf.unibz.it/

Location: Bolzano, Italy, 16 Jul 2019 – 19 Jul 2019.

Description: The International Joint Conference on Rules and Reasoning (RuleML+RR) is the leading international joint conference in the field of rule-based reasoning. Stemming from the synergy between the well-known RuleML and RR events, one of the main goals of this conference is to build bridges between academia and industry.

Participating Members:

- Alexander STEEN (Short Papers, Posters, and Demo Co-Chair)

Software Verication and Testing track at ACM Symposium on Applied Computing 2019 (SAC-SVT 2019)

https://sites.google.com/site/sacsvt2019/home/call-for-papers

Location: Limassol, Cyprus, 8 Apr 2019 – 12 Apr 2019.

Participating Members:

- Jun PANG (Program Committee Member)

Sommer der KI

https://www.mi.fu-berlin.de/inf/groups/ag-ki/news/Sommer-der-Kuenstlichen-Intelligenz1.html

Location: Berlin, Germany, 15 Jul 2019 – 15 Sep 2019.

Description: FU Berlin, Dept of Computer Science, has organised a ”Summer of Artificial Intelligence”-event for students and scientific stuff.

Participation through 20h lecture as part of the AI-Lecture (with Prof Christoph Benzmüller).

Participating Members:

- Christoph SCHOMMER (Invited Speaker)

Summer School on Real-World Crypto and Privacy 2019

http://summerschool-croatia.cs.ru.nl/2019/

Location: Sibenik, Croatia, 17 Jun 2019 – 21 Jun 2019.

Participating Members:

- Luan CARDOSO DOS SANTOS (Attendant)

Swiss Blockchain Winter School 2019

http://blockchainschool.epfl.ch/

Location: Interlaken, Switzerland, 11 Feb 2019 – 14 Feb 2019.

Participating Members:

- Daniel FEHER (Attendant)
- Sergei TIKHOMIROV (Attendant)

The 11th IEEE International Workshop on Security Aspects for Process and Services Engineering

Location: Milwaukee, United States of America, 15 Jul 2019.

Participating Members:

- Itzel VAZQUEZ SANDOVAL (Program Committee Member)

The 12th EAI International Conference on Bio-inspired Information and Communications Technologies (EAI BICT 2019)

http://bionetics.org/

Location: Pittsburgh, United States of America, 13 Mar 2019 – 14 Mar 2019.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 12thInternational Conference on Security for Information Technology and Communications(SECITC 2019)

Location: Bucharest, Romania, 14 Nov 2019 – 15 Nov 2019.

Participating Members:

- Peter Y A RYAN (Program Committee Member)
- Peter ROENNE (Keynote speaker)

The 13th IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2019)

http://ifiptm2019.compute.dtu.dk/IFIPTM19/IFIPTM.html

Location: Copenhagen, Denmark, 17 Jul 2019 – 19 Jul 2019.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 13th International Conference on Multiple Objective Programming and Goal Programming (MOPGP 2019)

http://mopgp.org/

Location: Marrakech, Morocco, 28 Oct 2019 – 31 Oct 2019.

Participating Members:

- Grégoire DANOY (Program Committee Member)

The 13th International Symposium on Theoretical Aspects of Software Engineering (TASE 2019)

http://www.se.gxnu.edu.cn/tase2019/

Location: Guilin, China, 29 Jul 2019 – 31 Jul 2019.

Participating Members:

- Jun PANG (Program Committee Member)

The 13th WISTP International Conference on Information Security Theory and Practice (WISTP 2019)

http://wistp.org/

Location: Paris, France, 11 Dec 2019 – 12 Dec 2019.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 15th International Workshop on Security and Trust Management (STM 2019)

https://stm2019.uni.lu/

Location: Luxembourg, Luxembourg, 26 Sep 2019 – 27 Sep 2019.

Participating Members:

- Olga GADYATSKAYA (Program Committee Member)
- Sjouke MAUW (Program Committee Co-Chair)
- Olga GADYATSKAYA (Organization Chair)

The 16th International Colloquium on Theoretical Aspects of Computing (ICTAC 2019)

http://www.redcad.org/events/ictac2019/

Location: Hammamet, Tunisia, 30 Oct 2019 – 4 Nov 2019.

Participating Members:

- Ross James HORNE (Program Committee Member)

The 17th IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA 2019)

http://ispa2019.com

Location: Xiamen, China, 16 Dec 2019 – 19 Dec 2019.

Participating Members:

- Grégoire DANOY (Program Committee Member)

The 17th International Annual Conference on Privacy Security and Trust (PST 2019)

https://pstnet.ca/pst2019/

Location: Fredericton, Canada, 26 Aug 2019 – 28 Aug 2019.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 17th International Conference on Applied Cryptography and Network Security (ACNS 2019)

https://www.acns19.com

Location: Bogota, Colombia, 5 Jun 2019 – 7 Jun 2019.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 18th IEEE International Conference on Trust Security and Privacy in Computing and Communications (TrustCom 2019)

https://forumpoint2.eventsair.com/QuickEventWebsitePortal/trustcom19/tc19

Location: Rotorua, New Zealand, 5 Aug 2019 – 8 Aug 2019.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 18thWorkshop on Privacy in the Electronic Society (WPES 2019)

https://crises-deim.urv.cat/wpes2019/cfp.html

Location: London, United Kingdom, 11 Nov 2019.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 2019 IEEE 5G World Forum (WF-5G 2019)

https://ieee-wf-5g.org/

Location: Dresden, Germany, 10 Sep 2019 – 12 Sep 2019.

Participating Members:

- Cengis HASAN (Program Committee Member)

The 2019 IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC 2019)

https://pimrc2020.ieee-pimrc.org/

Location: Istanbul, Turkey, 31 Aug 2019 – 3 Sep 2019.

Participating Members:

- Cengis HASAN (Program Committee Member)

The 2019 IEEE Wireless Communications and Networking Conference (WCNC 2019)

https://wcnc2019.ieee-wcnc.org/

Location: Marrakech, Morocco, 15 Apr 2019 – 19 Apr 2019.

Participating Members:

- Cengis HASAN (Program Committee Member)

The 21st International Conference on Formal Engineering Methods (ICFEM 2019)

http://csse.szu.edu.cn/icfem2019/index.html

Location: Shenzhen, China, 5 Nov 2019 – 9 Nov 2019.

Participating Members:

- Jun PANG (Program Committee Member)

The 22nd International Conference on Fundamental Approaches to Software Engineering (FASE 2019)

https://www.etaps.org/2019/fase

Location: Prage, Czechia, 8 Apr 2019 – 11 Apr 2019.

Participating Members:

- Jun PANG (Program Committee Member)

The 24th ACM Symposium on Access Control Models and Technologies (SACMAT 2019)

http://www.sacmat.org/2019/index.php

Location: Toronto, Canada, 4 Jun 2019 – 6 Jun 2019.

Participating Members:

- Jun PANG (Program Committee Member)

The 24th European Symposium on Research in Computer Security (ESORICS 2019)

https://esorics2019.uni.lu

Location: Luxembourg, Luxembourg, 23 Sep 2019 – 27 Sep 2019.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 24th International Conference on Engineering of Complex Computer Systems (ICECCS 2019)

http://formal-analysis.com/iceccs/2019/

Location: Hongkong, China, 10 Nov 2019 – 13 Nov 2019.

Participating Members:

- Jun PANG (Program Committee Co-Chair)

The 2nd InternationalWorkshop on Advances in Mobile App Analysis (A-Mobile 2019)

https://a-mobile.github.io/

Location: San Diego, United States of America, 11 Nov 2019.

Participating Members:

- Olga GADYATSKAYA (Program Committee Member)

The 30th International Conference on Concurrency Theory (CONCUR 2019)

https://event.cwi.nl/concur2019/

Location: Amsterdam, Netherlands, 26 Aug 2019 – 31 Aug 2019.

Participating Members:

- Jun PANG (Program Committee Member)

The 33rd Annual IFIPWG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2019)

https://dbsec2019.cse.sc.edu

Location: Charleston, United States of America, 15 Jul 2019 – 17 Jul 2019.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 3rd IFIP TC 5 TC 12 WG 8.4 WG 8.9 WG 12.9 International Cross-Domain Conference (CD-MAKE 2019)

https://cd-make.net/

Location: Canterbury, United Kingdom, 26 Aug 2019 – 29 Aug 2019.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 4th National Conference on Formal Methods and Applications (FMAC 2019)

https://basics.sjtu.edu.cn/news/fmac2019/index.html

Location: Shanghai, China, 3 Nov 2019 – 4 Nov 2019.

Participating Members:

- Jun PANG (Program Committee Member)

The 5th Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems (CyberICPS 2019)

https://www.ds.unipi.gr/cybericps2019/

Location: Luxembourg, Luxembourg, 23 Sep 2019 – 27 Sep 2019.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 6th International Conference on Cryptography and Security Systems (C&SS 2019)

https://fedcsis.org/2019/ccss/

Location: Leipzig, Germany, 1 Sep 2019 – 4 Sep 2019.

Participating Members:

- Sjouke MAUW (Program Committee Member)

The 6th International Workshop on Graphical Models for Security (GraMSec 2019)

https://gramsec.uni.lu/

Location: Hoboken, NJ, United States of America, 25 Jun 2019 – 28 Jun 2019.

Participating Members:

- Olga GADYATSKAYA (Program Committee Member)
- Sjouke MAUW (Program Committee Member)
- Ross James HORNE (Program Committee Co-Chair)

The 8th International Conference on Complex Networks and their Applications (Complex Networks 2019)

https://www.complexnetworks.org/

Location: Lisbon, Portugal, 10 Dec 2019 – 12 Dec 2019.

Participating Members:

- Andrzej MIZERA (Program Committee Member)

The Eighth International Conference on Advances in Vehicular Systems Technologies and Applications (VEHICULAR)

https://www.iaria.org/conferences2019/VEHICULAR19.html

Location: Rome, Italy, 30 Jun 2019 – 4 Jul 2019.

Participating Members:

- Ion TURCANU (Technical Program Committee Member)

The European Symposium on Research in Computer Security (ESORICS 2019)

Location: Luxembourg, Luxembourg, 23 Sep 2019 – 27 Sep 2019.

Participating Members:

- Peter Y A RYAN (General Chair)
- Alfredo RIAL (Chair of Poster Session)
- Peter ROENNE (Organization Chair)

The Genetic and Evolutionary Computation Conference

https://gecco-2019.sigevo.org/index.html/HomePage

Location: Prague, Czechia, 13 Jul 2019 – 17 Jul 2019.

Participating Members:

- Boonyarit CHANGAIVAL (Paper presentation)

The Genetic and Evolutionary Computation Conference (GECCO 2019)

https://gecco-2019.sigevo.org/index.html/HomePage

Location: Prague, Czechia, 13 Jul 2019 – 17 Jul 2019.

Description: The Genetic and Evolutionary Computation Conference (GECCO) presents the latest high-quality results in genetic and evolutionary computation since 1999. Topics include: genetic algorithms, genetic programming, ant colony optimization and swarm intelligence, complex systems (artificial life/robotics/evolvable hardware/generative and developmental systems/artificial immune systems), digital entertainment technologies and arts, evolutionary combinatorial optimization and metaheuristics, evolutionary machine learning, evolutionary multiobjective optimization, evolutionary numerical optimization, real world applications, search-based software engineering, theory and more.

Participating Members:

- Grégoire DANOY (Program Committee Member)
- Daniel STOLFI ROSSO (Program Committee Member)

VLDB

Location: Rio de Janeiro, Brazil, 27 Aug 2018 – 31 Jan 2019.

Participating Members:

- Martin THEOBALD (Paper presentation)

W03: 5G-Trials - From 5G Experiments to Business Validation

https://icc2019.ieee-icc.org/workshop/w03-5g-trials-5g-experiments-business-validation

Location: Shanghai, China, 20 May 2019 – 24 May 2019.

Description: Following the 5G development roadmap, 5G has successfully completed the design and development phase and has now moved to the trial phase. In Europe, three large testbed projects under H2020 5G PPP programme have started on 1 July 2018. With more than 50 million Euro funding in total, these projects will build the 5G testbed facilities for coming 5G trials in Europe. In China, two large-scale 5G trial projects led by China Mobile and China Unicom will start after July 2018. Similar 5G trial activities are in Japan, South Korea, the Americans, and other regions. In addition to public funded 5G trial programmes, major telecom operators, vendors and main players from vertical sectors have planned, or even started, their own 5G trials. In the next two years, 5G trials will become the main driver for 5G research and development.

Participating Members:

- Ridha SOUA (Technical Program Committee Member)

XAI@IJCAI 2019

https://sites.google.com/view/xai2019/home

Location: Macau, China, 11 Aug 2019.

Description: As AI becomes more ubiquitous, complex and consequential, the need for people to understand how decisions are made and to judge their correctness becomes increasingly crucial due to concerns of ethics and trust. The field of Explainable AI (XAI), aims to address this problem by designing AI whose decisions can be understood by humans.

This workshop brings together researchers working in explainable AI to share and learning about recent research, with the hope of fostering meaningful connections between researchers from diverse backgrounds, including but not

limited to artificial intelligence, human-computer interaction, human factors, philosophy, cognitive & social psychology.

This meeting will provide attendees with an opportunity to learn about progress on XAI, to share their own perspectives, and to learn about potential approaches for solving key XAI research challenges. This should result in effective cross-fertilization among research on ML, AI more generally, intelligent user interaction (interfaces, dialogue), and cognitive modeling.

Participating Members:

- Amro NAJJAR (Program Committee Member)

C.2 Doctoral Thesis Defense Committee Memberships

Udovenko Aleksei, University of Luxembourg

Date: 9 Apr 2019
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Alexei BIRYUKOV (Supervisor)

Arash ATASHPENDAR, University of Luxembourg

Date: 23 Jan 2019
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Sjouke MAUW (Chairman)
- Peter ROENNE (Vice-chairman)
- Peter Y A RYAN (Supervisor)

PhD Defense Jury External Partners:

- Cas Cremers (Member)
- Jintai Ding (Member)

Voke Augoye, Royal Holloway

Date: 27 Jun 2019
Location: London, United Kingdom

PhD Defense Jury Members:

- Peter Y A RYAN (Member)

Nicolas Blanchard, Paris VII

Date: 21 Jun 2019
Location: Paris, France

PhD Defense Jury Members:

- Peter Y A RYAN (Member)

Chris Carr, Norwegian University of Science and Technology

Date: 30 Apr 2019
Location: Trondheim, Norway

PhD Defense Jury Members:

- Peter Y A RYAN (Member)

Boonyarit Changaival, University of Luxembourg

Date: 3 Dec 2019
Location: Belval, Luxembourg

PhD Defense Jury Members:

- Ulrich SORGER (Chairman)
- Pascal BOUVRY (Supervisor)
- Grégoire DANOY (Member)

PhD Defense Jury External Partners:

- Frédéric Guinand (Member)
- Dzmitry Kliazovich (Expert)
- Kittichai LAVAGNANANDA (Vice-chairman)

Siwen GUO, University of Luxembourg

Date: 29 Nov 2019
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Leon VAN DER TORRE (Chairman)
- Christoph SCHOMMER (Supervisor)

PhD Defense Jury External Partners:

- Tiansi Dong (Member)
- Kai Hui (Member)
- Pouyan Ziafati (Vice-chairman)

Khaled Karray, Telecom ParisTech

Date: 1 Apr 2019
Location: Paris, France

PhD Defense Jury Members:

- Sjouke MAUW (Member)

Max Kemman, University of Luxembourg

Date: 26 Apr 2019
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Christoph SCHOMMER (Expert)

Emmanuel Kieffer, University of Luxembourg

Date: 18 Jan 2019
Location: Belval, Luxembourg

PhD Defense Jury Members:

- Ulrich SORGER (Chairman)
- Pascal BOUVRY (Supervisor)
- Grégoire DANOY (Member)

PhD Defense Jury External Partners:

- Anass Nagih (Vice-chairman)
- Franciszek Seredynski (Member)

Daoyuan Li, University of Luxembourg

Date: 11 Jan 2019
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Jacques KLEIN (Chairman)
- Tegawendé François d Assise BISSYANDE (Vice-chairman)
- Yves LE TRAON (Supervisor)

PhD Defense Jury External Partners:

- Matthieu Geist (Examiner)
- Jessica Lin (Examiner)
- Anne-Marie Solvi (Expert)

José Miguel LOPEZ BECERRA, University of Luxembourg

Date: 14 May 2019
Location: Belval, Luxembourg

PhD Defense Jury Members:

- Jean-Sébastien CORON (Chairman)
- Dimiter OSTREV (Vice-chairman)
- Peter Y A RYAN (Supervisor)

PhD Defense Jury External Partners:

- Michel Abdalla (Member)
- Steve Kremer (Member)

Hugues Mandon, ENS Paris-Saclay

Date: 19 Nov 2019
Location: Paris, France

PhD Defense Jury Members:

- Jun PANG (Member)

Ludovic Mouline, University of Luxembourg

Date: 29 Nov 2019
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Nicolas NAVET (Chairman)

Johannes Mueller, University of Stuttgart

Date: 20 Sep 2019
Location: Stuttgart, Germany

PhD Defense Jury Members:

- Peter Y A RYAN (Member)

Steve Muller, University of Luxembourg

Date: 26 Jun 2019
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Jacques KLEIN (Chairman)

- Yves LE TRAON (Supervisor)

PhD Defense Jury External Partners:

- Jean-Marie Bonnin (Co-supervisor)
- Jean-Marie Flaus (Examiner)
- Romaric Ludinard (Vice-chairman)
- Valérie Viet Triem Tong (Examiner)

Gilles Neyens, University of Luxembourg

Date: 31 Oct 2019
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Leon VAN DER TORRE (Chairman)
- Nicolas NAVET (Vice-chairman)
- Denis ZAMPUNIERIS (Supervisor)

PhD Defense Jury External Partners:

- Anthony Cleve (Member)
- Jens H. Weber (Member)

Aurelian Palisse, Rennes 1

Date: 4 Mar 2019
Location: Rennes, France

PhD Defense Jury Members:

- Peter Y A RYAN (Member)

Balázs PEJÓ, University of Luxembourg

Date: 9 Sep 2019
Location: Belval, Luxembourg

PhD Defense Jury Members:

- Yves LE TRAON (Chairman)
- Peter Y A RYAN (Supervisor)

PhD Defense Jury External Partners:

- Claudia Diaz (Member)
- Melek Önen (Member)

Alejandro Sanchez Guinea, University of Luxembourg

Date: 27 Aug 2019
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Jacques KLEIN (Chairman)
- Yves LE TRAON (Supervisor)

PhD Defense Jury External Partners:

- Kary Främling (Examiner)
- Sylvain Kubler (Examiner)
- Gregory Nain (Vice-chairman)

Lucas Schabhuser, TU Darmstadt

Date: 24 Apr 2019
Location: Darmstadt, Germany

PhD Defense Jury Members:

- Peter Y A RYAN (Member)

Sakthivel Manikandan Sundharam, University of Luxembourg

Date: 19 Mar 2019
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Pierre KELSEN (Chairman)
- Yves LE TRAON (Vice-chairman)
- Nicolas NAVET (Supervisor)

PhD Defense Jury External Partners:

- Sebastian Altmeyer (Member)
- Grolleau Emmanuel (Member)

Jorge Luis Toro Pozo, University of Luxembourg

Date: 14 May 2019
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Yves LE TRAON (Chairman)
- Sjouke MAUW (Supervisor)

PhD Defense Jury External Partners:

- Ioana Boureanu (Member)
- Stéphanie Delaune (Member)

Wojtek Widel, INSA

Date: 3 Dec 2019
Location: Rennes, France

PhD Defense Jury Members:

- Sjouke MAUW (Member)

C.3 Awards

ACM International Symposium on Software Testing and Analysis (ISSTA'19). Paper title: "Search-based Test and Improvement of Machine-Learning-Based Anomaly Detection Systems", 19 Jul 2019
Recipients: Maxime CORDY, Yves LE TRAON, Mike PAPADAKIS

ACM International Symposium on Software Testing and Analysis (ISSTA'19). Paper title: "Semantic Fuzzing with Zest"., 18 Jul 2019
Recipients: Yves LE TRAON, Mike PAPADAKIS

AI newcomer, 5 Dec 2019
Recipient: Alexander STEEN
https://ki50.de/ki-newcomer-offline-umfragebeendet/newcomer-geistes-und-sozialwissenschaften/alexander-steen/

Application Impact award, IJCAI2019 demo track, Runner-up, 16 Aug 2019
Recipient: Shohreh HADDADAN
Runner-up of the Application Impact award in the demonstrations track at IJCAI 2019

Appointed adjunct lecturer at the University of Cape Town, 1 Oct 2019
Recipient: Giovanni CASINI

Appointed associate researcher at ISTI-CNR, Pisa, Italy, 1 Oct 2019
Recipient: Giovanni CASINI

Best paper award at CMSB 2019, 18 Sep 2019

Recipients: Jun PANG, Soumya PAUL, Cui SU
The paper "Sequential reprogramming of Boolean networks made practical" received the Best Paper Award at the 17th International Conference on Computational Methods in Systems Biology (CMSB'19).

Best Paper Award at ICAI 2019, 9 Nov 2019

Recipients: Aryobarzan ATASHPENDAR, Christian GREVISSE, Steffen ROTHKUGEL

Best presentation award at the PhD Colloquium, 1 Oct 2019

Recipient: Marie-Laure ZOLLINGER

CASC-27 (LTB Division) 1st place, 29 Aug 2019

Recipient: Alexander STEEN
1st place at the CASC-27 competition, LTB division

CASC-27 (THF division), runner-up, 29 Aug 2019

Recipient: Alexander STEEN
Runner-up at the CASC-27 competition, THF division

Distinguished Paper Award ESEC/FSE 2019 for "The importance of accounting for real-world labelling when predicting software vulnerabilities", 29 Aug 2019

Recipients: Yves LE TRAON, Mike PAPADAKIS

Distinguished Reviewer Award for ICST 2019, 26 Apr 2019

Recipient: Mike PAPADAKIS

Security Project of the Year Award, 1 May 2019

Recipients: Pascal BOUVRY, Matthias R. BRUST
Pascal Bouvry and Matthias Brust received the Security Project of the Year Award during the Security Made in Luxembourg's Information Security Day 2019 for the project, Technical Standardisation for Trusted Use in the Field of Smart ICT, in collaboration with the Luxembourg Institute of Standardisation, Accreditation, Safety and Quality of Products and Services (ILNAS). The project tackles the challenge of standardisation and regulation in the rapidly developing worlds of big data and artificial intelligence, Internet of Things, and cloud computing.

Teaching Award, 2 Oct 2019
Recipient: Jean BOTEV

C.4 Media Appearances

Luxembourg Bitcoin (Postcast episode 56) (Basic Block Radio (Russian Podcast))

http://www.spreaker.com/user/immigrantcast/icast-ep-056-sergey-tikhomirov-luxemburg

Interview (Internet), 15 Dec 2019
Members: Sergei TIKHOMIROV
Basic Block Radio (http://www.basicblockradio.com) is a Russian-language pdcast on blockchain technology (the related Youtube channel at http://www.youtube.com/channel/UC95bSmaFa7R33GOyi6VfyGQ/ has some English-language content).

KI in der Medizin (Luxemburger Wort)

https://www.wort.lu/de/politik/kuenstliche-intelligenz-fuer-die-medizin-5dad9f32da2cc1784e34e1e3

Article (Newspaper), 19 Oct 2019 , issue 171, p. 16-17 (2 pages)
Members: Christoph SCHOMMER
Innovative developments in Artificial Intelligence (AI), Data Science and Computer Engineering have led to far-reaching consequences for many areas of economic and social life, including medicine and healthcare. This article presents some scientific innovations, but at the same time pleads for the inclusion of important factors such as explainability, ethics, comprehensibility and others.

Des enseignants de l'Uni élus par leurs étudiants (L'Essentiel)

Article (Newspaper), 3 Oct 2019 , p. 4
Members: Jean BOTEV

Sicherheitslucke im biometrischen Pass (Luxemburger Wort)

https://www.wort.lu/de/lokales/sicherheitsluecke-im-biometrischen-pass-5d8b823ada2cc1784e34c335

Article (Newspaper), 27 Sep 2019
Members: Ross James HORNE, Sjouke MAUW, Zachary Daniel SMITH
The vulnerability a ects all biometric passports worldwide

Panorama (100komma7)

https://www.100komma7.lu/program/episode/26867920190926120020190926121 0

News (Radio), 26 Sep 2019
Members: Ross James HORNE, Sjouke MAUW, Zachary Daniel SMITH
UNI.lu provides details on security de ciencies in E-Passports

Luxembourg researchers reveal privacy aw in e-passports (Luxembourg Times)

https://luxtimes.lu/luxembourg/38572-luxembourg-researchers-reveal-privacy-flaw-in-e-

Article (Newspaper), 26 Sep 2019
Members: Ross James HORNE, Sjouke MAUW, Zachary Daniel SMITH
The vulnerability affects all biometric passports worldwide

UNI RESEARCHERS DISCOVER E-PASSPORT FLAW (Delano)

https://delano.lu/d/detail/news/lux-maintain-epassports-after-data-flaw-discovery/208182

Article (Newspaper), 26 Sep 2019
Members: Ross James HORNE, Sjouke MAUW, Zachary Daniel SMITH
The vulnerability affects all biometric passports worldwide

Une faille qui devrait alerter les autorites (Paperjam)

https://paperjam.lu/article/faille-qui-devrait-alerter-aut

Article (Newspaper), 26 Sep 2019
Members: Ross James HORNE, Sjouke MAUW, Zachary Daniel SMITH
A team of researchers from the University of Luxembourg has identified a data breach that threatens privacy. How to understand this study? What are the consequences? And why should the authorities press a little harder where it hurts?

Mangel bei elektronesche Pass (RTL)

https://www.rtl.lu/tele/de-journal-vun-der-tele/v/3178397.html

News (TV), 26 Sep 2019
Members: Ross James HORNE, Sjouke MAUW, Zachary Daniel SMITH
Researchers at the University of Luxembourg found privacy deficiencies in the electronic passports.

Une faille dans les passeports electroniques (Paperjam)

https://paperjam.lu/article/faille-dans-passeports-electro

Article (Newspaper), 25 Sep 2019
Members: Ross James HORNE, Sjouke MAUW, Zachary Daniel SMITH
A team of researchers from the University of Luxembourg announced in a press release that they had discovered a security hole in electronic passports.

ICAO denies alleged privacy aw in biometric passports (BiometricUpdate.com)

https://www.biometricupdate.com/201909/icao-denies-alleged-privacy-flaw-in-biometric-passports

Article (Internet), 25 Sep 2019
Members: Ross James HORNE, Sjouke MAUW, Zachary Daniel SMITH
A group of researchers from the University of Luxemburg may have detected a critical security flaw in the International Civil Aviation Organization (ICAO) 9303 security standard that identifies travelers by scanning the chip implemented in biometric passports, the team announced at the European Symposium on Research in Computer Security (ESORICS) in Vienna, Austria this week. The ICAO, however, denies the vulnerability is present in the specification's current version.

Leo-III ist Weltmeister (Luxemburger Wort)

http://page.mi.fu-berlin.de/cbenzmueller/papers/2019-Leo-III-ist-Weltmeister.pdf

Article (Newspaper), 31 Aug 2019 , p. 15
Members: Alexander STEEN
Erfolg für Forscher der FU Berlin und der Uni Luxemburg im Automatischen Theorembeweiser

Le superordinateur luxembourgeois "Meluxina" fera partie du réseau européen EuroHPC (Governement.lu)

https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2019/06-juin/14-schneider-meluxina.html

Article (Internet), 23 Jun 2019
Members: Pascal BOUVRY, Valentin PLUGARU, Sébastien VARRETTE

Luxembourg Supercomputer 'Meluxina' Will be Part of the EuroHPC Network (HPCWire)

https://www.hpcwire.com/off-the-wire/luxembourg-supercomputer-meluxina-will-be-part-of-the-eurohpc-network/

Article (Internet), 15 Jun 2019
Members: Pascal BOUVRY, Valentin PLUGARU, Sébastien VARRETTE

Die Pragmatikerin (REVUE)

https://chatbots.uni.lu/home/in-press/

Article (Newspaper), 1 Jun 2019 , issue 24-5
Members: Sviatlana HOEHN

Léiermaterial meets Hashtags - Evaluatioun vun der ALMA-Approche (eduSphere Newsletter)

http://links.comgouv.lu/nl2/q5u9/mtxtg.html?m=AMUAAEBZW4MAAcgXzkwAAJknrgQAAV3KDCkAHrxEAAoPEwBdA5jF2SgzrKScSVSp0LS4BBfKbAAGzXk&b=5146c08f&e=57c708e9&x=38mTVLpJwRl67fs5lef-Og7NLNxAN4glX4r07QAxH00

News (Internet), 1 Jun 2019
Members: Christian GREVISSE
Relevant Léiermaterial zu engem spezifesche Problem ze fannen ass net einfach an Zäiten, an deenen engem den Internet eng scho bal ze grouss Unzuel un deels gudden, deels manner gudde Ressourcen zur Verfügung stellt. Am Kader vun enger Dokteraarbecht wollte Fuerscher vun der Uni Lëtzebuerg kucken, wéi gutt Schüler an engem Gebitt kënnen eens ginn, an deem se bis elo nach kee Virwëssen hunn. Mat der Hëllef vum SCRIPT gouf en Experiment mat 36 Schüler aus dem Lycée Hubert Clément an dem Lycée Bel-Val duerchgefouert, an deem se Aufgaben zur Computerprogrammatioun léise sollten. Als Spill ronderëm dat eigentlecht Experiment sollten d'Schüler dem Homer Simpson hëllefen, e simuléierte WhatsApp-Chat z'entschlësselen. Wat hir Léisungen zu den Aufgabe méi richteg goufen, wat d'Kommunikatioun nees méi däitlech gouf.

Luxembourg ganz digital: Schnessen und Strips. So funktioniert moderne Sprachforschung an der Universität Luxembourg (Luxemburger Wort)

https://www.wort.lu/de/panorama/luxemburgisch-ganz-digital-5cc15d73da2cc1784e342c75

Article (Newspaper), 24 Apr 2019
Members: Christoph SCHOMMER
The "Strips" research project is the subject of an article in the Luxemburger Wort.

EU and ASEAN discuss high performing computing in support to research (Singapore, 14-15 March 2019) (European Commission Website)

https://eeas.europa.eu/headquarters/headquarters-homepage/60085/eu-and-asean-discuss-high-performing-computing-support-research-singapore-14-15-march-2019_es

Article (Internet), 15 Mar 2019
Members: Pascal BOUVRY, Sébastien VARRETTE

Luxembourg to be the first European country to create an artificial intelligence (AI) partnership with NVIDIA (Luxembourg Government)

https://gouvernement.lu/en/actualites/toutes_actualites/communiques/2019/01-janvier/30-bettel-partenariat-nvidia.html

Article (Internet), 30 Jan 2019
Members: Pascal BOUVRY, Sébastien VARRETTE

Ein europäisches CERN für die Künstliche Intelligenz (Luxemburger Wort)

https://wort.lu/de/politik/ein-europaeisches-cern-fuer-die-kuenstliche-intelligenz-5c2de14f182b657ad3b9d152

Article (Newspaper), 3 Jan 2019 , p. 4
Members: Christoph SCHOMMER

C.5 Guest Researchers

The following guest researchers were invited to the CSC:

Matteo Acclavio (Roma Tre University)
Period: 19 Nov 2019 – 22 Nov 2019
Hosted by: Ross James HORNE
Reason: Research collaboration

Prof. Dr. Florian Adamsky (Hof University)

Period: 21 Nov 2019 – 22 Nov 2019
Hosted by: Thomas ENGEL
Reason: Scientific Workshop

Roberto Araujo

Period: 12 Feb 2019 – 13 Feb 2019
Hosted by: Peter Y A RYAN

Hamed Arshad (University of Oslo)

Period: 1 Oct 2019 – 31 Dec 2019
Hosted by: Ross James HORNE
Reason: Research representation

Gergei Bana (Missouri University)

Period: 2 Dec 2019 – 4 Dec 2019
Hosted by: Wojciech JAMROGA

Prof Dr Christoph Benzmüller (Freie University Berlin)

Period: 1 Jan 2019 – 30 Jun 2020
Hosted by: Leon VAN DER TORRE

Prof. Dr. Roland Bouffanais (Singapore University of Technology and Design (SUTD))

Period: 16 Sep 2019 – 26 Sep 2019
Hosted by: Pascal BOUVRY, Matthias R. BRUST
Reason:

- Research collaboration
- Prof. Bouffanais provided a course on “Network Science” at the doctoral school (Course offer in DP-CSCE : Using Network Science to Design and Control Networked Systems).

Ioanna Boureanu (University of Surrey)

Period: 14 May 2019
Hosted by: Sjouke MAUW, Yunior RAMIREZ CRUZ, Jorge Luis TORO POZO
Reason: PhD defense and research presentation

Assoc.-Prof. Dr. Armelle Brun (Université de Lorraine)

Period: 25 Nov 2019
Hosted by: Thomas ENGEL
Reason: Research Visit, Cooperation discussion

Dr. German Castignani (Motion-S)
Period: 19 Dec 2019
Hosted by: Thomas ENGEL
Reason: Research visit

Dr. German Castignani (Motion-S)
Period: 19 Jun 2019
Hosted by: Thomas ENGEL
Reason: Appointment Committee

Dr. German Castignani (Motion-S)
Period: 21 Jun 2019
Hosted by: Thomas ENGEL
Reason: Appointment Committee

Dr. German Castignani (Motion-S)
Period: 14 May 2019
Hosted by: Thomas ENGEL
Reason: Research visit

Dr. German Castignani (Motion-S)
Period: 5 Sep 2019
Hosted by: Thomas ENGEL
Reason: Appointment Committee

Dr. German Castignani (Motion-S)
Period: 28 Jan 2019
Hosted by: Thomas ENGEL
Reason: Research visit

Dr. German Castignani (Motion-S)
Period: 21 Nov 2019 – 22 Nov 2019
Hosted by: Thomas ENGEL
Reason: Scientific Workshop

Dr. German Castignani (Motion-S)
Period: 12 Jun 2019
Hosted by: Thomas ENGEL
Reason: Research visit

Richard Clayton
Period: 26 Apr 2019 – 27 Apr 2019
Hosted by: Peter Y A RYAN

Stephanie Delaune (IRISA Rennes)
Period: 14 May 2019
Hosted by: Sjouke MAUW, Yunior RAMIREZ CRUZ, Jorge Luis TORO POZO
Reason: PhD defense and research representation

Huseyin Demirci
Period: 30 Oct 2019 – 31 Oct 2019
Hosted by: Peter Y A RYAN

Damien Desfontaines
Period: 4 Feb 2019 – 8 Feb 2019
Hosted by: Balazs PEJO

Jintai Ding
Period: 22 Jan 2019 – 23 Jan 2019
Hosted by: Peter Y A RYAN

Jintai Ding
Period: 8 Jul 2019 – 9 Jul 2019
Hosted by: Peter Y A RYAN

Dr Huimin Dong (Zhejiang University)
Period: 4 Nov 2019 – 20 Dec 2019
Hosted by: Leon VAN DER TORRE

Tiansi Dong (Bonn University)
Period: 11 Apr 2019
Hosted by: Jun PANG
Reason: Research presentation

Prof. Dr. Gabi Dreo Rodosek (Code Institute, Universität der Bundeswehr, München)
Period: 2 May 2019 – 3 May 2019
Hosted by: Thomas ENGEL
Reason: Appointment Committee, Research Visit

Ehsan Ebrahimi
Period: 28 Mar 2019 – 29 Mar 2019
Hosted by: Peter Y A RYAN

Anton Feenstra (Vrije Universiteit Amsterdam)
Period: 21 Feb 2019 – 23 Feb 2019
Hosted by: Jun PANG, Soumya PAUL
Reason: Research collaboration

Dr. Volker Fusenig (Siemens München)
Period: 21 Nov 2019 – 22 Nov 2019
Hosted by: Thomas ENGEL
Reason: Scientific Workshop

Gavin Goerke (American University of Paris)
Period: 1 Jul 2019 – 31 Aug 2019
Hosted by: Alexander STEEN
Reason: Student internship

Prof. Frederic Guinand (Le Havre University, France)
Period: 2 Dec 2019 – 4 Dec 2019
Hosted by: Pascal BOUVRY

Wei Guo (Nanjing University)
Period: 6 May 2019 – 7 May 2019
Hosted by: Jun PANG, Zhiqiang ZHONG
Reason: Research collaboration

Dennis Jackson
Period: 22 Jan 2019 – 23 Jan 2019
Hosted by: Peter Y A RYAN

Christian Johansen (University of Oslo)
Period: 11 Dec 2019 – 13 Dec 2019
Hosted by: Sergiu BURSUC, Ross James HORNE
Reason: Research presentation

Niklas Kalckreuth
Period: 18 Nov 2019 – 29 Nov 2019
Hosted by: Arianna ROSSI

Timotheus Kampik (Umea University, Sweden)
Period: 20 Oct 2019 – 2 Nov 2019
Hosted by: Amro NAJJAR, Leon VAN DER TORRE

Filip Kucerak
Period: 18 Jun 2019 – 23 Jun 2019
Hosted by: Pascal BOUVRY, Sébastien VARRETTE
Reason: Winner of the EU Contest for Young Scientists

Prof. Kittichai Lavangnananda (KMUTT, Bangkok, Thailand)
Period: 28 Nov 2019 – 9 Dec 2019
Hosted by: Pascal BOUVRY

Hyunwoo Lee (Seoul National University)
Period: 11 Mar 2019 – 16 Mar 2019
Hosted by: Zachary Daniel SMITH
Reason: Research collaboration

Cheng-Te Li (National Cheng Kung University)
Period: 29 Aug 2019 – 30 Aug 2019
Hosted by: Jun PANG
Reason: Research collaboration

Chonghui Li (Zhejiang University)
Period: 11 Nov 2019 – 20 Jan 2020
Hosted by: Leon VAN DER TORRE

HPC Prace Summer School student Sean Mahon
Period: 1 Jul 2019 – 31 Aug 2019
Hosted by: Pascal BOUVRY, Sébastien VARRETTE

Christian Majenz
Period: 9 Dec 2019 – 10 Dec 2019
Hosted by: Peter Y A RYAN

Karola Marky
Period: 5 Apr 2019 – 8 Apr 2019
Hosted by: Peter Y A RYAN

Maxime Martinasso (Swiss National Supercomputing Centre (CSCS), Switzerland)
Period: 23 Sep 2019 – 24 Sep 2019
Hosted by: Pascal BOUVRY, Sébastien VARRETTE

Chloe Martindale
Period: 7 May 2019 – 8 May 2019
Hosted by: Peter Y A RYAN

Prof. Dr. Christoph Meinel (Hasso Plattner Institut / University of Potsdam)
Period: 2 May 2019 – 3 May 2019
Hosted by: Thomas ENGEL
Reason: Appointment Committee, Research Visit

Prof. Thomas Meyer (University of Cape Town)
Period: 4 Jun 2019 – 5 Jul 2019
Hosted by: Giovanni CASINI, Leon VAN DER TORRE
Reason: Visit for the MIREL project

Dr. Jedrzej Musial (Poznan University of Technology (PUT), Poland)
Period: 1 Jul 2019 – 31 Aug 2019
Hosted by: Pascal BOUVRY, Grégoire DANOY

Dr. Jedrzej Musial (Poznan University of Technology (PUT), Poland)
Period: 7 Dec 2019 – 14 Dec 2019
Hosted by: Pascal BOUVRY, Grégoire DANOY

David Naccache
Period: 11 Jan 2019 – 12 Jan 2019
Hosted by: Peter Y A RYAN

Dr. Amro Najjar (Umea University, Sweden)
Period: 2 Apr 2019 – 6 Apr 2019
Hosted by: Leon VAN DER TORRE

Vivek Nigam (Fortiss Gmbh)
Period: 12 Mar 2019 – 14 Mar 2019
Hosted by: Ross James HORNE
Reason: Research collaboration

Olayinka Olaoluwa
Period: 8 Apr 2019 – 5 Jun 2019
Hosted by: Peter Y A RYAN

Prof. Dr.-Ing. Andriy Panchenko (Brandenburg University of Technology)
Period: 11 Dec 2019
Hosted by: Thomas ENGEL
Reason: Appointment Committee, Research Visit

Prof. Dr.-Ing. Andriy Panchenko (Brandenburg University of Technology)
Period: 26 Sep 2019
Hosted by: Thomas ENGEL
Reason: Supervision of a doctoral candidate

Prof. Dr.-Ing. Andriy Panchenko (Brandenburg University of Technology)
Period: 2 May 2019 – 3 May 2019
Hosted by: Thomas ENGEL
Reason: Research Visit

Prof. Dr.-Ing. Andriy Panchenko (Brandenburg University of Technology)
Period: 4 Feb 2019 – 5 Feb 2019
Hosted by: Thomas ENGEL
Reason: Research visit

Lisha Qiao (Zhejiang University)
Period: 21 Mar 2019 – 27 Mar 2019
Hosted by: Leon VAN DER TORRE

Prof. Franciszek Seredynski (Cardinal Stefan Wyszyński University, Warsaw, Poland)
Period: 8 Dec 2019 – 13 Dec 2019
Hosted by: Pascal BOUVRY

Isa Sertkaya
Period: 1 Apr 2019 – 2 Apr 2019
Hosted by: Peter Y A RYAN

Prof. Guillermo Simari (Universidad Nacional del Sur)
Period: 3 Feb 2019 – 5 Mar 2019
Hosted by: Leon VAN DER TORRE
Reason: Worked on developing computational solutions in the context of normative reasoning for decision-making in the context of the MIREL project.

Lutz Strassburger (LiX, Ecole Polytechnique)
Period: 20 Nov 2019 – 22 Nov 2019
Hosted by: Ross James HORNE
Reason: Research collaboration

HPC Prace Summer School student Matteo Stringher
Period: 1 Jul 2019 – 31 Aug 2019
Hosted by: Pascal BOUVRY, Sébastien VARRETTE

Dr Juliana STROPP (University Madrid)
Period: 1 Dec 2019 – 30 Jun 2020
Hosted by: Christoph SCHOMMER
Reason: Marie Curie

Dr. Alexandru Tantar (Luxembourg Institute of Technology (LIST))
Period: 21 Nov 2019 – 22 Nov 2019
Hosted by: Thomas ENGEL
Reason: Scientific Workshop

Rolando Trujillo-Rasua (Deakin University)
Period: 13 May 2019 – 17 May 2019
Hosted by: Sjouke MAUW, Yunior RAMIREZ CRUZ, Jorge Luis TORO POZO
Reason: PhD Defense, research collaboration and research presentation

Leone Valentina
Period: 15 Jan 2019 – 14 Oct 2019
Hosted by: Martin THEOBALD

Dr. Gerard Wagener (CIRCL Luxembourg)
Period: 21 Nov 2019 – 22 Nov 2019
Hosted by: Thomas ENGEL
Reason: Scientific Workshop

Caesar Wu (University of Melbourne, Australia)
Period: 4 Dec 2019 – 18 Dec 2019
Hosted by: Pascal BOUVRY

William Zhang (Zhejiang University)
Period: 21 Mar 2019 – 27 Mar 2019
Hosted by: Leon VAN DER TORRE

Yang Zhang (CISPA)
Period: 8 Aug 2019 – 9 Aug 2019
Hosted by: Jun PANG
Reason: Research collaboration

Yang Zhang (CISPA)
Period: 19 Dec 2019
Hosted by: Jun PANG
Reason: Research collaboration

Yury Zhauniarovich (Perfect Equanimity)
Period: 24 Jun 2019 – 26 Jun 2019
Hosted by: Olga GADYATSKAYA
Reason: Research collaboration

C.6 Visits

The following visits by CSC members to external organisations took place:

Alfredo CAPOZUCCA

Institution: Innopolis University, Tatarstan, Russia
Location: Kazan, Russia
Period: 5 Sep 2019 – 8 Sep 2019.
Reason: Invited Professor - DevOps course responsible at Bachelor and Master levels

Alfredo CAPOZUCCA

Institution: Innopolis University
Location: Kazan, Russia
Period: 2 Oct 2019 – 6 Oct 2019.
Reason: Invited Professor - DevOps course responsible at Bachelor and Master levels

Alfredo CAPOZUCCA

Institution: Innopolis University
Location: Kazan, Russia
Period: 30 Oct 2019 – 3 Nov 2019.
Reason: Invited Professor - DevOps course responsible at Bachelor and Master levels

Giovanni CASINI

Institution: University of Cape Town
Location: Cape Town, South Africa
Period: 18 Feb 2019 – 19 Apr 2019.
Reason: Visiting Prof. Thomas Meyer at the Dep. of Computer Science for the MIREL project

Giovanni CASINI

Institution: Stanford University
Location: Stanford, United States of America
Period: 22 May 2019 – 21 Jun 2019.
Reason: Visiting the Center for the Study of Language and Information for the MIREL project

Stanislav DASHEVSKYI

Institution: University of Padua
Location: Padua, Italy
Period: 19 Feb 2019 – 20 Feb 2019.
Reason: Research collaboration

Jérémie DAUPHIN

Institution: National Institute of Informatics
Location: Tokyo, Japan
Period: 18 Feb 2019 – 1 Apr 2019.
Reason: Visiting Prof. Ken Satoh for the MIREL project

Jérémie DAUPHIN
Institution: National Institute of Informatics
Location: Tokyo, Japan
Period: 12 Apr 2019 – 26 Jul 2019.
Reason: Visiting Prof. Ken Satoh for the MIREL project

Ali FARJAMI
Institution: University of Tehran
Location: Tehran, Iran
Period: 24 Jun 2019 – 4 Aug 2019.
Reason: Ali Farjami contributed to the project "I/O mechanism over an algebra".

Olga GADYATSKAYA
Institution: University of Padua
Location: Padua, Italy
Period: 19 Feb 2019 – 20 Feb 2019.
Reason: Research collaboration

Olga GADYATSKAYA
Institution: Leiden University
Location: Leiden, Netherlands
Period: 21 May 2019.
Reason: Research presentation

Olga GADYATSKAYA
Institution: CNR
Location: Pisa, Italy
Period: 10 Jun 2019.
Reason: Research collaboration

Shohreh HADDADAN
Institution: National Institute of Informatics
Location: Tokyo, Japan
Period: 15 Mar 2019 – 24 Apr 2019.
Reason: Visit for the MIREL project

Shohreh HADDADAN
Institution: NOMOTIKA, University of Turin
Location: Turin, Italy
Period: 14 Oct 2019 – 20 Dec 2019.
Reason: Visit for the MIREL project

Sviatlana HOEHN
Institution: Vitebsk State University
Location: Vitebsk, Belarus
Period: 21 Apr 2019 – 1 May 2019.

Ross James HORNE
Institution: IRISA Rennes
Location: Rennes, France
Period: 4 Feb 2019 – 8 Feb 2019.
Reason: Research collaboration

Ross James HORNE
Institution: INRIA Nancy
Location: Nancy, France
Period: 29 May 2019.
Reason: Research collaboration

Ross James HORNE
Institution: Uppsala University
Location: Uppsala, Sweden
Period: 19 Aug 2019 – 23 Aug 2019.
Reason: Research collaboration

Wojciech JAMROGA
Institution: University of Naples
Location: Naples, Italy
Period: 28 Oct 2019 – 1 Nov 2019.

Réka MARKOVICH
Institution: CSIRO, Data 61
Location: Brisbane, Australia
Period: 26 Apr 2019 – 14 Jun 2019.
Reason: Visit in the context of the MIREL project

Réka MARKOVICH
Institution: Stanford University
Location: Stanford, United States of America
Period: 1 Jul 2019 – 31 Aug 2019.
Reason: Visit for the MIREL project

Réka MARKOVICH
Institution: Zhejiang University
Location: Hangzhou, China
Period: 1 Sep 2019 – 9 Sep 2019.

Sjouke MAUW
Institution: Leiden University
Location: Leiden, Netherlands
Period: 25 Mar 2019 – 26 Mar 2019.
Reason: Evaluation

Sjouke MAUW
Institution: Telecom ParisTech
Location: Paris, France
Period: 31 Mar 2019 – 2 Apr 2019.
Reason: PhD Defense

Sjouke MAUW
Institution: Leiden University
Location: Leiden, Netherlands
Period: 11 Jun 2019 – 13 Jun 2019.
Reason: Evaluation

Sjouke MAUW
Institution: Delft University
Location: Delft, Netherlands
Period: 26 Jun 2019 – 27 Jun 2019.
Reason: Evaluation

Sjouke MAUW
Institution: NTNU
Location: Trondheim, Norway
Period: 12 Sep 2019 – 13 Sep 2019.
Reason: Research collaboration

Sjouke MAUW
Institution: Utrecht University
Location: Utrecht, Netherlands
Period: 12 Sep 2019 – 13 Sep 2019.
Reason: Evaluation

Sjouke MAUW
Institution: Eindhoven University
Location: Eindhoven, Netherlands
Period: 1 Oct 2019 – 2 Oct 2019.
Reason: Evaluation

Sjouke MAUW
Institution: UvA
Location: Amsterdam, Netherlands
Period: 4 Nov 2019 – 5 Nov 2019.
Reason: Evaluation

Sjouke MAUW
Institution: VU
Location: Amsterdam, Netherlands
Period: 6 Nov 2019 – 7 Nov 2019.
Reason: Evaluation

Sjouke MAUW
Institution: Radboud University
Location: Nijmegen, Netherlands
Period: 18 Nov 2019 – 19 Nov 2019.
Reason: Evaluation

Sjouke MAUW
Institution: Groningen University
Location: Groningen, Netherlands
Period: 27 Nov 2019 – 29 Nov 2019.
Reason: Evaluation

Sjouke MAUW
Institution: IRISA
Location: Rennes, France
Period: 3 Dec 2019 – 4 Dec 2019.
Reason: PhD defense

Sjouke MAUW
Institution: Twente University
Location: Enschede, Netherlands
Period: 8 Dec 2019 – 10 Dec 2019.
Reason: Evaluation

Asya MITSEVA
Institution: Brandenburg University of Technology
Location: Cottbus, Germany
Period: 6 Jan 2019 – 17 Jan 2019.
Reason: Erasmus+ teaching staff mobility.

Asya MITSEVA
Institution: Brandenburg University of Technology
Location: Cottbus, Germany
Period: 27 Jun 2019 – 5 Jul 2019.
Reason: Research collaboration.

Amro NAJJAR
Institution: University of Leon
Location: Leon, Spain
Period: 17 May 2019 – 25 May 2019.

Amro NAJJAR
Institution: Stanford University
Location: Stanford, United States of America
Period: 16 Nov 2019 – 18 Dec 2019.
Reason: Research visit for the MIREL project

Nicolas NAVET

Institution: Inria Grenoble – Rhône-Alpes
Location: Grenoble, France
Period: 15 Nov 2019.
Reason: Talk entitled "Generative design for E/E architectures in 2020 and beyond: the start of the Centaur Era?" given in the SPADES Inria team.

Aleksandr PILGUN

Institution: University of Padua
Location: Padua, Italy
Period: 19 Feb 2019 – 20 Feb 2019.
Reason: Research collaboration

Valentin PLUGARU

Institution: Jülich Supercomputing Centre (JSC) - Forschungszentrum Jülich
Location: Jülich, Germany
Period: 7 Mar 2019.
Reason: The European High Performance Computing Joint Undertaking (EuroHPC-JU), launched on 15 February 2019 the call for expression of interest for the selection of the Hosting Entities for Petascale Supercomputers.

During the Q1-Q2 2019 preparatory phase for Luxembourg's application to the call, workshops were held in Luxembourg and Jülich for an exchange on knowledge and experience in the management of a supercomputing site.

In the workshop on 7 March 2019 I participated as HPC expert part of the Luxembourg delegation which included representatives from the Luxembourg Ministry of the Economy, LuxConnect S.A., University of Luxembourg and the Luxembourg Institute of Science and Technology.

Luxembourg's application to the EuroHPC call has been successful, with the official announcement presented on 14 June 2019: https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2019/06-juin/14-schneider-meluxina.html

Valentin PLUGARU

Institution: National Electronics and Computer Technology Center (NECTEC)
Location: Bangkok, Thailand
Period: 30 Jul 2019 – 2 Aug 2019.
Reason: "A Week with HPC Experts: Knowledge and Best Practice Sharing", between NECTEC and University of Luxembourg.

Early in 2019, the National Science and Technology Development Agency (NSTDA) Supercomputer Center (ThaiSC) was newly founded and operates under NECTEC. Its core mission is to provide high performance computing (HPC) service for Thai R&D community at the national scale. Its vision is to be a leading HPC facility and computational science R&D center in ASEAN.

ThaiSC organized a four-days program on "Knowledge and Best Practice Sharing Workshop" from 30 July - 2 August 2019 in Thailand Science Park, Pathum Thani. The purpose of the program was to learn and improve the services of ThaiSC through experience sharing.

Given my expertise and the continuing collaboration between NECTEC and UL since 2011, I participated in this program as an expert in the field of HPC management, providing inputs on the management of an HPC service including policies, KPIs, procurements, services for industrial partners, and also HPC architecture, technologies and service stacks.

Livio ROBALDO

Institution: Nomotika SRL
Location: Turin, Italy
Period: 2 Jan 2019.

Peter ROENNE

Institution: University of Surrey
Location: Guildford, United Kingdom
Period: 15 May 2019 – 16 May 2019.

Peter ROENNE

Institution: Oxford Blockchain Institute
Location: Oxford, United Kingdom
Period: 3 Aug 2019 – 5 Aug 2019.

Peter ROENNE

Institution: Norwegian University of Science and Technology
Location: Trondheim, Norway
Period: 1 Sep 2019 – 3 Sep 2019.

Arianna ROSSI

Institution: Weizenbaum Institute for the Networked Society
Location: Berlin, Germany
Period: 27 Feb 2019 – 28 Feb 2019.

Arianna ROSSI

Institution: Faculté de Droit et Criminologie, UCLouvain
Location: Louvain-la-Neuve, Belgium
Period: 24 Apr 2019 – 25 Apr 2019.

Christoph SCHOMMER

Institution: Freie Universität Berlin
Location: Berlin, Germany
Period: 19 Nov 2018 – 29 Nov 2019.
Reason: Seminar ”inforrmation retrieval” (20h)

Christoph SCHOMMER
Institution: Singapore University SUTD
Location: Singapore, Singapore
Period: 1 Jun 2019 – 8 Jun 2019.
Reason: Research and Teaching stay

Christoph SCHOMMER
Institution: Freie Universität Berlin
Location: Berlin, Germany
Period: 15 Jul 2019 – 19 Jul 2019.
Reason: Course (20h) Artifiical Intelligence

Christoph SCHOMMER
Institution: Freie Universität Berlin
Location: Berlin, Germany
Period: 9 Sep 2019 – 19 Sep 2019.
Reason: Course Artificial Intelligence (Block course)

Zachary Daniel SMITH
Institution: Seoul National University
Location: Seoul, South Korea
Period: 2 Jun 2019 – 6 Jun 2019.
Reason: Research collaboration and presentation

Zachary Daniel SMITH
Institution: Surrey University
Location: Surrey, United Kingdom
Period: 18 Nov 2019 – 19 Nov 2019.
Reason: Research collaboration

Alexander STEEN
Institution: Universität des Saarlands
Location: Saarbrücken, Germany
Period: 2 Jan 2019 – 3 Jan 2019.
Reason: Visiting Jörg Siekmann

Alexander STEEN
Institution: Stanford University
Location: Stanford, United States of America
Period: 10 Apr 2019 – 16 Jun 2019.
Reason: Visit for the MIREL project

Alexander STEEN
Institution: SRI International
Location: Menlo Park, United States of America
Period: 26 Apr 2019.
Reason: Gave an invited talk at the AI lab, hosted by Richard Waldinger

Alexander STEEN
Institution: Free University of Amsterdam
Location: Amsterdam, Netherlands
Period: 23 Jul 2019 – 27 Jul 2019.
Reason: Visiting Jasmin Blanchette

Alexander STEEN
Institution: Freie Universität Berlin
Location: Berlin, Germany
Period: 30 Oct 2019 – 3 Nov 2019.
Reason: Visiting Christoph Benzmüller to collaborate on the Leo-III theorem prover.

Sergei TIKHOMIROV
Institution: Security and Privacy Group, Technical University of Vienna
Location: Vienna, Austria
Period: 4 May 2019 – 30 Jul 2019.

Ion TURCANU
Institution: Honda R&D Europe
Location: Offenbach, Germany
Period: 12 Apr 2019.
Reason: HIGE 2018 final report meeting

Ion TURCANU
Institution: Honda R&D Europe
Location: Offenbach, Germany
Period: 17 Dec 2019.
Reason: New project kickoff meeting

Leon VAN DER TORRE
Institution: Zhejiang University
Location: Hangzhou, China
Period: 8 Jan 2019 – 10 Feb 2019.

Leon VAN DER TORRE
Institution: University of Bologna
Location: Bologna, Italy
Period: 28 Mar 2019 – 2 Apr 2019.

Leon VAN DER TORRE
Institution: CSIRO, Data 61
Location: Brisbane, Australia
Period: 8 May 2019 – 14 Jun 2019.

Leon VAN DER TORRE
Institution: University of Bologna
Location: Bologna, Italy
Period: 20 Jun 2019 – 22 Jun 2019.

Leon VAN DER TORRE
Institution: University of Montpellier
Location: Montpellier, France
Period: 10 Jul 2019 – 12 Jul 2019.

Leon VAN DER TORRE
Institution: Cambridge University
Location: Cambridge, United Kingdom
Period: 21 Aug 2019 – 24 Aug 2019.

Leon VAN DER TORRE
Institution: Zhejiang University
Location: Hangzhou, China
Period: 1 Sep 2019 – 17 Sep 2019.

Leon VAN DER TORRE
Institution: University of Porto
Location: Porto, Portugal
Period: 4 Oct 2019 – 8 Oct 2019.

Leon VAN DER TORRE
Institution: University of Bologna
Location: Bologna, Italy
Period: 18 Nov 2019 – 20 Nov 2019.

Leon VAN DER TORRE
Institution: CRIL
Location: Lens, France
Period: 25 Nov 2019 – 27 Nov 2019.

Marie-Laure ZOLLINGER
Institution: ETH Zurich
Location: Zurich, Switzerland
Period: 4 Mar 2019 – 6 Mar 2019.

Marie-Laure ZOLLINGER
Institution: University of Surrey
Location: Surrey, United Kingdom
Period: 13 May 2019 – 17 May 2019.

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 2019. The most significant changes are:

- Improvement of the user interface through the use of selection widgets that support search and auto-completion. This change makes the user interface more responsive and prevents the user from having to scroll through very long lists to find a particular element.
- Asynchronous rendering of reports and websites using a task queue. This change prevents the system from being swamped by long-running requests for rendered PDF files and improves responsiveness.
- The implementation was ported from Python 2 to Python 3 and from Django 1.11 to Django 2.2.

ACVTool

https://github.com/pilgun/acvtool

License: APACHE License, Version 2.0

Members: Stanislav DASHEVSKYI (Designer), Olga GADYATSKAYA (Designer), 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)

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.

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 Software Changes: a second version of the tool has been started to generalised the assessment coverage. In this manner, the tool can used to assess knowledge on different domains, while keeping enough flexibility on the configuration of the assessment method such that no modifications at the level of the tool are required.

ASSA-PBN

http://satoss.uni.lu/software/ASSA-PBN/

License: free use

Members: Andrzej MIZERA (Designer), Jun PANG (Analyst), Soumya PAUL (Designer), Cui SU (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/.

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)

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 maintenance and development of the BiCS Management Tool have been continued. The focus is in improvement of the tool, adding new functionality and finding/fixing bugs as well as refactoring the current code to make it stable and decrease the manual administration work as much as possible. Also proposed a new architecture for future releases based on SPA, microservices, DevOps and Cloud approaches.

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), 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: New website was developed and deployed to production. The newer version is under active development and is planned to be deployed in the middle of February 2020. It includes changes in the website architecture, uses new CMS (Wagtail), and it is based on deploying as a serverless app by using automated continuous delivery pipeline.

BlockSci

http://github.com/cryptolu/BlockSci

License: GNU General Public License Version 3

Members: Daniel FEHER (Developer)

Description: A high-performance tool for Zcash blockchain science and exploration.

CheckMasks: formal verification of side-channel countermeasures for cryptographic implementations

https://github.com/coron/checkmasks

License: GPL v2

Members: Jean-Sébastien CORON (Designer)

Description: 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.

References:

[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)

Coco Müller

License: Proprietary

Members: Sviatlana HOEHN (Supervisor)

Description: Practicing foreign language conversation with a machine may have multiple advantages: a machine does not judge, a machine is always available and accessible from everywhere. In this project we focus on language understanding and generation for German as a communication language for non-native speakers.

Changes: In the last quarter of 2019, the chatbot passed the “alpha” tests and went to “beta” stage on Facebook Messenger.

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)

Description: DBVerify is a set of Tamarin implementation of several state-of-the-art distance-bounding protocols as well as their MSC representation. It intends to show the usage of the causality-based verication methodology proposed in our paper ”Distance-Bounding Protocols: Verication without Time and Location” (published at IEEE S&P’18). It was developed by Zach Smith (ZS) and Jorge Toro-Pozo (JT).

Changes: Extended to include the methodology in the ACM CCS 2019 paper ”Post-collusion security and distance bounding”.

Disputool

https://disputool.uni.lu/

License: Free use

Members: Shohreh HADDADAN (Developer)

Description: This website was created as a demonstration of my research project: ”Argument mining in political debates data”. It contains the annotated dataset

with argument components(Claim/Premise) divided by date and year.

The neural network model with the best results trained on identifying argument components is also integrated in this website so that users can interact and test the model. This demo website is going to be improved with more visualizations including topic model visualizations soon.

E4L: Energy for Life

License: to be defined

Members: Kevin Laurent BIEWESCH (Developer), Alfredo CAPOZUCCA (Architect), Phillip DALE (Developer), Boris FLOKA (Developer), Michele MELCHIORRE (Developer), Romain ROLAND (Developer), Thibault Jean Angel SIMONETTO (Developer), Max WOLTER (Developer)

Description: E4L: Energy for Life is a web application aimed at helping people to calculate their daily energy consumption, and allow them to compare between days, and between people. In this manner, users input information using pictures that best fit their daily experience, and then the tool compares the persons data, to Luxembourg, European, and World averages. Thus, the tool is supposed to help people understand better energy or how much they use. The development of this web application forms the core of a larger educational and research concept. This work is done in collaboration with the Laboratory for Energy Materials (LEM).

Changes: A second version of the tool has been started to generalised the assessment coverage. In this manner, the tool can used to assess knowledge on different domains, while keeping enough flexibility on the configuration of the assessment method such that no modifications at the level of the tool are required.

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

FELICS

https://github.com/cryptolu/FELICS

License: GNU General Public License Version 3

Members: Luan CARDOSO DOS SANTOS (Developer), Johann GROSZSCHÄDL (Developer)

Description: FELICS is an open-source framework for the fair and consistent evaluation of lightweight cryptographic primitives on 8-bit AVR, 16-bit MSP430, and 32-bit ARM Cortex-M microcontrollers. Further information about FELICS

can be found on the CryptoLux Wiki at https://www.cryptolux.org/index.php/FELICS.

Changes: In 2019, the FELICS framework was extended to support Authenticated Encryption with Associated Data (AEAD) algorithms. A detailed description of the AEAD extension can be found in the paper "FELICS-AEAD: Benchmarking of Lightweight Authenticated Encryption Algorithms" by Luan Cardoso dos Santos, Johann Großschädl, and Alex Biryukov: https://orbilu.uni.lu/handle/10993/41537.

Findel

https://github.com/cryptolu/findel

License: GNU General Public License Version 3

Members: Alexei BIRYUKOV (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".

Fudomo

https://atom.io/packages/language-fudomo

License: MIT

Members: Christian GLODT (Designer, Developer, Tester), Pierre KELSEN (Tester, Supervisor)

Description: Implementation of a model transformation approach based on functional decomposition, including a plugin for the Atom text editor as well as command-line tools and libraries.

Changes: The initial implementation was started in June 2019.

IDP

http://icr.uni.lu/mcramer/index.php?id=3

License: Public

Members: Diego Agustin AMBROSSIO (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

LegendrePRF

http://github.com/cryptolu/LegendrePRF

License: MIT

Members: Aleksei UDOVENKO (Developer)

Description: This repository contains an implementation of the attack from the paper Cryptanalysis of the Legendre PRF and Generalizations by *Ward Beullens, Tim Beyne, Aleksei Udovenko, and Giuseppe Vitto*. The code can be used to break **Challenge 2** of the Legendre PRF Bounties in under 1500 CPU-hours. For more details, please refer to the paper.

LEO-III

https://github.com/leoprover/Leo-III

License: BSD

Members: Alexander STEEN (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.

Changes: Leo-III 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. It is based on a paramodulation calculus with additional ordering constraints and, in tradition of its predecessor LEO-II, heavily relies on cooperation with external (mostly first-order) theorem provers for increased performance. Leo-III won the annual World Championship for Automatic Theorem Proving ("CADE ATP System Competition", in short CASC) which took place on 28-29 August 2019 in Brazil. It is now in version 1.4.

Lightning-Privacy

https://sites.google.com/view/lightning-privacy/home

License: GNU General Public License Version 3

Members: Sergei TIKHOMIROV (Developer)

Description: The scripts and data used for the paper "A Quantitative Analysis of Security, Anonymity and Scalability for the Lightning Network".

LUNA

http://engelmann.uni.lu/stripsannotation/index.php

License: Open Toolbox

Members: Christoph SCHOMMER (Analyst), Joshgun SIRAJZADE (Architect)

Description: Despite some recent work, the ongoing research for the processing of Luxembourgish is still largely in its infancy. While a rich variety of linguistic processing tools exist, especially for English, these software tools offer little scope for the Luxembourgish language. LuNa (a Tool for Luxembourgish National Corpus) is an Open Toolbox that allows researchers to annotate a text corpus written in Luxembourgish language and to build/query an annotated corpus. The aim of the paper is to demonstrate the components of the system and its usage for Machine Learning applications like Topic Modelling and Sentiment Detection. Overall, LuNa bases on a XML-database to store the data and to define the XML scheme, it offers a Graphical User Interface (GUI) for a linguistic data preparation such as tokenization, Part-Of-Speech tagging, and morphological analysis – just to name a few.

Presented at:

19th Industrial Conference on Data Mining, ICDM 2019. Poster Proceedings 2019. New York. 17 - 21 July 2019.

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 re-implementation of the MICS management system that was started in 2018 was continued in 2019. The numerous changes that have been applied have primarily served to add missing small features and to fine-tune the working of the system.

MinUS

http://satoss.uni.lu/software/MinUS

License: free use

Members: Jun PANG (Analyst)

Description: This tool, MinUS, integrates the technologies of trajectory pattern mining with the state-of-the art research on discovering user similarity with trajectory patterns. Specifically, with MinUS, we provide a platform to manage movement datasets, and construct and compare users trajectory patterns. Tool users can compare results given by a series of user similarity metrics, which allows them to learn the importance and limitations of different similarity metrics and promotes studies in related areas, e.g., location privacy. Additionally, MinUS can also be used by researchers as a tool for preliminary process of movement data and parameter tuning in trajectory pattern mining. The tool is available at http://satoss.uni.lu/software/MinUS.

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.

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.

The goal of the software is to allow automate the “augmentation” of CPAL models with dependability mechanisms (e.g., process and data redundancy, voting). The software takes a model as input and transform it into a functionally equivalent model that meets additional dependability properties. Currently, the software is able to augment a model with the N-Version Programming fault-tolerance pattern, which is a central pattern in the field of critical systems.

This is the first MT framework dedicated to the CPAL language. Because it operates within the boundaries of the CPAL language it allows to retain the ability to accomplish non-functional analyses on both the original and the transformed model, be it in a simulation environment or on the actual target. For example, both scheduling and code coverage analysis, are still applicable to the transformed model, in order to properly assess MT suitability, overhead and performance in a specific application scenario. The MT framework is thread-safe and features a plugin based infrastructure and internal caches for speed. The MT framework has been designed according to a modular four-layer architecture depicted in the figure below and implemented as about 9500 lines of C code.

Authors: Tingting Hu, Nicolas Navet, Ivan Cibrario Bertolotti, Loïc Fejoz, and Lionel Havet

ReCon

https://github.com/cryptolu/ReCon

License: GNU General Public License Version 3

Members: Alexei BIRYUKOV (Designer), Daniel FEHER (Developer)

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 Cryptographic Library in Python

License: Internal use only

Members: Artem KALIAHIN (Developer), Peter Y A RYAN (Supervisor)

Selene User Interface

License: Internal use only

Members: Marie-Laure ZOLLINGER (Developer)

Changes: Iteration, testing of user experience.

Sketchnoting

License: N/A

Members: Aryobarzan ATASHPENDAR (Developer), Christian GREVISSE (Architect)

Description: Enhanced sketchnoting (iOS app) for the retrieval and integration of learning material.

Features handwriting recognition and semantic annotation for retrieving resources relevant to the concepts mentioned in the handwritten notes from existing Knowledge Graphs. Drawing recognition enables visual queries, allowing for enhanced search capabilities.

SPARKLE

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

License: GNU General Public License Version 3

Members: Luan CARDOSO DOS SANTOS (Developer), Johann GROSZSCHÄDL (Developer)

Description: Reference and optimized C implementation of the permutation SPARKLE, the authenticated encryption algorithm SCHWAEMM, and the hash function ESCH.

SPARKLE

https://github.com/cryptolu/sparkle

License: GNU General Public License Version 3

Members: Aleksei UDOVENKO (Developer)

Description: SPARKLE is an ARX-based cryptographic permutation suitable for software implementation on 8/16/32-bit microcontrollers. SCHWAEMM and ESCH are an authenticated encryption algorithm and a hash function, respectively, which use the SPARKLE permutation in a sponge construction. This repository contains supporting software for the security analysis of SPARKLE, SCHWAEMM, and ESCH.

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)

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), 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.

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	67.79
Research Associate	23.97
Professor	22.69
Postdoctoral Researcher	20.56
Research Scientist	16.98
Student / Intern	13.86
Scientific / Technical Support Staff	11.53
Administrative Staff	3.77
Project Coordinator	1.20
Program Coordinator	1.00
Chief Scientist	0.16
Total	*183.52*

Table E.1: Number of Staff by Category

E.2 Distribution of Staff by Category

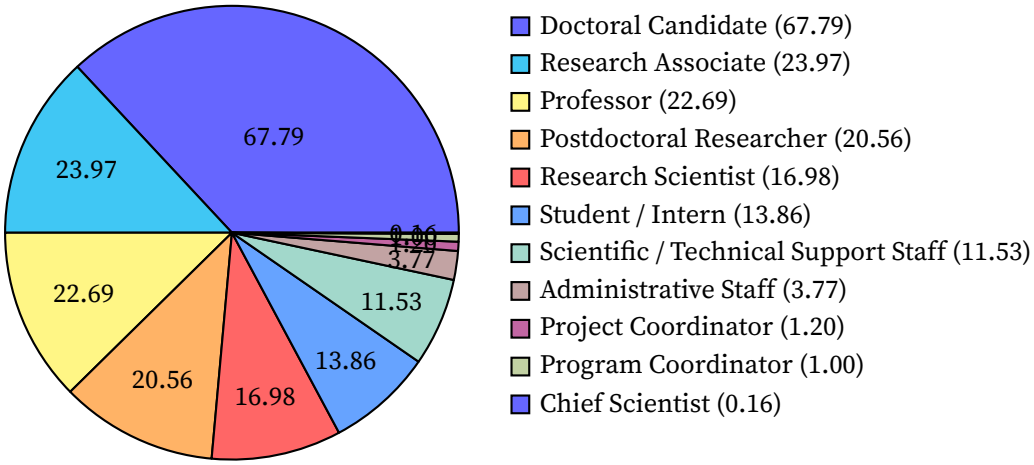


Figure E.1: Staff Distribution

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	BIRYUKOV	Alexei
	BOUVRY	Pascal
	BRIAND	Lionel (0.75 FTE)
	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
	STEENIS	Bernard
	THEOBALD	Martin

Category	Last Name	First Name
	VAN DER TORRE	Leon
	ZAMPUNIERIS	Denis
Research Scientist	BERNARD	Nicolas
	BISSYANDE	Tegawendé François d Assise
	BOTEV	Jean
	CAPOZUCCA	Alfredo
	CORDY	Maxime
	DANOY	Grégoire
	FRANCK	Christian
	HU	Tingting (0.84 FTE)
	KLEIN	Jacques (0.83 FTE)
	LENZINI	Gabriele
	MA	Qin (0.83 FTE)
	PANG	Jun
	PAPADAKIS	Mike
	PINEL	Frederic (0.84 FTE)
	RIES	Benoit
	ROENNE	Peter (0.50 FTE)
	RUPP	Andy (0.16 FTE)
	VARRETTE	Sébastien
	WEYDERT	Emil
Postdoctoral Researcher	ALEKSANDROVA	Marharyta (0.16 FTE)
	AMBROSSIO	Diego Agustin (0.50 FTE)
	BOYTSOV	Andrey (0.80 FTE)
	BURSUC	Sergiu (0.33 FTE)
	CASINI	Giovanni (0.99 FTE)
	COGLIATI	Benoît-Michel
	DESPOTOVIC	Vladimir (0.33 FTE)
	ELLAMPALLIL VENUGOPAL	Vinu (0.99 FTE)
	HASAN	Cengis (0.50 FTE)
	HOEHN	Sviatlana
	HORNE	Ross James
	HU	Tingting (0.16 FTE)
	HURIER	Médéric (0.33 FTE)
	KIEFFER	Emmanuel (0.71 FTE)
	LOPEZ BECERRA	Jose Miguel (0.67 FTE)
	MARKOVICH	Réka
	MIZERA	Andrzej (0.71 FTE)
	MOULINE	Ludovic (0.13 FTE)
	MUELLER	Johannes (0.42 FTE)
	NAJJAR	Amro (0.67 FTE)
	OSVIK	Dag Arne (0.78 FTE)
	PARENT	Xavier (0.99 FTE)

Category	Last Name	First Name
	PAUL	Soumya (0.91 FTE)
	RAMPARISON	Mathias (0.25 FTE)
	RIAL	Alfredo
	SAHU	Rajeev Anand
	SIRAJZADE	Joshgun (0.50 FTE)
	STEEN	Alexander (0.99 FTE)
	STOLFI ROSSO	Daniel (0.91 FTE)
	TITCHEU CHEKAM	Thierry (0.16 FTE)
	WASIM	Muhammad Umer (0.63 FTE)
Research Associate	ALEKSANDROVA	Marharyta (0.83 FTE)
	ALLIX	Kevin
	ATASHPENDAR	Arash (0.91 FTE)
	BANA	Gergely (0.16 FTE)
	BARTEL	Alexandre
	BEIERLE	Christof (0.41 FTE)
	BHAUMIK	Ritam (0.20 FTE)
	BOUALOUACHE	Abdelwahab (0.63 FTE)
	BOYTSOV	Andrey (0.20 FTE)
	BRUST	Matthias R.
	CHEN	Xihui (0.96 FTE)
	DASHEVSKYI	Stanislav (0.78 FTE)
	FOTIADIS	Georgios (0.96 FTE)
	GADYATSKAYA	Olga (0.49 FTE)
	IOVINO	Vincenzo (0.66 FTE)
	JAMROGA	Wojciech (0.50 FTE)
	KAISER	Daniel
	KINTIS	Marinos (0.16 FTE)
	KRISHNASAMY	Ezhilmathi (0.33 FTE)
	MESTEL	David
	MSADEK	Mohamed Nizar (0.08 FTE)
	OSTREV	Dimiter
	OSVIK	Dag Arne (0.21 FTE)
	RAMIREZ CRUZ	Yunior
	ROBALDO	Livio
	ROBERT	Jérémy
	ROENNE	Peter (0.49 FTE)
	ROSSI	Arianna (0.75 FTE)
	SCHIFFNER	Stefan
	SOUA	Ridha
	SYMEONIDIS	Iraklis
	TURCANU	Ion
	WANG	Jun (0.24 FTE)
	WANG	Qingju
Program Coordinator	LADID	Latif
Project Coordinator	OCHSENBEIN	Anne (0.50 FTE)

Category	Last Name	First Name
	OESTLUND	Stefanie (0.70 FTE)
Scientific / Technical Support Staff	BRANT	Florence (0.20 FTE)
	CARTIAUX	Hyacinthe
	CREPALDI	Marco (0.18 FTE)
	GLODT	Christian
	GROSZSCHÄDL	Johann
	HOUITTE	Pierre-Yves (0.67 FTE)
	KARPATI	Daniel (0.33 FTE)
	KONCHENKO	Stanislav (0.99 FTE)
	MACHALEK	Aurel
	MUELLER	Johannes (0.40 FTE)
	PARISOT	Clément (0.66 FTE)
	PLUGARU	Valentin
	RAMPARISON	Mathias (0.08 FTE)
	REIS	Sandro
	SKORSKI	Maciej (0.16 FTE)
	STEMPER	André
	UDOVENKO	Aleksei (0.50 FTE)
	WASIM	Muhammad Umer (0.36 FTE)
Doctoral Candidate	AL-JAWAHERI	Husam (0.50 FTE)
	ANTONIADIS	Nikolaos
	ATASHPENDAR	Arash (0.08 FTE)
	BALOGLU	Sevdenur (0.50 FTE)
	BARTHEL	Jim Jean-Pierre (0.99 FTE)
	BENEDICK	Paul-Lou
	BHADAURIA	Anshuman Singh (0.91 FTE)
	BUSCEMI	Alessio (0.96 FTE)
	CAPPONI	Andrea (0.99 FTE)
	CARDOSO DOS SANTOS	Luan (0.99 FTE)
	CHANGAIVAL	Boonyarit (0.99 FTE)
	CHAYCHI	Samira (0.25 FTE)
	CHEN	Ninghan (0.59 FTE)
	CHENG	Hao (0.16 FTE)
	CHITIC	Ioana Raluca (0.33 FTE)
	DAMODARAN	Aditya Shyam Shankar
	DAUPHIN	Jérémie (0.99 FTE)
	DE LA CADENA RAMOS	Augusto Wladimir
	DI MAIO	Antonio
	DUFLO	Gabriel (0.80 FTE)

Category	Last Name	First Name
	EL ORCHE	Fatima Ezzahra (0.99 FTE)
	ESMAEILZADEH DILMAGHANI	Saharnaz
	ESTAJI	Ehsan (0.59 FTE)
	FARJAMI	Ali (0.99 FTE)
	FEHER	Daniel (0.99 FTE)
	FISCARELLI	Antonio Maria
	FU	Shange (0.70 FTE)
	GAO	Jun
	GENÇ	Ziya Alper
	GHAMIZI	Salah (0.96 FTE)
	GREVISSE	Christian (0.99 FTE)
	GUO	Siwen (0.99 FTE)
	HADDADAN	Shohreh
	HU	Hailong (0.08 FTE)
	HURIER	Médéric (0.66 FTE)
	IBRAHIM	Abdallah Ali Zainelabden Abdallah (0.99 FTE)
	JAFARNEJAD	Sasan
	JAHIC	Benjamin (0.99 FTE)
	KAMLOVSKAYA	Ekaterina
	KELLER	Patrick (0.29 FTE)
	KIEFFER	Emmanuel (0.08 FTE)
	KIM	Kisub
	KOLBE	Niklas
	KONG	Pingfan
	LIU	Chao
	LIU	Kui
	LOPEZ BECERRA	Jose Miguel (0.33 FTE)
	MA	Wei
	MAHYA	Parisa (0.16 FTE)
	MAI	TIEU LONG (0.99 FTE)
	MEDER	Jeff Alphonse Antoine (0.29 FTE)
	MEDER	Paul Joseph Yves
	MITSEVA	Asya (0.99 FTE)
	MOULINE	Ludovic (0.87 FTE)
	NEYENS	Gilles (0.74 FTE)
	NOTARNICOLA	Luca
	PEJO	Balazs (0.74 FTE)
	PEREIRA	Vitor
	PILGUN	Aleksandr
	RIDA	Ahmad (0.99 FTE)
	RIOM	Timothée
	ROSSI	Arianna (0.24 FTE)
	RWEMALIKA	Renaud

Category	Last Name	First Name
	SALA	Petra
	SAMIR LABIB	Nader
	SMITH	Zachary Daniel (0.99 FTE)
	SOROUSH	Najmeh
	STOJKOVSKI	Borce (0.99 FTE)
	SU	Cui
	SUN	Ningyuan (0.16 FTE)
	TAWAKULI	Amal (0.99 FTE)
	TEMPERONI	Alessandro (0.63 FTE)
	TIKHOMIROV	Sergei (0.99 FTE)
	TITCHEU CHEKAM	Thierry (0.83 FTE)
	TORCHYAN	Khachatur
	TORO POZO	Jorge Luis (0.41 FTE)
	UDOVENKO	Aleksei (0.33 FTE)
	VAN WIER	Jeroen
	VAZQUEZ SANDOVAL	Itzel
	VITTO	Giuseppe
	YURKOV	Semen (0.75 FTE)
	ZHONG	Zhiqiang (0.99 FTE)
	ZOLLINGER	Marie-Laure
Administrative Staff	EDWARDSDOTTIR	Helga Fanney
	FINNSSON	
	FLAMMANG	Danièle (0.74 FTE)
	PUECH	Andrea (0.20 FTE)
	SCHMITZ	Fabienne
	SCHROEDER	Isabelle (0.50 FTE)
	WOLTERS	Nicola (0.33 FTE)
Student / Intern	ANTROPOVA	Daria (0.08 FTE)
	ATASHPENDAR	Aryobarzan (0.36 FTE)
	BERNARDO	Lutiano Gabriel (0.01 FTE)
	BONTE	Eliott Cyril Michel (0.08 FTE)
	CARBOGNANI	Enrico Alarico (0.11 FTE)
	CHENG	Hao (0.46 FTE)
	CHERNAKOV	Pavel (0.13 FTE)
	DE JESUS SOUSA	Tiago Alexandre (0.08 FTE)
	DEMARCHE	Eric (0.36 FTE)
	DUPONT	Briag Gerard Benjamin (0.05 FTE)
	ELZUBAIR	Ayman (0.54 FTE)
	FARAH	Aamir (0.13 FTE)
	FELTEN	Charel (0.01 FTE)
	FILIMONOV	Ihor (0.48 FTE)

Category	Last Name	First Name
	FLOKA	Boris (0.28 FTE)
	FRANCI	Adriano (0.35 FTE)
	GAREEV	Daniel (0.11 FTE)
	GHOLAMI BOROUJENI	Farzaneh (0.08 FTE)
	GOERKE	Gavin (0.16 FTE)
	HAMZIC	Ervin (0.64 FTE)
	HAWLADER	Faisal
	HUMBERT	Tom (0.08 FTE)
	JACOBS	Kwinten (0.02 FTE)
	JAHIC	Alen (0.30 FTE)
	JAHIC	Dzenita (0.34 FTE)
	KALF	Patrick (0.28 FTE)
	KELLER	Patrick (0.36 FTE)
	KEPUSKA	Ema (0.54 FTE)
	KIHN	Pol (0.05 FTE)
	KIM	Minsuk (0.17 FTE)
	KOC	Muhammed Fatih (0.17 FTE)
	KREMER	Iris Pascale (0.26 FTE)
	LANG	Scott (0.22 FTE)
	LIMONIER	Joris, Shan, Andre (0.18 FTE)
	LOVASZ	Abel (0.25 FTE)
	MAGALHAES	Gilles (0.25 FTE)
	MORSELETTO	Sofia (0.49 FTE)
	NASIB	Sadi (0.14 FTE)
	OUHSSAIN	Hamza (0.38 FTE)
	PETREAN-MACELARU	Alex (0.09 FTE)
	POGOSIAN	Davit (0.22 FTE)
	REBELO NEVES	Jason (0.19 FTE)
	REICHER	Thomas (0.25 FTE)
	RIGHETTI ABIGO	Luciano (0.41 FTE)
	ROLAND	Romain (0.55 FTE)
	SANCHEZ	Julien (0.29 FTE)
	SEVESTRE	Tom (0.29 FTE)
	SIMONETTO	Thibault Jean Angel (0.49 FTE)
	THAMILSELVAN	Venkateshwaran (0.16 FTE)
	VIEGAS MILANI	Adriano (0.07 FTE)
	VIJAYAKUMAR	Bharathi (0.11 FTE)
	WEBER	Rodrigo Lucas (0.13 FTE)
	WILSON	Marc (0.02 FTE)
	XU	Jingjing (0.16 FTE)
	YAMAN	Kendal (0.41 FTE)
Chief Scientist	KLEIN	Jacques (0.16 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

https://dcs.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:

Isabelle Glemot-Schroeder, Andrea Puech and Fabienne Schmitz
Email: dcs@uni.lu