CSC | Computer Science and Communications

UNIVERSITY OF LUXEMBOURG

FACULTY OF SCIENCE, TECHNOLOGY AND COMMUNICATION

Computer Science and Communications

Activity Report 2016

CSC | Computer Science and Communications

Computer Science and Communications

Activity Report 2016

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

Computer Science and Communications
Activity Report 2016

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

Administrative Contact:

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

http://csc.uni.lu

Editor: Christian Glodt
Release date: 2017-07-17
Note: This report was created using LaTeX with a template based on previous work by Sebastien Varrette.

Preface

Dear reader,

This annual report synthesises the progress and activities of the Computer Science & Communications (CSC) Department in 2016. It gives an overview of most of the many activities conducted in the CSC.

In 2016 we had the first scientific evaluation of the CSC, and many of the insights from the self assessment report have found their way into this report. As a consequence, the structure of the report has changed with respect to the annual CSC reports of the past ten years.

In this report, you will find the most significant facts of 2016, concerning our research projects, organized events, awarded papers, visiting researchers and publications.

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

Best regards,

Leon van der Torre

Sjouke Mauw

Contents

1 Mission 1

2 Executive Summary 3

3 Research Areas 5

4 Research Groups 9

4.1 Algorithmic Decision Theory (ADT) 9

4.2 Applied Crypto Group (ACG) 11

4.3 Applied Security and Information Assurance (APSIA) 11

4.4 BigData, Data Science & Databases (BigData) 13

4.5 Collaborative and Socio-Technical Systems (COaST) 14

4.6 Communication and Information Theory (Cain) 15

4.7 Critical and Extreme Security and Dependability (CritiX) 16

4.8 Critical Real-Time Embedded Systems (CRTES) 18

4.9 CryptoLux team 19

4.10 Foundations of Model-Driven Engineering (FMDE) 21

4.11 Individual and Collective Reasoning (ICR) 22

4.12 Information Mining and Learning (MINE) 24

4.13 Methods and Tools for Scientific Requirements Engineering (MESSIR) 26

4.14 Parallel Computing and Optimisation Group (PCOG) 27

4.15 Proactive Computing 29

4.16 Security and Networking Lab (SECAN-Lab) 30

4.17 Security and Trust of Software Systems (SaToSS) 32

4.18 Security, Reasoning and Validation (SerVal) 35

4.19 Systems and Control Engineering (SCE) . . . 36
4.20 Team Leprévost . . . 38

5 Organizational Structure 41

6 Education 43
6.1 Doctoral Programme in Computer Science and Computer Engineering . . . 43
6.2 Certificate Smart ICT for business innovation . . . 43
6.3 Master in Information and Computer Sciences (MICS) . . . 44
6.4 Master en Management de la Sécurité des Systèmes d'Information 44
6.5 Bachelor of Engineering in Computer Science (BINFO) . . . 45

Appendix 46

A Publication List 47
A.1 Book . . . 48
A.2 Book Chapter . . . 49
A.3 Journal . . . 49
A.4 Thesis . . . 55
A.5 Conference . . . 56
A.6 Technical Report . . . 75
A.7 Miscellaneous . . . 76
A.8 Unpublished . . . 78

B Research Projects 81
B.1 COST Action Projects . . . 82
B.2 Directorate-General for Education and Culture (EC) Projects . . . 85
B.3 EC - FP7 Projects . . . 88
B.4 ESA Projects . . . 92
B.5 European Defence Agency - EDA Projects . . . 93
B.6 External organisation funding Projects . . . 94
B.7 FNR - AFR Projects . . . 99
B.8 FNR - AFR PhD Projects . . . 100
B.9 FNR - AFR PostDoc Projects . . . 110
B.10 FNR - AFR Projects . . . 113

B.11 FNR - CORE Projects 114
B.12 FNR - INTER Projects 129
B.13 FNR - Luxembourg (AFR - PHD) Projects 143
B.14 FNR - Other Projects 144
B.15 Horizon 2020 (EU) Projects 154
B.16 International call ANR - FNR Luxembourg () Projects 167
B.17 UL (PUL) Projects 168
B.18 UL Funding Projects 171
B.19 Undefined Funding Projects 175
B.20 Unfunded Projects 175

C Representational Activities **181**
C.1 Conference Committee Memberships 181
C.2 Doctoral Thesis Defense Committee Memberships 239
C.3 Awards 247
C.4 Media Appearances 248
C.5 Guest Researchers 251
C.6 Visits 259

D Software Developments **267**

E Staff Statistics **281**
E.1 Number of Staff by Category (Full-Time Equivalent) 281
E.2 Distribution of Staff by Category 282
E.3 List of Members by Category 282

F List of Acronyms **289**

Chapter 1

Mission

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

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

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

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

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

Chapter 2

Executive Summary

The Computer Science and Communications Department, also known as CSC (http://csc.uni.lu), includes a staff of more than 165 full-time equivalent members involved in both teaching and research activities.

The scope of the lectures in the study programmes at Bachelor and Master levels includes topics covering fundamental aspects of computer science as well as practical ones. Close supervision and guidance are ensured by an open door policy and project based lecturing. The CSC is also involved in life-long learning by organising a master degree in Information Systems Security Management in collaboration with LIST, the Luxembourg Institute of Science and Technology.

Many of CSC faculty staff members, as well as their research groups, are involved in SnT and LCSB research, thus forging a tighter connection between the computer science research unit and the interdisciplinary research centers. Five laboratories of the interdisciplinary centre in security, reliability and trust (SnT) are also headed by CSC professors and several of our professors are involved personally as fellows in the two interdisciplinary centres of the University (LCSB and SnT).

The CSC is thus very involved in the development of the Interdisciplinary Centre of Security and Trust (SnT) research center. As a matter of fact, a majority of the research projects of the SnT have Principal Investigators from the CSC and most of the PhD students from SnT are supervised by CSC faculty members. The CSC thus counts among its major achievements its continued support of the SnT.

The CSC is cooperating in a large set of international as well as regional projects. The CSC (http://csc.uni.lu) is divided into 4 themes:

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

Head

- Leon van der Torre, professor, head of CSC

Vice head

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

Academic Staff

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

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

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

Since CSC counts among its major achievements the continued support of the SnT, please look at the SnT 2016 annual report to get a complementary overview of CSC activities in the area of Security, Reliability and Trust.

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 School of Computer Science and Computer Engineering 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 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, 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 would strengthen or complete the topics covered by CSC according to this priority. Instead of a top-down overarching cohesion, we have underlying synergies/cohesion within and between labs/themes coming from shared research interests. Another dimension that should not be neglected is cohesion through the elaboration of consistent teaching programs.

Detailed Research Program

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

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

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

Regarding Intelligent and Adaptive Systems (ILIAS), we investigate the theoretical foundations and algorithmic realisations of intelligent systems for complex problem solving and decision making in uncertain and dynamic environments. Our activities fit the rapidly growing role of artificial intelligence, big data and robotics. The collaboration with LCSB and LSF, the involvement with the High Performance Computing facility (HPC) and the Computational Sciences initiative, and the FinTech affinity, reflect Luxembourg's strategic priorities. Current research areas are:

- Knowledge Representation and Reasoning: concerned with normative reasoning in multi-agent systems (e.g., logics for security and compliance, machine ethics), legal knowledge representation, inference under uncertainty and inconsistency, logic-based models for intelligent agents/robots, and computational choice.
- Algorithmic Decision Theory: the theory and practice of systems for decision support.
- Data Science: the areas of interest include text mining and information extraction, data mining and knowledge discovery. The interdisciplinary character is documented by active collaborations with the Luxembourg School of Finance, the Life Sciences, Psychology and Digital History.
- Information Theory and Stochastic Inference: the main research topics here are signal processing, error-correcting codes and probabilistic graphical models.
- Parallel Computing and Optimisation: research on parallel computing and optimisation 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.

This proliferation of digital communication and the transition of social interac-

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

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

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

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

Chapter 4

Research Groups

4.1 Algorithmic Decision Theory (ADT)

Head of research group: Prof. Dr. Raymond Bisdorff

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

Summary of the group's achievements in 2016

The year 2016 was particularly successful. We developed multicriteria ranking algorithms for large sets of potential decision alternatives: up to several millions of alternatives evaluated on multiple incommensurable ordinal performance criteria and in potential presence of many missing data. This research is motivated by the development of a visualization tool - a *heat map* - for performance tables showing the decision alternatives linearly ordered form the best to the worst, and the marginal criterion performances colored by quantiles equivalence classes (see picture below). By using Python-3.5 multiprocessing resources and the Digraph3 multicriteria software library, we may linearly rank without ties on the UL HPC gaia-80 machine with 120 single threaded cores and a CPU memory of 2.5 TB, in less than three hours (2h55') a huge set of 2.5 millions of decision alternatives evaluated on 21 performance criteria by balancing an economic, an ecological and a societal decision objective. Data input is, on the one side, a 2500000x21 performance tableau of size 5GB, and on the other side, a theoretical outranking space consisting of 6.25 trillions (6.25 x 1012) of pairwise comparisons. A "small" set of 1000 decision alternatives, in a similar setting, may thus be ranked typically in less than a second.

Main publications and achievements in 2016

1. **R. Bisdorff (2016). Computing linear rankings from trillions of pairwise outranking situations.** In Proceedings of DA2PL'2016 *From Multiple Criteria Decision Aid to Preference Learning*, R. Busa-Fekete, E. Hüllermeier, V. Mousseau and K. Pfannschmidt (Eds.), University of Paderborn (Germany), Nov. 7-8 2016: 1-6. In this paper, we present in this paper a sparse HPC implementation for outranking digraphs of huge orders, up to several millions of decision alternatives. The proposed outranking digraph model is based on a quantiles equivalence class decomposition of the underlying multicriteria performance tableau. When locally ranking each of these ordered components, we may readily obtain an overall linear ranking of big sets of decision alternatives.

2. **R. Bisdorff, A sparse outranking digraph model for HPC-ranking of big performance tableaux.** Presentation at EURO 2016, *28th European Conference on Operational Research*, Poznan (Poland), 3-6 July, 2016. In the context of the ongoing GDRI-Algodec "Algorithmic Decision Theory", supported o.a. by the CNRS (France) and the FNR (Luxembourg), we develop multicriteria ranking HPC algorithms for large sets of potential decision alternatives: up to several millions of alternatives evaluated on multiple incommensurable ordinal performance criteria.

3. ***R. Bisdorff, Ranking big performance tableaux with multiple incommensurable criteria and missing data.*** *Presentation at ORBEL30, the 30th Belgian Conference on Operations Research, Louvain-la-Neuve, 28-29 January, 2016.* This research is motivated by the development of a visualization tool - a heat map - for performance tables showing the decision alternatives linearly ordered form the best to the worst, and the individual performances colored by quantiles equivalence classes (see Figure below).

criteria	Rcv	dwT	upT	MTBF	RspT	stoC	auD	enC	auT	snpC	Thrpt	Lat	LB	ouT
weights	2.00	2.00	2.00	2.00	2.00	3.00	1.00	1.00	1.00	3.00	2.00	2.00	2.00	2.00
tau(*)	0.53	0.53	0.44	0.35	0.18	0.04	0.00	0.00	0.00	0.00	0.00	0.00	0.00	-0.58
MS	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	NA	NA	NA	4.00	0.00
Ela	4.00	4.00	4.00	4.00	4.00	3.00	4.00	4.00	4.00	4.00	NA	NA	4.00	0.00
Sig	4.00	4.00	4.00	4.00	3.00	3.00	4.00	4.00	4.00	4.00	NA	NA	4.00	0.00
Cen	4.00	4.00	4.00	4.00	2.00	3.00	4.00	4.00	4.00	NA	NA	NA	4.00	0.00
Cit	4.00	4.00	2.00	3.00	2.00	3.00	4.00	4.00	4.00	4.00	NA	NA	4.00	2.00
Ggl	3.00	2.00	4.00	2.00	2.00	4.00	4.00	4.00	4.00	4.00	NA	NA	4.00	1.00
HP	3.00	3.00	3.00	4.00	4.00	3.00	4.00	4.00	4.00	4.00	NA	NA	4.00	2.00
GMO	2.00	3.00	1.00	3.00	4.00	3.00	4.00	4.00	4.00	NA	NA	NA	4.00	4.00
Rsp	3.00	NA	NA	NA	NA	3.00	4.00	4.00	4.00	4.00	NA	NA	4.00	NA
Amz	3.00	2.00	2.00	3.00	3.00	4.00	4.00	4.00	4.00	NA	NA	NA	4.00	2.00
Dig	3.00	1.00	2.00	3.00	2.00	3.00	4.00	4.00	4.00	NA	NA	NA	4.00	5.00

Color legend:

quantile	0.14%	0.29%	0.43%	0.57%	0.71%	0.86%	1.00%

(*) tau: Ordinal (Kendall) correlation between marginal criterion and global ranking relation.

Illustration: Example heat map from a CloudCom 2015 conference paper by Shyam Wagele et al.

4.2 Applied Crypto Group (ACG)

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

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

Summary of the group's achievements in 2016

New attack found against a multilinear map cryptographic scheme. The paper has appeared at the CRYPTO 2016 conference, one of the two most important conferences in cryptography.

Jean-Sebastien Coron was program co-chair of the EUROCRYPT 2016 conference, one of the two most important conferences in cryptography.

Main publications and achievements in 2016

- Jean-Sébastien Coron, Moon Sung Lee, Tancrède Lepoint, Mehdi Tibouchi: Cryptanalysis of GGH15 Multilinear Maps. CRYPTO (2) 2016: 607-628. The paper describes a new attack against a multilinear map cryptographic scheme
- Jean-Sébastien Coron, Aurélien Greuet, Emmanuel Prouff, Rina Zeitoun: Faster Evaluation of SBoxes via Common Shares. CHES 2016: 498-514. The paper describes a faster algorithm for protecting a block-cipher against side-channel attacks.
- Alberto Battistello, Jean-Sébastien Coron, Emmanuel Prouff, Rina Zeitoun: Horizontal Side-Channel Attacks and Countermeasures on the ISW Masking Scheme. CHES 2016: 23-39. The paper describes a new side-channel attack against a side-channel countermeasure.

4.3 Applied Security and Information Assurance (APSIA)

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

The APSIA group (1 professor, 1 senior scientist, 10 post docs and 8 phd students, and 3 external associates), is part of the SnT and has strong connections to CSC and the LACS laboratory. The group specializes in the design and analysis of security and privacy mechanisms and protocols. Of particular interest: authenticated key establishment protocols, both classical and quantum, and including password-based and out of band-based and secure, verifiable voting protocols. APSIA also has expertise in the socio-technical aspects of security and trust.

Summary of the group's achievements in 2016

2016 was a fruitful year for APSIA: several new projects awarded including a new CORE and Junior-CORE, as well contributing of the success of the LACS DTU PRIDE proposal. The group grew to around twenty members and is set to grow further in 2017. Three members successfully defended their PhD theses and two of these were retained as post-docs. Overall the group published over 40 papers, many in highly prestigious conferences such a Crypto. In addition, the group's output included five books/edited volumes, notably "The New Codebreakers", a collection of articles in honour of David Kahn, and "Real World Electronic Voting; Design, Analysis and Deployment", presenting the state of the art in secure voting systems. Ryan founded the Voting Workshops in association with Financial Crypto and co-chaired Voting'16 with Dan Wallach, and the Socio-Technical Aspects in Security and Trust Workshop this year associated with the ACM ACSAC. We also established a sub-group of four members working on quantum information assurance.

Courses taught: Information Security Basics, Security Modelling, Principles of Security Engineering and Theoretical Foundation of Computing

The group continues to run the internal "breakfast" talks as well contributing to the SRMs, the joint SATOSS/APSIA seminars: 32 talks featuring speakers from 13 different countries.

Main publications and achievements in 2016

- Jean Lancrenon, Marjan Skrobot, Qiang Tang: Two More Efficient Variants of the J-PAKE Protocol. ACNS 2016: 58-76. (18% acceptance rate) which extends the suite of J-PAKE protocols. The work has practical implications, since the original J-PAKE protocol is up for standardization in IETF and its Eliptic Curve version is authentication mechanism of choice in Thread protocol that is widely used in IoT products. These proposals improve the efficiency of the original J-PAKE protocol by 30%.
- Peter Y. A. Ryan, Peter B. Rønne, Vincenzo Iovino: Selene: Voting with Transparent Verifiability and Coercion-Mitigation. Financial Cryptography Workshops 2016: 176-192. This paper presents a new direction voter-verifiable schemes, making the verification much more intuitive than in prior schemes while maintaining a high degree of coercion resistance.
- Jan Camenisch, Maria Dubovitskaya, Alfredo Rial: UC Commitments for Modular Protocol Design and Applications to Revocation and Attribute Tokens. CRYPTO (3) 2016: 208-239. When designing protocols modularly in the universal composability framework, frequently it is necessary to guarantee that two or more ideal functionalities receive the same input, but no method to accomplish this has been provided. We describe a method based on a new ideal functionality for commitments.

4.4 BigData, Data Science & Databases (BigData)

Head of research group: Prof. Dr. Martin Theobald

The BigData group at the University of Luxembourg is a new research group that has been established in February 2017. The group is headed by Martin Theobald, who previously held positions at the Max-Planck-Institute in Saarbruecken, at the University of Antwerp, and at Ulm University. The group currently consists of one PhD student at the University of Luxembourg, Amal Tawakuli, and two external PhD Students, Dat Ba Nguyen (Max-Planck-Institute for Informatics, Saarbruecken) and Maarten Van den Heuvel (University of Antwerp).

Our research activities focus on 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.

(2) Probabilistic & Temporal Databases

A second research focus lies in the development of probabilistic and temporal database models and systems. The team was involved in the development of the Trio probabilistic database system at Stanford University, which was the first principled approach to couple data uncertainty with relational data by using SQL as a query language. Further ongoing research activities (in collaboration with the University of Zurich) are in the context of temporal database models that now also fully support the afore-described probabilistic extensions.

(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.

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.

Main publications and achievements in 2016

- Sairam Gurajada, Martin Theobald: Distributed Set Reachability. SIGMOD Conference 2016: 1247-1261
- Dat Ba Nguyen, Martin Theobald, Gerhard Weikum:J-NERD: Joint Named Entity Recognition and Disambiguation with Rich Linguistic Features. TACL 4: 215-229 (2016)
- Yafang Wang, Zhaochun Ren, Martin Theobald, Maximilian Dylla, Gerard de Melo: Summary Generation for Temporal Extractions. DEXA (1) 2016: 370-386

4.5 Collaborative and Socio-Technical Systems (COaST)

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

As part of the Communicative Systems Laboratory (Com.Sys), Prof. Rothkugel's group focuses on distributed collaborative systems, complex self-organizing networks and socio-technical modelling.

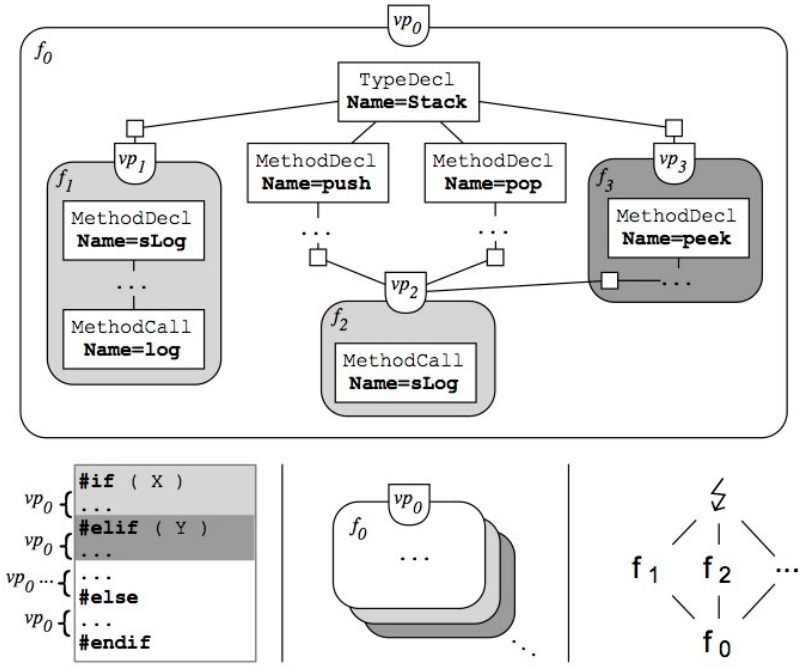
Summary of the group's achievements in 2016

Prof. Rothkugel's group counted 5 members (1 professor, 1 senior researcher, 3 PhD students) and 8 publications in 2016. In the context of both ongoing research projects CoCoDA^2 and CollaTrEx, new implementations have been developed; the CollaTrEx prototype system and basic framework for collaborative context-aware mobile training and exploration were presented at different scientific conferences, winning a best paper award. Members of the group furthermore organized various international scientific events and conferences such as MMVE 2016 or SASO 2016 and SASOST 2016. The group's teaching activities comprised numerous lectures and seminars in the various bachelor and master programs (BINFO, MICS, BINFO-FC) offered by the University of Luxembourg, as well as guest lecturing abroad.

Main publications and achievements in 2016

- **Jean Botev, Ralph Marschall, Steffen Rothkugel. CollaTrEx – Collaborative context-aware mobile training and exploration.** In Proc. 1st EAI International Conference on Design, Learning & Innovation, pp.113-120, 2016. Best Paper Award. This paper discusses the CollaTrEx framework for collaborative context-aware mobile exploration and training designed for the in-situ collaboration within groups of learners performing diverse educational activities together to explore their environment. It comprises a front-end prototype for tablet devices, as well as a web-based back-end solution for the creation and management of available activities which are determined by absolute and relative spatio-temporal context.

- **Benjamin Behringer, Steffen Rothkugel. Integrating feature-based implementation approaches using a common graph-based representation.** In Proc. 31st ACM/SIGAPP Symposium on Applied Computing, pp.1504-1511, 2016. This paper introduces a structured document graph model as common, generic representation for compositional and annotative feature implementations, enabling projections that allow fluid changes between compositional, annotative or mixed versions of the software product line.
- **Heiko Hamann, Yara Khaluf, Jean Botev, Mohammad Divband Soorati, Eliseo Ferrante, Oliver Kosak, Jean-Marc Montanier, Sanaz Mostaghim, Richard Redpath, Jon Timmis, Frank Veenstra, Mostafa Wahby, Aleš Zamuda. Hybrid societies: challenges and perspectives in the design of collective behavior in self-organizing systems.** In Frontiers in Robotics and AI, Vol.3, No.14, 2016. This article analyzes and opens up perspectives for the design of hybrid societies, discussing formalization and engineering aspects together with interdisciplinary approaches to the design of self-organizing bio-hybrid and socio-technical systems.



4.6 Communication and Information Theory (Cain)

Head of research group: Prof. Dr. Ulrich Sorger

The Cain group is a small research group both in the ILIAS, and the ComSys laboratories. It is a part of the SECAN-Lab, too. There are frequent collaborations and exchanges with researchers from other groups like Bouvry's Parallel Computing and Optimisation Group (PCOG), Engel's Security and Networking

Lab (SECAN-Lab), or Biryukov's cryptology research group (CryptoLUX). The group is currently composed of three people; besides the head there is Christian Franck who joined in 2015 as a research scientist and Andrea Capponi who joined in 2016 as a PhD candidate. Our plan is to further grow the group by one or two additional PhD students. The core expertise of the group are mathematical principles behind the efficient encoding of information and the realisation of reliable error-free digital communication systems.

Main publications and achievements in 2016

- A. Capponi, C. Fiandrino, C. Franck et al., "Performance of Internet of Things-based Mobile Crowdsensing Systems for Sensing as a Service Applications in Smart Cities", 8th IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2016
- C. Franck, U. Sorger, "Some Properties of Homogenous Trellis-Constrained Codes", 9th International Symposium on Turbo Codes & Iterative Information Processing (ISTC), 2016
- C. Franck, U. Sorger, "Untraceable VoIP Communication based on DC-nets", E-print/Working paper, 2016

4.7 Critical and Extreme Security and Dependability (CritiX)

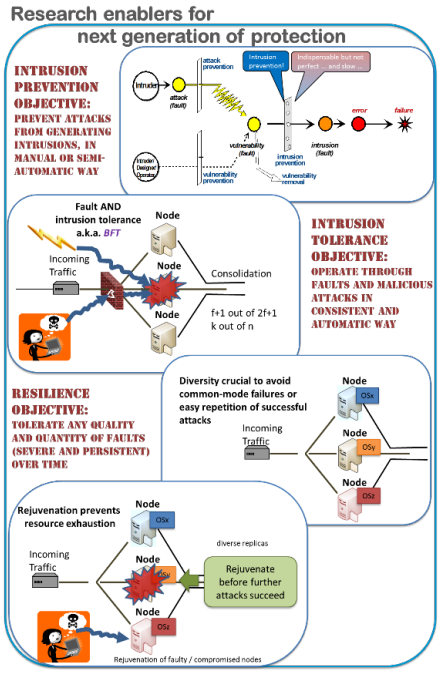
Head of research group: Prof. Dr. Paulo Esteves-Veríssimo

The CritiX lab (https://wwwen.uni.lu/snt/research/critix) was set up in September 2014 at SnT, and the bulk of the group started their activities in Q3 of 2015. The group intends to investigate and develop paradigms and techniques for defeating extreme adversary power (severe and continued threats) and sustaining perpetual and unattended operation (in a systematic and automatic way) and focusses on four scientific priorities: Resilience of cyber-physical system infrastructures and control; Internet and cloud infrastructures resilience; Security and dependability of embedded components; Data privacy and integrity in highly sensitive sectors.

Summary of the group's achievements in 2016

The team aims to discover and publish state-of-the-art advances in: - Ultra-resilient minimal roots-of-trust and enclaves; - Innovative, hybridisation-aware distributed algorithms, models, and architectures; - High-confidence vertical verification of mid-sized software; - Privacy- and integrity-preserving decentralised data processing. To support proof-of-concept prototyping of its discoveries, the group has set up a Private Cloud and a CPS (cyber-physical systems)

laboratory.
The increase in manpower was substantial, from 3 to 6 Research Associates. The CritiX research group managed to get in contact with several companies whose interests match with the research topics of CritiX. One of them being in progress with a positive outlook. A collaboration with LCSB (in cooperation with the SnT APSIA group) continues informally, having good perspectives. Prof. Paulo Esteves-Veríssimo (PJV) participated as lecturer in the PaRIS teaching initiative and hold a course at the MICS Master program in the fall 2016 semester at University of Luxembourg.



Members of the group were involved in several events, some selected are: IFIP WG10.4 Workshop in Aspen-US; participation as a UL element, to the ERC Starting Grants panel; Grande Region Sec. & Reliab. Day workshop; keynote on Cyberdefence at Military Academy International Symposium, Lisbon-PT; Cybersecurity ”Made in Lux”, REPER Lux, Brussels-BE, with the presence of Rectorate team elements; keynote European Cybersecurity Conference, Lisbon-PT; DSN conference as vice-chair of steering committee, Toulouse-FR; IFIP WG10.4 Workshop in Sorèze-FR; ESORICS conference, Iraklion-GR; address to Brazilian academia, military and information agencies, government and MPs, in the context of advisory to the Brazilian government on cybersecurity and cyberdefense, Brasilia-BR; invited to participate to the (closed) 2nd NATO Cyber Defence Smart Defence Projects Conference, Oeiras-PT; ACM CCS conference, Vienna-AU; keynote at Dagstuhl Seminar on Network Attack Detection and Defense, Dagstuhl-DE; organiser of the 1st CERTS@RTSS, Workshop on Security and Dependability in Critical Embedded Real-time Systems, run very successfully, Porto-PT. PJV was pivot of the participation of UL as founding member of the recent EU ECSO cPPP in cybersecurity.

Main publications and achievements in 2016

- Internet and cloud infrastructures resilience: identifying and addressing the main threat vectors to SDN. During the year of 2016, the high impact SDN survey published in January 2015, ramped-up from 160 to over 600 citations (GSC), placing the CritiX team at the center of international SDN expertise
- Resilience of Cyber-Physical System Infrastructures and Control: Paper on autonomous and cooperating vehicles threat plane and safety-security gap published in a workshop of the top-level ACM CCS conference.
- Security and Dependability of Embedded Components: Ongoing project on

a reference architecture based on many-cores and SoC and Paper on fixing vulnerabilities of Intel SGX's enclaves was published at SysTex.
- Using the Coq theorem prover, we have verified the correctness of the core of the KeYmaera X theorem prover for hybrid systems. Joint work with two colleagues from CMU, led to a publication at CPP 2017.

4.8 Critical Real-Time Embedded Systems (CRTES)

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

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

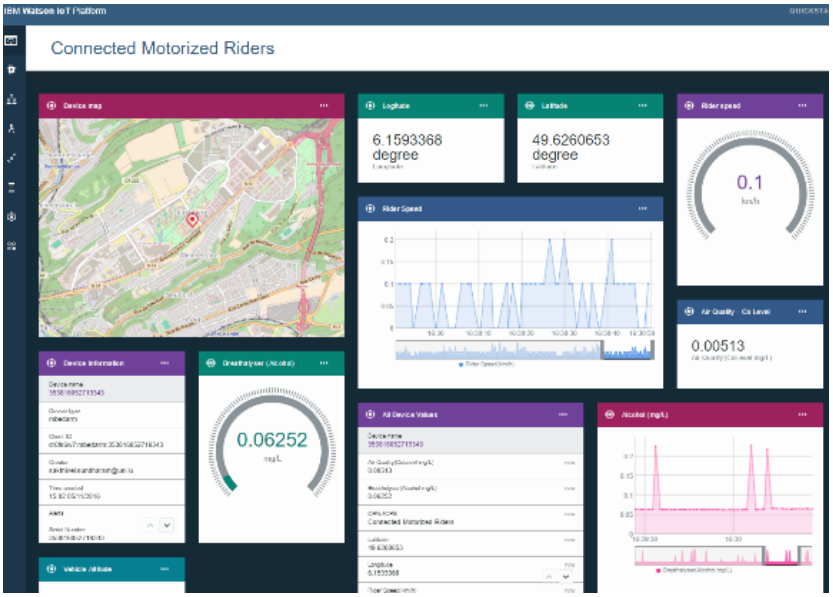
Summary of the group's achievements in 2016

The CRTES group was made up of 4 members (1 associate-professor, 1 post-doc, 2 PhD students) with 15 publications in 2016. Most of the work of the group was in the field of Model-Driven Engineering (MDE) for Embedded Systems, with the continued development of the CPAL (Cyber-Physical Action Language) design flow, especially towards fully automating the system configuration and synthesis steps. Several applications were also developed such as a safety add-on component for UAVs in collaboration with two companies, an Autosar-compliant automotive function and an IOT-based smart mobility system. The project "Eye-in-the-sky", involving a CRTES member, investigates the use of UAVs to monitor air pollutant levels in real-time and won the "Best Engineering Project" at the Morpheus Cup during ICT Spring 2016 in Luxembourg. Results were also obtained in the field of timing analysis, especially in timing analysis for automotive and avionics systems and their seamless integration in a MDE flow. Prof. Navet was in the defense board of 4 Phd thesis and 2 habilitation thesis, in the TPC of several international conferences, and has been involved in the CSC teaching programs especially as the course director of the professional Bachelor in Computer Science.

Main publications and achievements in 2016

- **N. Navet, Timing Analysis of Automotive Architectures and Software.** In this invited talk at the 19th Design, Automation and Test in Europe Conference (DATE 2016), we review the main timing verification techniques that are used in the design of automotive embedded systems and discuss what we can expect from them and what their limitations are. We then emphasize the need to question the models and their assumptions, and cross-validate their results. Finally, we discuss the prerequisites for a safe use of timing-accurate simulation as verification technique and illustrate on case studies from the automotive domains.

- **S. Altmeyer, N. Navet, Towards a declarative modeling and execution framework for real-time systems.** In ACM SIGBED Review, vol 13, n°2, pp30-33, 2016. In the programming model proposed in this article, the developer states the permissible timing behavior of the system, then, a system synthesis step involving both analysis and optimization generates a scheduling solution, which is enforced at run-time by the execution environment. With respect to the synchronous programming models, our approach implements a weaker version of time-determinism, still providing a form of timing-predictability sufficient in many applications while remaining closer to mainstay software development practices.
- **S. M. Sundharam, S. Altmeyer, L. Havet, N. Navet, Connected Motorized Riders - A Smart Mobility System to Connect Two and Three-Wheelers.** Runner up at the "Grand Challenge: Smart Embedded Applications and IoT" 2016 organised at the IIT Patna, India. This IoT-based smart mobility system for two and three-wheelers helps manage traffic congestions, improve air quality and identify traffic violations such as overspeeding behaviors. The system supports GSM and IoT network connectivity, with IBM Watson IoT platform as cloud backend, and was tested in Luxembourg and India.



4.9 CryptoLux team

Head of research group: Prof. Dr. Alex Biryukov

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

Summary of the group's achievements in 2016

In 2016 the CryptoLux group consisted of 10 members (1 professor, 1 senior researcher, 2 postdocs, 5 PhD students, and 1 technical assistant), who published a total of 15 papers in major international journals and conference proceedings. The group successfully completed the FNR CORE project ACRYPT (Applied Cryptography for the Internet of Things) and got an UL-internal research project on future directions in symmetric cryptography approved for funding. In addition, members of the group were active in the ongoing research project CAESAREA (funded by UL) and the AFR Ph.D. project EAC (funded by FNR). Research highlights in 2016 include the introduction of the concept of Egalitarian Computing, the presentation of the proof-of-work function Equihash (which is used for block mining in the Zcash crypto currency), the reverse-engineering of Sboxes, the design and implementation of the lightweight block cipher SPARX, and standardization activities related to the Argon2 password hashing function. Professor Biryukov and other members of the group served on the technical program committee of numerous conferences including CRYPTO 2016, the annual flagship conference of the IACR, as well as top security conferences ACM CCS and NDSS. CryptoLux members taught various courses in the MICS bachelor and master program and supervised student projects and theses. The team participated in scientific outreach activities at Researchers' Days 2016 presenting a workshop on applied cryptography for kids and their parents, as well as a workshop at Bee-creative. Last but not least, Aleksei Udovenko and his team won the hack.lu Capture the Flag (CTF) competition and made it into the final stage of the DEFCON CTF.

Main publications and achievements in 2016

- **Alex Biryukov, Dmitry Khovratovich, Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem. Network and Distributed System Security Symposium (NDSS), pp.1-13, 2016.** Proof-of-work (PoW) is a central concept in modern cryptocurrencies and denial-of-service protection tools, but the requirement for fast verification so far has made it an easy prey for GPU-, ASIC-, and botnet-equipped users. In this paper we solve this open problem and show how to construct an asymmetric proof-of-work based on a computationally-hard problem which is memory-hard to compute but is easy to verify.
- **Daniel Dinu, Leo Perrin, Aleksei Udovenko, Vesselin Velichkov, Johann Großschädl, Alex Biryukov, Design Strategies for ARX with Provable Bounds: Sparx and LAX, Advances in Cryptology–ASIACRYPT , pp. 484-513, 2016.** In this paper we present, for the first time, a general strategy for designing ARX symmetric-key primitives with provable resistance against single-trail differential and linear cryptanalysis. This has been a long standing open problem in the area of ARX design.
- **Alex Biryukov, Leo Perrin, Aleksei Udovenko: The Secret Structure of the S-Box of Streebog, Kuznechik and Stribob, EUROCRYPT, pp.226-247, 2016.** In this paper we analyse the S-box used by Russian encryption standards. This transformation is only specified as a look up table and the reason behind

its choice is unknown. We managed to reverse-engineer this S-Box and describe its unpublished structure. Our decomposition allows a more efficient hardware implementation but the choice of the components is puzzling a perspective.

4.10 Foundations of Model-Driven Engineering (FMDE)

Head of research group: Prof. Dr. Pierre Kelsen

FMDE is a small research group: besides the head (Pierre Kelsen) it comprised 3 members in 2016: Qin Ma (research scientist, half-time), Loïc Gammaitoni (PhD student) and Christian Glodt (research associate). The research group explores fundamental questions in the area of model-driven engineering but also explores concrete applications (e.g., enterprise architecture and robotics).

Summary of the group's achievements in 2016

Besides working with other group members on the validation of compound model transformations, Qin Ma collaborated with colleagues from LIST and University of Duisburg-Essen in the field of enterprise architecture, decision making support, and conceptual modeling, resulting in one publication.

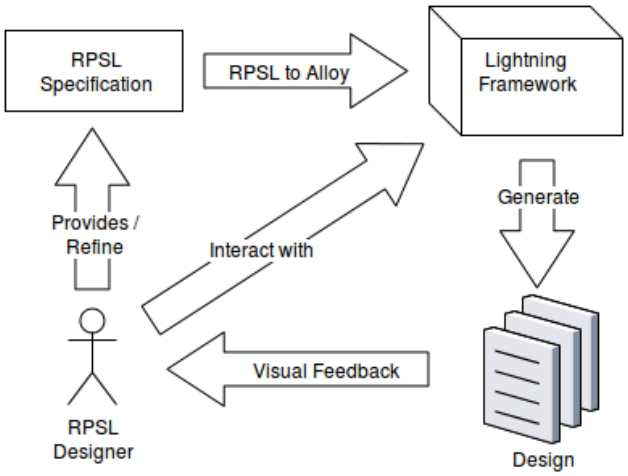
Loïc Gammaitoni started an interdisciplinary collaboration with a PhD student in the Engineering Research unit. This resulted in a successful application of the Lightning tool in the field of robotics, as documented by a SIMPAR publication.

Christian Glodt adapted the CSC Information Management System to provide most of the data for the self-assessment report required by the research evaluation. He also performed major work on "Accord", the successor of the CSC Information System, which is to be used on a faculty-wide scale.

Main publications and achievements in 2016

- *L. Gammaitoni, P. Kelsen, and Q. Ma. "Agile Validation of Higher Order Transformations Using F-Alloy". In: Agile Validation of Higher Order Transformations Using F-Alloy. 2016.* We describe the extension of the formal model transformation language F-Alloy to support the efficient validation of compound model transformations.
- *L. Gammaitoni and N. Hochgeschwender. "RPSL meets lightning: A model-based approach to design space exploration of robot perception systems". In IEEE International Conference on Simulation, Modeling, and Programming for Autonomous Robots. 2016.* This interdisciplinary work uses the Lightning language workbench in design space exploration in the context of robotic systems engineering.
- *Q. Ma and S. de Kinderen. "Goal-Based Decision Making Using Goal- Oriented Problem Structuring and Evaluation Visualization for Multi Criteria Decision*

Analysis". In: Lecture Notes in Computer Science (LNCS) 9619. 2016. We propose the Goal-based Decision Making (GDM) framework for providing decision as well as computational support for the GDM framework using tool chaining.



4.11 Individual and Collective Reasoning (ICR)

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

The ICR group is one of the pillars of the Interdisciplinary Lab for Intelligent and Adaptive Systems (ILIAS). In addition to its involvement in the SnT, it has established interdisciplinary links with the C^{2}DH, the FDEF (Law) and the FLSHASE (Institute for Cognitive Science and Assessment), but also collaborates with LIST. Areas of research are normative reasoning in multi-agent contexts (deontic logics, logics for security, compliance, machine ethics), legal knowledge representation and reasoning, logic-based models for intelligent agents / robots, computational argumentation and defeasible reasoning with uncertain/inconsistent information.

Summary of the group's achievements in 2016

In 2016, ICR hosted 20 researchers (1 professor, 1 visiting and 1 guest professor, 1 senior researcher, 6 postdocs and 10 PhD students), and produced 44 publications (32 in Orbilu for now). This year saw multiple activities of MIREL (Mining and Reasoning with Legal Texts), a H2020 MC RISE network with an overall volume of more than 1 Mio Euro, which is also coordinated by Prof. L. van der Torre.

ICR continued its development of the CSC Robolab by hiring a postdoc, Dr. F. Lera. He cooperates among others with LuxAI, a spinoff company founded

by Dr. P. Ziafati, a former ICR PhD student, in the context of an FNR proof-of-concept project (robotics for autistic children).

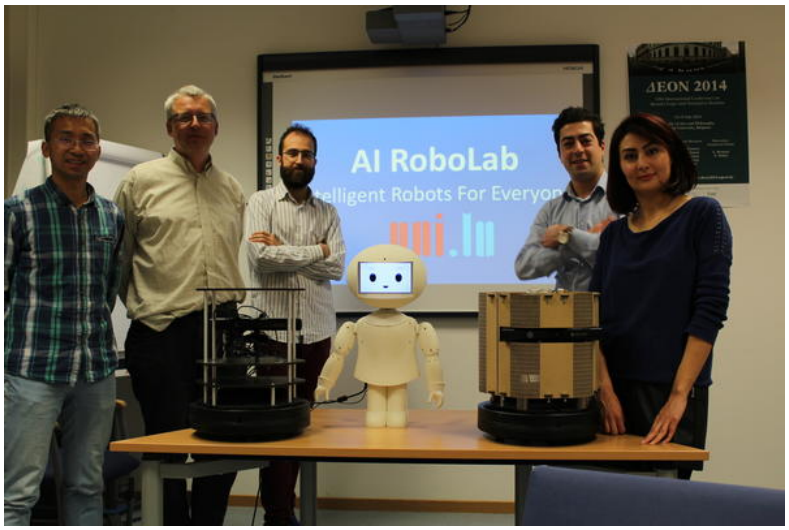
ICR continued to develop its links with China by hosting Prof. B. Liao (Zhejiang University), a visiting professor who spends 3 months/year in Luxembourg (FNR Mobility). The fruitful longterm collaboration with our highly productive guest professor D. Gabbay (King's College, Bar-Illan University) continued also in 2016 and has also allowed to bring forward handbook projects and innovative forms of teaching.

In addition to courses offered in the MICS, BINFO, and the Doctoral School of Computer Science, ICR is also a major player in the ERASMUS+ network LAST-JD (Joint International Doctoral Degree in Law, Science, and Technology), which each year involves 9-month visits of several PhD students in Luxembourg. ICR is furthermore part of the starting interdisciplinary Doctoral Training Unit "Digital History and Hermeneutics". Together with theoretical and empirical (with cognitive neuroscience) work on formal models for real-world argumentation (INTER CAFA), this reinforces our interdisciplinary profile.

Last but not least, Xin Sun, Llio Humphreys, Alessio Antonini and Mizanur Rahman successfully finished their PhD studies in 2016.

Main publications and achievements in 2016

- **Guido Boella, Luigi Di Caro, Llio Humphreys, Livio Robaldo, Piercarlo Rossi, Leon van der Torre.** *Eunomos, a legal document and knowledge management system for the Web to provide relevant, reliable and up-to-date information on the law.* Artificial Intelligence Law 24(3): 245-283 (2016).
- **Diego Agustın Ambrossio, Xavier Parent, Leon van der Torre.** *Cumulative aggregation.* In "Deontic Logic and Normative Systems. Proceedings of the13th International Conference, DEON'2016, Bayreuth, Germany (pp. 1-15), College Publications 2016". There are two ways to aggregate conditional obligations, simple and cumulative aggregation. The paper proposes two corresponding logical systems with factual detachment and prove representation results for both. We investigate the relation between these systems and input/output logics recently introduced by Parent and van der Torre.
- **Marc van Zee, Dragan Doder.** *AGM-style revision of beliefs and intentions.* In Proceedings of the 22nd European Conference on Artificial Intelligence (ECAI'2016) (pp. 1511-1519)". A logic for temporal beliefs and intentions based on Shoham's database perspective is introduced. It distinguishes strong beliefs (independent from intentions) and weak beliefs (resulting from adding intentions). The paper formulates AGM-style postulates for the revision of beliefs and intentions, ensuring that strong beliefs stay coherent with the intentions, and proves a corresponding representation theorem.



4.12 Information Mining and Learning (MINE)

Head of research group: Prof. Dr. Christoph Schommer

The *MINE* group is part of the ILIAS research laboratory; it follows a strongly *interdisciplinary* mission, for example, with the *C²DH* and with researchers of other disciplines. *MINE* is a small group of 3-5 members only, whose research interest focuses on the *data life cycle* (see Figure) and, in particular, on disciplines like *Natural Language Processing* and *Text Analytics, Data Science and Data Mining*, and *Artificial Companions*. Besides, a central focus lies in the education of students on all levels and on common education, for example with the Dept of Mathematics. For more detailed information: http://wiki.uni.lu/mine

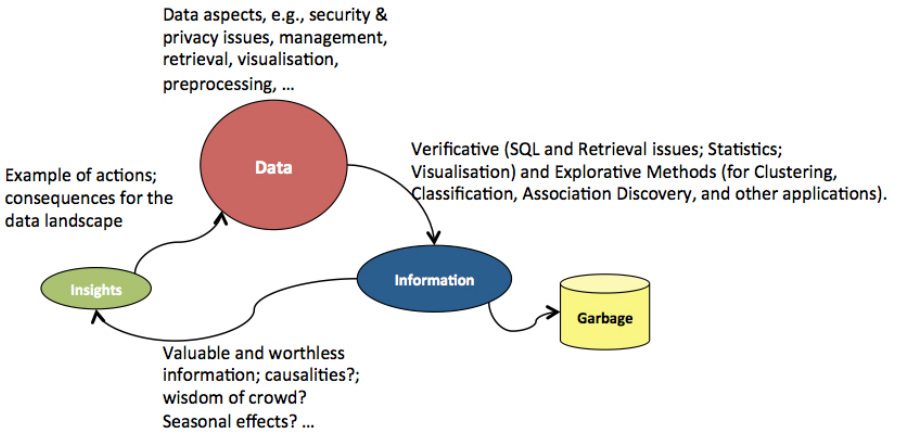
Summary of the group's achievements in 2016

Although a caesura with regards to staff happened, the year of 2016 has been *MINE's most successful one* since its foundation in 2003: first, *MINE* has become a member of the Doctoral Training Unit (PRIDE) « *Digital History and Hermeneutics* ». Prof Schommer has been elected as a DHH Management Board Member in order to work on the link between *History* and *Computer Science*. Furthermore, MINE has got accepted an internal, but interdisciplinary, project called *STRIPS*. This is a common project with the linguist Prof Peter Gilles and RTL Luxembourg ; it aims at realizing a semantic search on Luxembourgish texts to detect and to monitor patterns like emotions, topics, or sentiments over time. In addition, Prof Schommer and Winfried Höhn organised an international workshop on *Exploring Old Maps,* together with colleagues from the University of Würzburg, Germany. Prof Schommer and Sviatlana Höhn organised a *Workshop on Machine Translation for the Public Sector, which*

was supported by the members of the European Commission. Likewise, Prof Schommer contributed to the *Pain and Suffering* project (lead by Prof Anton and Dr. Bustan from the Psychophysiology and Neurophysiology Laboratory of the University of Luxembourg). Also, Prof Schommer had been invited to give a course « Data Science » at the *IIIS institute of the Tsinghua University*, Bejing, China. In 2016, Prof Schommer had been Invited Program Committee member of 12 conferences, for example the 39th *Conference on Cognitive Science* (*CogSci*), the *European Conference on Machine Learning* (*ECML-PKDD*), *Digital Humanities*, or *30th IEEE Conference on Computer-based Medical Systems* (CBMS). Importantly, Prof Schommer guided the following PhD students, either as supervisor, co-supervisor, or external expert : Dr. Alessio Antonini (external expert and member of the defence committee ; Departimenta di Informatica, Università di Torino), Dr. Florian Feltes (Internal Expert and co-Chairman of the Defence Committee; Dept of Economics, Luxembourg), Dr. Martin Sewell (external expert, UC London, UK), Dr. Llio Humphreys (co-Supervisor and Chairman of Defense), Dr. Andreas (co-Supervisor, with Dept of Finance), Dr. Dimitrios Kampas (Supervisor), and Dr. Sviatlana Höhn (Supervisor).

Main publications and achievements in 2016

- Bustan, S., Gonzalez-Roldan, A. M., Schommer, C., Kamping, S., Loeffler, M., Brunner, M., Flor, H., Anton, F.: « Facteurs psychologiques, cognitifs et les influences contextuelles dans la douleur et la souffrance liée à la douleur. » 16e congrès national de la société française d'étude et de traitement de la douleur (SFETD), Bordeaux, France.
- Höhn, W., Schommer, C.: « Annotating and Geo-referencing of Digitized Early Maps ». Digital Humanities, Krakau, Poland.
- Dr. Sviatlana Höhn: « Data-driven repair models for text chat with language learners ». PhD Thesis.
- Dr. Dimitrios Kampas: « Topic Identification considering word order in Markov Chains ». PhD Thesis.



4.13 Methods and Tools for Scientific Requirements Engineering (MESSIR)

Head of research group: Prof. Dr. Nicolas Guelfi

The MESSIR group is part of the LASSY laboratory. It focuses on introducing model driven engineering approaches for requirements analysis. From a more global perspective the MESSIR group addresses also experimental research in software engineering education in a global context.

Summary of the group's achievements in 2016

In 2016, the group has made available to the community as the result of an open source project its requirements analysis method called MESSIR and its supporting open source tool (called Excalibur). They have been deployed in the context of research and teaching collaboration at Peter the Great St.Petersburg Polytechnic University. After this validation phase, scientific publications will present the first results and are planned for the 2017-2020 period.

First results in experimental research in software engineering education in a global context have been conducted and published which represent the first steps in the development of this research axis by the group.

The group members are also acting as experts for the court of justice of Luxembourg in trials for which software engineering expertise are required. An important expertise has been conducted partly in 2016 for the court for which we were requested to answer to a conformance question on a precise case.

Main publications and achievements in 2016

- **Guelfi, Nicolas, Benjamin Jahic, and Benoît Ries**. "TESMA: Towards the Development of a Tool for Specification, Management and Assessment of Teaching Programs." Proceeding of the 2nd International Conference on Applications in Information Technology. The University of Aizu Press, 2016. The tool and approach presented here are the basis of our next project on experimental research in software engineering education. It uses advanced techniques of MDE based on DSL and code generation techniques.
- **Guelfi, Nicolas, Alfredo Capozucca, and Benoît Ries**. "Measuring the SWEBOK Coverage: An Approach and a Tool", SWEBoK Evolution Town Hall, Engineering Disciplines Committee of the Professional & Educational Activities Board of the IEEE Computer Society. This paper presents an approach and a tool to measure the knowledge coverage with respect to a knowledge standard like the SWEBOK (Software Engineering Body Of Knowledge).
- In 2016, we have been invited professors at Peter the Great St.Petersburg Polytechnic University where we have run a bachelor and a master course on software engineering and development. We have also started collaboration on experimental research in software engineering education whose results will be partly published in 2017.

4.14 Parallel Computing and Optimisation Group (PCOG)

Head of research group: Prof. Dr. Pascal Bouvry

The Parallel Computing and Optimisation group conducts research on parallel computing and optimization techniques, in particular how different species may co-evolve taking local decisions while ensuring global objectives, to tackle large and difficult problems. The main application domains are security, trust and reliability; reliable scheduling and routing on new generations of networks; sustainable development and systems biomedicine. Detailed information about the group is available at http://pcog.uni.lu/.

Summary of the group's achievements in 2016

In 2016, the PCOG team counted 17 members (1 professor, 2 senior researchers, 6 postdocs, 8 PhD students) and produced a total of 28 publications (6 journal articles, 22 conference articles).

5 PhD students successfully defended their thesis in 2016. The group is also involved in the H2020 Erasmus+ LAST-JD "Joint International Doctoral Degree in Law, Science and Technology", with Prof. Bouvry co-supervising 2 PhD students. The group successfully completed the Green@Cloud project (FNR CORE) and two EU COST actions (Nesus and Chipset). In addition, the PCOG runs the IShoP (Internet Shopping Optimisation) project together with Poznan University of Technology (FNR Pollux) and participates to ASIMUT (Aid to SItuation Management based on MUtlmodal, MultiUAVs, Multi-level acquisition Techniques), first European Defense Agency (EDA) project accepted in Luxembourg. Two best paper awards were obtained in 2016, one at IEEE Cloudnet 2016 from IEEE Communication Society to Andrea Sciarrone, Claudio Fiandrino, Igor Bisio, Fabio Lavagetto, Dzmitry Kliazovich and Pascal Bouvry *"Smart Probabilistic Fingerprinting for Indoor Localization over Fog Computing Platforms"*, and one to Lin Wang, Lei Jiao, Dzmitry Kliazovich and Pascal Bouvry "Reconciling Task Assignment and Scheduling in Mobile Edge" at the conference HotPNS 2016. PCOG team members taught in several Bachelor and Master programs (BINFO, Bachelor en Sciences de la Vie, MICS, Professional Master in Entrepreneurship). In addition, 2016 was marked by the first promotion of the professional certificate on Smart ICT for business innovation directed by Prof. Pascal Bouvry, and conducted in collaboration with the ILNAS.

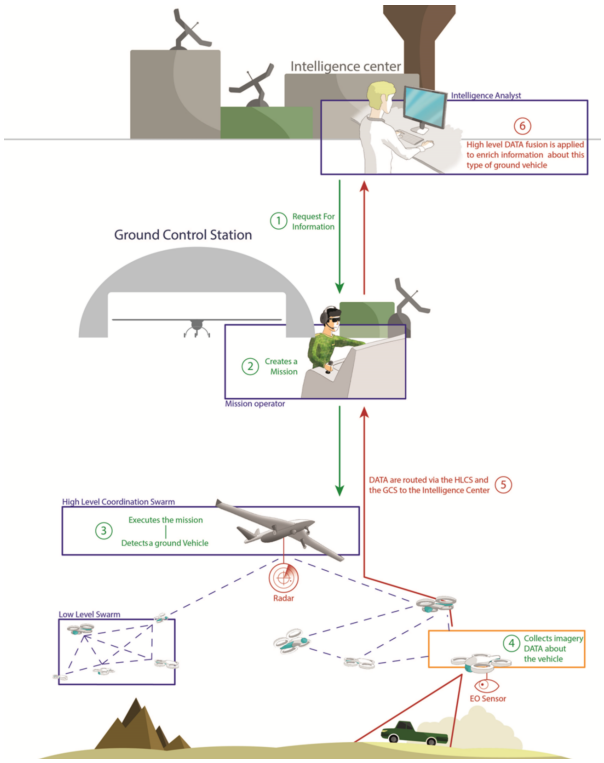
PCOG is also strongly involved in the management of the High-Performance Computing (HPC) of the University, Prof. Pascal Bouvry being "Chargé de Mission auprès du Recteur" in charge of the University HPC.

Main publications and achievements in 2016

- IEEE CloudCom 2016 - General Chairs: Prof. Bouvry and Dr. Varrette - http://2016.cloudcom.org. The 8th IEEE International Conference on Cloud Comput-

ing Technology and Science was held from December 12 to 15 in Luxembourg, attracted 170 top scientists from all over the world and positioned Luxembourg as a center of excellence in the field of Cloud Computing becoming a significant milestone for research in Luxembourg.

- The High-Performance Computing platform of the UL. Managed by Prof. Bouvry, it is currently the largest facility of this type in Luxembourg (after GoodYear's industrial R&D Center). As of January 2016, the HPC platform featured a computational power of 87 TFlops (5316 computing cores) and 5.1 PBytes for storage (incl. 1.7 PB for backups), serving 335 users. In terms of cumulative hardware investments since 2007 (excluding server rooms costs), the UL HPC has reached a total of 5.244 M€.
- ASIMUT Project – https://asimut.gforge.uni.lu/. The ASIMUT project is conducted in collaboration with Thales (France), University of Bordeaux (France), Fraunhofer IOSB (Germany) and Fly-n-Sense (SME, France). The PCOG team developed novel mobility models for multi-level UAV swarms based on nature-inspired techniques, i.e. ant colony optimisation (ACO) and chaos theory. This contribution was integrated in the ASIMUT demonstration framework and successfully evaluated via state-of-the-art simulations. A video of the evaluation session is available here: https://asimut.gforge.uni.lu/_downloads/asimut.mp4. ASIMUT also resulted in three publications in international conferences 2016 : ACM DRONET'16, IEEE MFI'16 and ACM DIVANET '16.



4.15 Proactive Computing

Head of research group: Prof. Dr. Denis Zampuniéris

This small group, counting 4 members (1 professor, 2 PhD students, 1 technical assistant) is part of the LASSY research laboratory. It focuses on formalizing and implementing proactive computing principles into the development of innovative, pervasive and/or autonomic software systems for several real-world application fields. The proactive computing paradigm provides us with a new way to make the multitude of computing systems, devices and sensors spread through our modern environment, work for/pro the human beings and be active on our behalf.

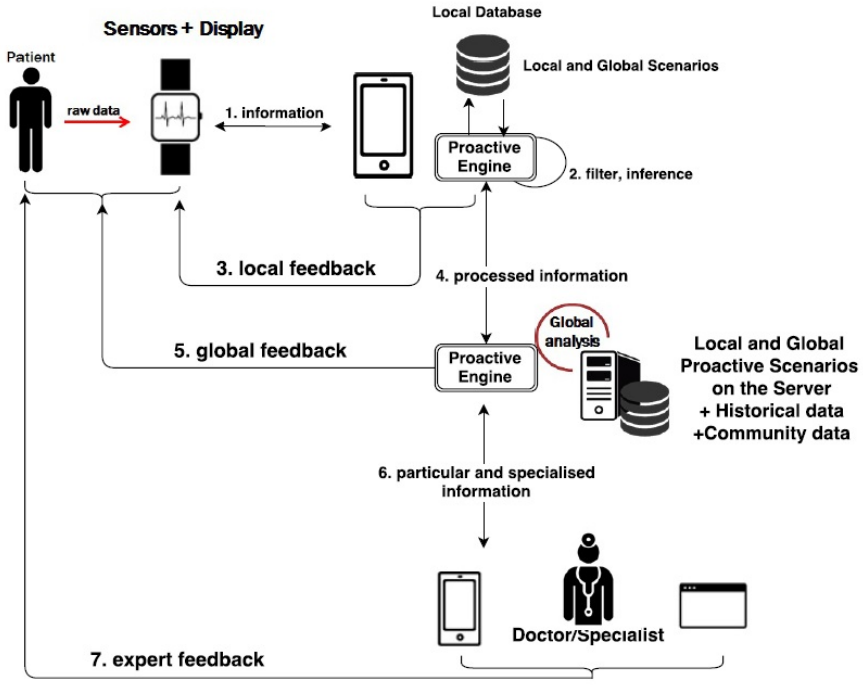
Summary of the group's achievements in 2016

Apart from their regular research and publication work and their participation in teaching programmes offered by our Faculty, the group members welcomed and supervised several students (local or from universities abroad) in internship for their Bachelor or Master thesis. In December 2016, the PhD student Remus Dobrican successfully defended his thesis with the grade "outstanding".

Main publications and achievements in 2016

- **Remus Dobrican and Denis Zampuniéris. A Proactive Solution, using Wearable and Mobile Applications, for Closing the Gap between the Rehabilitation Team and Cardiac Patients.** In Proc. IEEE International Conference on Healthcare Informatics (ICHI), pp. 146-155, Chicago (USA), 2016. The aim of this work is to implement a proactive e-Health system that will allow patients, following a Cardiac Rehabilitation (CR) program outside the hospital, to exercise safely, according to their recommended training zones. The CR e-Health system includes a smartwatch application, a smartphone application and several server-side applications, working on predefined but personalised proactive scenarios which are alerting, guiding and supporting the patients. While training, patients benefit from multiple levels of feedback. Communities of patients are created for stimulating and motivating patients to perform according to their CR programs. Opposed to traditional home-based CR e-Health applications, patient profiles and training zones are created and handled dynamically by the system for each individual patient.
- **Remus Dobrican, Gilles Neyens and Denis Zampuniéris. A Context-Aware Collaborative Mobile Application for Silencing the Smartphone during Meetings or Important Events.** In International Journal on Advances in Intelligent Systems, 9(1&2), pp. 171-180, 2016. This study describes a mobile application that uses group-driven collaboration and location-based collaboration for automatically switching smartphones into silent mode during meetings or important events. More precisely, for the first step of the collaboration, a partial agreement algorithm will be used for establishing if a meeting is confirmed by its participants and, for the second round, confirming if the meeting will take place, based on the location of the participants. The application uses

a new technique for exchanging information, for coordinating and for making decisions in a distributed way, called Global Proactive Scenarios (GPaS). For executing these GPaS, a rule-based middleware architecture for mobile devices has been developed which allows developers to define the possible actions of their applications in a structured way without having to take care of the communication and coordination of the mobile devices. Also, there is no need for developing a server-side application: the full logic is integrated into the GPaS.



”Architecture of our Proactive e-Health System with multiple levels of monitoring, expertise and feedback.”

4.16 Security and Networking Lab (SECAN-Lab)

Head of group: Prof. Dr. Thomas Engel

SECAN-Lab addresses both fundamental and applied research in computer networking and security, namely in the areas of privacy by distribution, network and system security, SCADA and cyber security, IoT, and vehicular communication and multimodal traffic management.

2016 achievements

SECAN-Lab successfully completed 11 of its 31 projects and had 7 new projects approved for funding, of which 6 began in 2016 and focused on the group's core areas, including security and privacy in data communication, vehicular communication for traffic management, and IoT. SECAN-Lab was involved in various international scientific conferences (published 36 papers), including IETF annual meeting and IPv6 World Congress, in addition to receiving several awards. Stefanie Östlund won Best Partner Award for her contribution on the ethical and legal issues in the project FETCH. Luca Lamorte and Maria Rita Palattella received the 2016 Google IoT Technology Research Award for their work on the SECAN-Lab F-Interop project which develops interoperability, conformance and performance test tools, running on a federation of European testbeds. Latif Ladid received the IPv6 Life Time Achievement Award for his achievements over the past 20 years in deploying IPv6 worldwide. Moreover, team members have taught extensively within the University of Luxembourg's BSc and MSc programs. The annual SECAN-Lab Dagstuhl retreat consolidated the group's activities in collaboration with external guests and partners. Finally, Lara Codeca, Susann Gottmann, Martin Kracheel and Nico Nachtigall successfully defended their PhD theses.

Main publications and achievements in 2016

- A. Panchenko, F. Lanze, A. Zinnen, M. Henze, J. Pennekamp, K. Wehrle, T. Engel. **Website Fingerprinting at Internet Scale.** *Proceedings of the 23rd Internet Society (ISOC) Network and Distributed System Security Symposium* (SDSS), San Diego, USA. The website fingerprinting attach aims to identify the content of encrypted and anonymized connections by observing patterns of data flows such as packet size and direction. This attach can be performed by a local passive eavesdropper – one of the weakest adversaries in the attacker model of anonymization networks such as Tor. In this paper, we present a novel website fingerprinting attack that outperforms all state-of-the-art methods in terms of classification accuracy while being computationally dramatically more efficient. In order to evaluate the severity of the website fingerprinting attach in reality, we collected the more representative dataset where we avoid simplified assumptions made in the related work regarding selection and type of webpages and the size of the universe. Using this data, we explore the practical limits of website fingerprinting at Internet scale.
- R. Soua, E. Kalogeiton, G. Manzo, J. M. Duarte, M. R. Palattella, A. Di Maio, T. Braun, T. Engel, L. A.Villas, G. A. Rizzo, A. Giancula. **SDN coordination for CCN and FC content dissemination in VANETs.** *Proceedings of the 8th Internatinal Conference on Ad Hoc Networks (ADHOCNETS),* Ottawa, Canada. Content dissemination in vehicular Ad-hoc Networks has a myriad of applications, ranging from advertising and parking notifications, to traffic and emergency warnings. This heterogeneity requires optimizing content storing, retrieval and forwarding among vehicles to deliver data with short latency and without jeopardizing network resources. In this paper, for a few reference scenarios, we illustrate how approaches that combine Content Centric Networking (CCN) and Floating Content (FC) enable new and efficient spolia-

tions this issue. Moreover, we describe how a network architecture based on Software Defined Networking (SDN) can support both CCN and FC by coordinating distributed caching strategies, by optimizing the packet forwarding process and the availability of floating data items. For each scenario analyzed, we highlight the main research challenges open, and we describe a few possible solutions.

- T. Dermann, R. Frank., S. Faye, G. Castignani, T. Engel. **Towards Privacy-Neutral Travel Time Estimation from Mobile Phone Signaling Data**. *Proceedings of the 2016 IEEE International Smart Cities Conference (IS2C)*. Today's mobile penetration rates enable cellular signaling data to be useful in diverse fields such as a transportation planning, the social sciences and epidemiology. Of particular interest for these applications are mobile subscriber dwell times. They express how long users stay in the service in range of a base station. In this paper, we want to evaluate whether dwell time distributions can serve as predictors for road travel times. To this end, we transform floating car data into synthetic dwell times that we use as weights in a graph-based model. The model predictions are evaluated using the floating car ground truth data. Additionally, we show a potential link between handover density and travel times. We conclude that dwell times are a promising predictor for travel times, and can serve as a valuable input for intelligent transportation systems.

4.17 Security and Trust of Software Systems (SaToSS)

Head of research group: Prof. Dr. Sjouke Mauw

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

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

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

Summary of the group's achievements in 2016

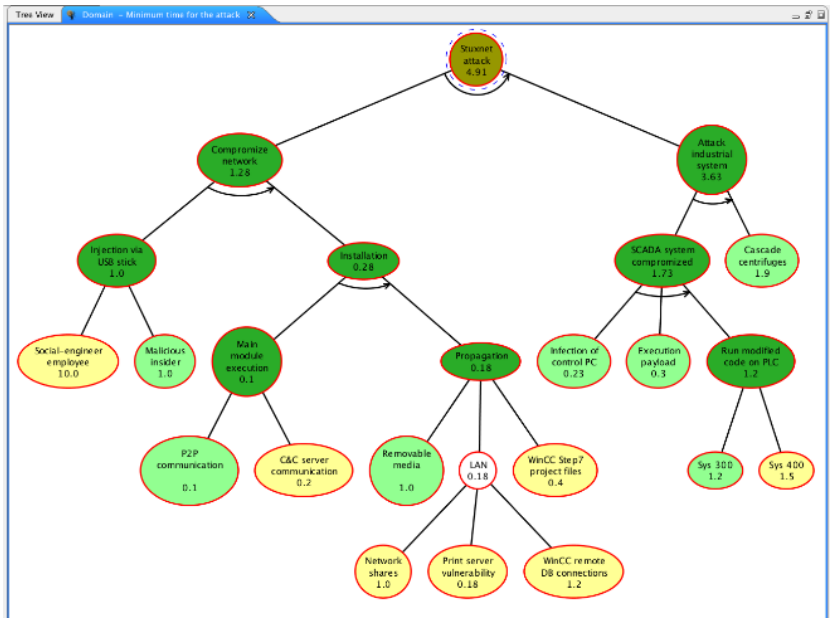
2016 was a very successful year for SaToSS. In 2016 the SaToSS group counted 17 researchers (1 professor, 1 senior researcher, 6 postdocs, 8 PhD students and 1 technical assistant), which is more than ever. Further, the group published 43 papers, which is the highest number of publications per year since its inception. Through its expertise in attack trees, the SaToSS group was involved in FP7 project TREsPASS that successfully finished in 2016 and in the Singaporean project Securify). Further we are running one FNR-funded CORE project (ADT2P on attack trees), two Junior CORE projects (COMMA on malware analysis and DIST on distance-bounding protocols), and one UL-funded project (SEC-PBN on computational modelling in biology). Various projects have been approved for funding in 2016. Most important is the FNR-PRIDE project SPsquared which funds 12 PhD students for a new interdisciplinary Doctoral Training Unit in Security and Privacy (PI Prof. Mauw, involving 11 other researchers from our university). Two more projects have been approved in 2016: AFR project DroidMod (security of Android apps) and FNR-INTER project AlgoReCell (models of biological networks). SaToSS members were active in the organization of various international scientific events, including: IFIPTM 2016, GraMSec 2016, VTSA 2016. Our weekly security seminar SRM (together with the APSIA group of Prof. Peter Y A Ryan) was organized 32 times in 2016, featuring speakers from 13 different countries. Our group members were involved in teaching for the computer science bachelor (BINFO), the computer science master (MICS), the master in integrated systems biology (MISB) and the professional master in computer security (MSSI). Yang Zhang successfully defended his PhD thesis in 2016.

Main publications and achievements in 2016

- **Sjouke Mauw, Jorge Toro-Pozo, and Rolando Trujillo-Rasua. A class of pre-computation-based distance-bounding protocols.** In Proc. 1st IEEE European Symposium on Security and Privacy (EuroS&P'16), pages 97-111, 2016. Distance-bounding protocols are security protocols that guarantee an upper limit on the distance between two communicating parties. Such protocols are needed in e.g. smart card payments, to ensure that the card is in the vicinity

of the payment terminal and not being remotely exploited. In this paper we provide a unified analysis for a class of distance-bounding protocols and we define novel distance-bounding protocols with an excellent attack resistance in relation to the available memory.

- **Andrzej Mizera, Jun Pang, and Qixia Yuan. Fast simulation of probabilistic Boolean networks.** In Proc. 14th International Conference on Computational Methods in Systems Biology (CMSB'16), LNCS 9859, pp. 216-231. 2016. Computational methods play a key role in systems biology, aiming to model and analyse biological systems from a holistic perspective in order to provide a comprehensive, system-level understanding of cellular behaviour. This poses a significant challenge of developing efficient methods for studying large real-life biological systems. This paper presents a novel method to speed up the simulation of Probabilistic Boolean Networks (PBNs), a well-established framework for analysing gene regulatory networks. The mean idea is to reduce the network size by removing the unnecessary nodes and divide the remaining nodes into groups for parallel simulation. The proposed method results in a significant speed up (up to 50 times) for simulating PBNs, which enables the computation of steady-state probabilities for PBNs of thousands of nodes.
- **Olga Gadyatskaya, Ravi Jhawar, Piotr Kordy, Karim Lounis, Sjouke Mauw, and Rolando Trujillo-Rasua. Attack trees for practical security assessment: Ranking of attack scenarios with ADTool 2.0.** In Proc. 13th International Conference on Quantitative Evaluation of SysTems (QEST'16), LNCS 9826, pages 159-162, 2016. This paper marks the development of the second iteration of our very successful tool for attack tree design and analysis: ADTool 2.0. For an example see the figure.



4.18 Security, Reasoning and Validation (SerVal)

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

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

- Software Reliability
  - Software Testing (Mutation Testing, Search-Based Testing, ...)
  - Semi-Automated and Fully-Automated Program Repair
  - Models to improve software design and validation
  - IoT interoperability
- Data Analytics
  - Multi-objective reasoning and optimization
  - Model-driven data analytics (on top of Models@run.time)
  - Time Series Pattern Recognition
  - Information Retrieval and Data mining to collect knowledge
  - Predictive and Prescriptive techniques (Decision Support Services)
- Mobile Security
  - Malware detection, prevention and dissection
  - Static Analysis to check source code properties, including security
  - Vulnerability Detection

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, Fintech, Smart Grid and Smart Home infrastructures, and the latest paradigms of databases.

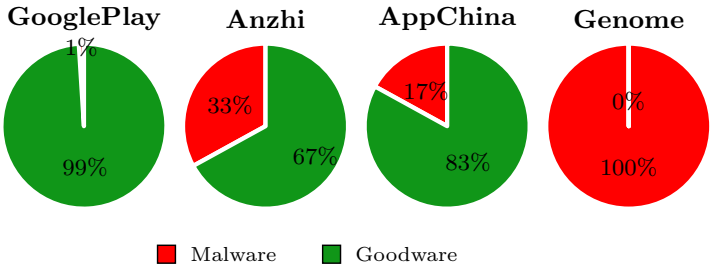
Summary of the group's achievements in 2016

2016 was a very fruitful year for Serval. The number of members increased to about 30 researchers. They published about 45 papers in top venues such as POPL, ICSE, Empirical Software Engineering, DIMVA, ISSTA, etc. They acquired two new FNR junior CORE projects, one AFR and one PhD position on the successful FNR-PRIDE project named SP^2. Prof. Le Traon acquired a mobility grant to visit UC Berkeley for about one year.

Main publications and achievements in 2016

- AndroZoo: Collecting Millions of Android Apps for the Research Community, Kevin Allix, Tegawendé F. Bissyande, Jacques Klein, Yves Le Traon, in Proceedings of the 13th International Workshop on Mining Software Repositories (2016, May) Short Summary: In this paper, we present a growing collection of Android Applications collected from several sources, including the official Google Play app market. Our dataset, AndroZoo, currently contains now

more than five million apps that we make available to the research community. Each app has been analysed by tens of different AntiVirus products to know which applications are detected as Malware. The following figure illustrates the share of malware in various datasets, where apps are considered as malware when they are flagged by at least 10 antivirus products.



- Comparing White-box and Black-box Test Prioritization, Christopher Henard, Mike Papadakis, Mark Harman, Yue Jia, Yves Le Traon, in 38th International Conference on Software Engineering (ICSE'16) (2016) Short Summary: Although white-box regression test prioritization has been well-studied, the more recently introduced black-box prioritization approaches have neither been compared against each other nor against more well-established white-box techniques. We present a comprehensive experimental comparison of several test prioritization techniques, including well-established white-box strategies and more recently introduced black-box approaches.
- DroidRA: Taming Reflection to Support Whole-Program Analysis of Android Apps, Li Li, Tegawendé F.Bissyande, Damien Octeau, Jacques Klein, in The 2016 International Symposium on Software Testing and Analysis (2016, July) Short Summary: Android developers heavily use reflection in their apps for legitimate reasons, but also significantly for hiding malicious actions. In this paper we propose the DroidRA instrumentation-based approach to address this issue in a non-invasive way. With DroidRA, we reduce the resolution of reflective calls to a composite constant propagation problem. We leverage the COAL solver to infer the values of reflection targets and app, and we eventually instrument this app to include the corresponding traditional Java call for each reflective call.

4.19 Systems and Control Engineering (SCE)

Head of research group: Prof. Dr. Jürgen Sachau

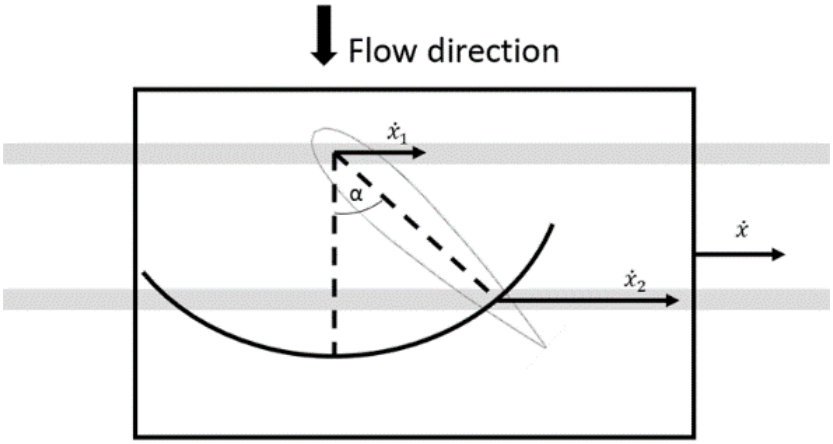
The Systems and Control Engineering group, led by Prof. Dr.-Ing. Jürgen Sachau is affiliated to the Computer Science and Communications research unit. It is also associated with the Electrical Engineering Institute of FSTC. The SnT group is devoted to systems and control technology development and demonstration of grid integration, conversion and storage and solar-fed structures for distributed energy systems. Detailed information about the group is available at http://sce.uni.lu/.

Summary of the group's achievements in 2016

In 2016 SCE, counted 4 members (1 professor, 2 PhD students, 1 technical assistant). The team published 4 publications during that year. The group also successfully completed the development of a hydrokinetic turbine prototype, based on the oscillating hydrofoil approach a turbine is built in Luxembourg and tested in a canal in Aachen at the RWTH Aachen University. Additionally, an energy economic analysis for the turbine prototype for Luxembourg was done for Luxembourg for different renewable energy scenarios. In addition, three custom-built inverter controllers with dedicated FPGA hardware control have been built in the laboratory. They have been extensively used in the experimental implementation of PhD Surena Neshvad's researchs on inverter broadband stimulation injedction, distrbuted generation adaptive protection and advanced state estimation. Surena Neshvad also successfully defended his PhD thesis in 2016.

Main publications and achievements in 2016

- **S. Neshvad, H. Margossian, J. Sachau, "Topology and Branch Parameter Estimation in Power Systems through Pseudo-Random Binary Stimulations", IET Generation, Transmission and Distribution.** This paper describes a method for identifying the system parameters associated with the power system model. In particular, the proposed algorithm addresses the topology identification task in the scope of state estimation. The goal is to reduce the a priori knowledge for state estimation, and to obtain information on the power system network. Broadband stimulation signals are injected at from several Distributed Generators (DGs) in the grid and their effects measured at other locations. It combines and correlates various measurements in order to obtain a reliable snapshot of the power network parameters.
- **H. Margossian, S. Neshvad, J. Sachau, "Adaptive Protection with Distribution Network Configuration and Distributed Generation Status Estimation", IEEE Transaction on Power Delivery.** This paper proposes a framework for adaptive feeder protection in distribution grids with a high amount of distributed generators (DGs) installed. The scheme adapts the feeder protection relay settings according to the changes in the connection status of those DGs that have a significant impact on the fault current. The core of the method consists in the identification of the connection status of the DGs using an iterative modified state estimation (SE) program. The approach is illustrated using a realistic 31-node distribution network model.
- **D. Norta , Development of an Oscillating Foil Turbine**. D Norta has proposed an oscillating foil turbine concept with several advantages compared to ordinary oscillating foil and rotational turbines. It is applicable in rivers of a lower depth but with a width/depth ratio larger than one and has an at least 27% larger cross sectional extraction pane compared to the rotational turbines. The concept is designed with two degrees of freedom of the foils motion. Using those degrees of freedom it is possible to extract at any time of the motion of the foil at any flow velocity of the river the maximum power.



4.20 Team Leprévost

Head of reseach group: Prof. Dr. Franck Leprévost

Summary of the achievements in 2016

During most of 2016 Franck Leprévost was on sabbatical leave after 10 years as vice-president of the University of Luxembourg. He spent 3 months at the European Investment Bank/European Investment Fund in Luxembourg, and 8 months at the Peter the Great Saint Petersburg Polytechnic University in Russia. The aim of these stays was twofold: re-enter the active world of research, and capitalize on the leadership experience. Research has been conducted on the Elliptic Curve Discrete Logarithm Problem (one of the main mathematical problems underlying Public-Key Cryptology) over finite fields. Computations were conducted to identify and interpret in a innovative way coefficients of some p-adic expansions that are necessary to address the ECDLP under some conditions. This is a joint work between N. Bernard, P. Bouvry & F. Leprévost. A further direction was to pursue the long-term work on anonymity of communication. We already published a series of articles on this subject in the past years. Still we further developed a prototype aiming at non-observability of communication. Related publications are in the pipe. Another direction was to report to the community of academic leaders the experience of the University of Luxembourg, and its fast growing development. This lead to an article, that will appear as a chapter of a book. The experience gained in Russia on the 5-100 program, aiming 5 Russian universities in the top 100 in the world by 2020, will lead to either a long article or even to a book. Although most of the material was acquired during 2016, the outcome will only be realized in 2017 at the earliest.

Main publications and achievements in 2016

- "From the Sagrada Familia to the University of Luxembourg" (author: F. Leprévost). Accepted for publication. This article will be a chapter of a book edited by Phil Altbach and Jamil Salmi on "Accelerated Universities". The book itself will be published in 2017.
- "Computation around ECDLP over Fp" (authors: F. Leprévost, N. Bernard, P. Bouvry). Submitted.

Chapter 5

Organizational Structure

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

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

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

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

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

In addition to the labs, which organize resources and competencies with a long-term view, we foresee orthogonal structures, which may be called institutes, which allow us to react quickly in an agile way to funding opportunities, societal demands and technological hypes. Institutes are formed by a number of professors/postdocs/students, preferably representing various labs. Examples are: AI institute, FinTech institute, Machine Learning institute.

Chapter 6

Education

6.1 Doctoral Programme in Computer Science and Computer Engineering

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

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

6.2 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 in-

novation; 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).

6.3 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 six profiles:

- Adaptive Computing;
- Communication Systems;
- Information Security;
- Intelligent Systems;
- Network Systems;
- Reliable Software Systems.

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

In 2016 there were around 60 students from more than 25 countries in the MICS.

6.4 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.

Its 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 academicbackground (technical, managerial, legal...) required for security officers to face the challenges of nowadays security threats.

In 2016, the MSSI organized the Information Security Education Day (ISED). It is a yearly one-day event co-organized by University of Luxembourg and Luxembourg Institute of Science and Technology and sponsored by CLUSIL, CSC and SnT. ISED provides an ideal forum where academics and practitioners can learn about the different facets of a key-topic, exchange and discuss ideas, and compare experiences. In this spirit, ISED seeks to be an interdisciplinary event, open to all. The speakers have expertise in different areas covering the legal, technical and research-wise facets of the theme. 2016 theme was ”Security in the realm of Big Data & Analytics”.

6.5 Bachelor of Engineering in Computer Science (BINFO)

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

The main learning objectives of the BINFO are the following:

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

The required degree for application is the Luxembourg ”Diplôme de fin d’études secondaires” or ”secondaires techniques” or ”de technicien - division informatique” or a foreign equivalent recognised by the Ministry of National Education. More information at http://binfo.uni.lu.

Appendix A

Publication List

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

Publication Category	**Quantity**	**Section**
Book	7	A.1 (p.48)
Book Chapter	4	A.2 (p.49)
Journal	68	A.3 (p.49)
Thesis	19	A.4 (p.55)
Conference	184	A.5 (p.56)
Technical Report	10	A.6 (p.75)
Miscellaneous	20	A.7 (p.76)
Unpublished	24	A.8 (p.78)
Total	*336*	

Table A.1: Overview of publications per category

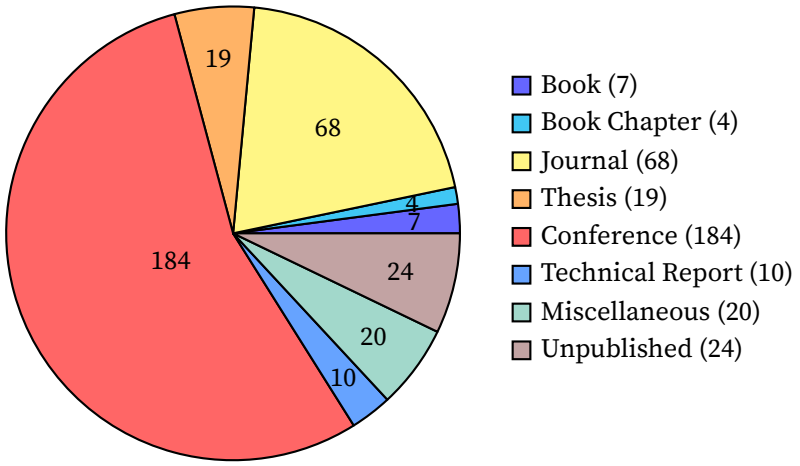


Figure A.1: Distribution of Types of Publications

A.1 Book

[1] R. Booth, G. CASINI, S. Klarman, R. Gilles, and I. Varzinczak, eds. *DARe-16 - Proceedings of the International Workshop on Defeasible and Ampliative Reasoning*. CEUR Workshop Proceedings, 2016. URL: http://hdl.handle.net/10993/30347.

[2] J. Clark, Sarah, P. Y. A. RYAN, D. Wallach, M. Brenner, and K. Rohloff, eds. *Financial Cryptography and Data Security - FC 2016 International Workshops, BITCOIN, VOTING, and WAHC*. Springer, 2016. URL: http://hdl.handle.net/10993/31725.

[3] T. van Dijk and C. SCHOMMER, eds. *Proceedings International Workshop Exploring Old Maps 2016*. University of Luxembourg, 2016. URL: http://hdl.handle.net/10993/27963.

[4] D. M. Gabbay and K. Schlechta. *A New Perspective on Nonmonotonic Logics*. Springer, 2016. ISBN: 978-3-319-46815-0. DOI: 10.1007/978-3-319-46817-4. URL: http://hdl.handle.net/10993/31405.

[5] S. M. Habib, J. Vassileva, S. MAUW, and M. Mühlhäuser, eds. *Proceedings of the 10th IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2016)*. Springer, 2016. ISBN: 978-3-319-41354-9. DOI: 10.1007/978-3-319-41354-9. URL: http://hdl.handle.net/10993/31073.

[6] F. Hao and P. Y. A. RYAN, eds. *Real-World Electronic Voting: Design, Analysis and Deployment*. Auerbach Publications, 2016. URL: http://hdl.handle.net/10993/31727.

[7] P. Y. A. RYAN, D. Naccache, and J.-J. Quisquater, eds. *The New Codebreakers - Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Springer, 2016. URL: http://hdl.handle.net/10993/31728.

A.2 Book Chapter

[8] C. BARTOLINI, D. E. KATEB, Y. L. TRAON, and D. Hagen. "Cloud Providers Viability: How to Address it from an IT and Legal Perspective?" In: *Economics of Grids, Clouds, Systems, and Services*. Springer International Publishing, 2016, pp. 281–295. ISBN: 978-3-319-43177-2. DOI: 10.1007/978-3-319-43177-2. URL: http://hdl.handle.net/10993/28485.

[9] D. M. Gabbay and O. Rodrigues. "Further Applications of the Gabbay-Rodrigues Iteration Schema in Argumentation and Revision Theories". In: *Computational Models of Rationality, Essays dedicated to Gabriele Kern-Isberner on the occasion of her 60th birthday*. College Publications, 2016. URL: http://hdl.handle.net/10993/31445.

[10] S. KUBLER, K. Främling, and A. Zaslavsky. "IoT Platforms Initiative". In: *Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds*. River Publishers, 2016, pp. 265–292. ISBN: 978-87-93379-81-7. URL: http://hdl.handle.net/10993/28167.

[11] P. Y. A. RYAN. "Crypto Santa". In: *The New Codebreakers - Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Springer, 2016. URL: http://hdl.handle.net/10993/31730.

A.3 Journal

[12] M. Abraham, I. Belfer, U. Schild, and D. M. Gabbay. "Quantum States and Disjunctive Attacks in Talmudic Logic". In: *Journal of Logics* (2016), p. 789. URL: http://hdl.handle.net/10993/31413.

[13] S. ALTMEYER and N. NAVET. "Towards a declarative modeling and execution framework for real-time systems". In: *ACM SIGBED Review* 3.2 (2016), pp. 30–33. URL: http://hdl.handle.net/10993/23413.

[14] D. A. AMBROSSIO, X. PARENT, and L. V. D. TORRE. "Cumulative Aggregation". In: *Deontic Logic and Normative Systems* (2016). URL: http://hdl.handle.net/10993/30218.

[15] P. Baroni, D. M. Gabbay, and M. Giacomin. "Introduction to the special issue on Loops in Argumentation". In: *J. Log. Comput.* 6.4 (2016), pp. 1051–1053. DOI: 10.1093/logcom/exu012. URL: http://hdl.handle.net/10993/31444.

[16] A. Bessani, N. F. Neves, P. E. VERISSIMO, D. Wagner, A. Fonseca, S. Rui, P. Luz, and M. Correia. "JITeR: Just-in-time application-layer routing". In: *Computer Networks* 104 (2016), pp. 122–136. URL: http://hdl.handle.net/10993/28232.

[17] L. I. U. Bing, L. LUCIA, S. NEJATI, L. BRIAND, and T. Bruckmann. "Simulink Fault Localisation: an Iterative Statistical Debugging Approach". In: *Software Testing, Verification & Reliability* 6.6 (2016), pp. 431–459. URL: http://hdl.handle.net/10993/24737.

[18] A. BIRYUKOV and D. KHOVRATOVICH. "Egalitarian computing". In: *USENIX Security 2016* (2016). URL: http://hdl.handle.net/10993/27654.

[19] A. BIRYUKOV, D. KHOVRATOVICH, and L. P. PERRIN. “Multiset-Algebraic Cryptanalysis of Reduced Kuznyechik, Khazad, and secret SPNs”. In: *IACR Transactions on Symmetric Cryptology* 6.2 (2016), pp. 226–247. DOI: 10.13154/tosc.v2016.i2.226-247. URL: http://hdl.handle.net/10993/30023.

[20] G. Boella, L. D. Caro, L. HUMPHREYS, L. ROBALDO, P. Rossi, and L. V. D. TORRE. “Eunomos, a legal document and knowledge management system for the Web to provide relevant, reliable and up-to-date information on the Law”. In: *Artificial Intelligence & Law* (2016). URL: http://hdl.handle.net/10993/28068.

[21] G. Boella, G. Pigozzi, and L. V. D. TORRE. “AGM Contraction and Revision of Rules”. In: *Journal of Logic, Language and Information* 5.3 (2016), pp. 273–297. URL: http://hdl.handle.net/10993/30685.

[22] P. CAIRE, A. MOAWAD, V. Efthymiou, A. bikakis, and Y. L. TRAON. “Privacy Challenges in Ambient Intelligence Systems”. In: *Journal of Ambient Intelligence and Smart Environments* (2016). URL: http://hdl.handle.net/10993/26416.

[23] A. D. Caro and V. IOVINO. “On the Power of Rewinding Simulators in Functional Encryption”. In: *Designs, Codes and Cryptography* (2016). URL: http://hdl.handle.net/10993/28143.

[24] L. CODECA, R. FRANK, S. FAYE, and T. ENGEL. “Luxembourg SUMO Traffic (LuST) Scenario: Traffic Demand Evaluation”. In: *IEEE Intelligent Transportation Systems Magazine* (2016). URL: http://hdl.handle.net/10993/28678.

[25] J. Cortes-Mendoza, A. Tchernykh, F. Armenta-Cano, P. BOUVRY, Drozdov, and L. Didelot. “Biobjective VoIP Service Management in Cloud Infrastructure”. In: *Scientific Programming* 4.5706790 (2016). DOI: 10.1155/2016/5706790. URL: http://hdl.handle.net/10993/30188.

[26] M. CRAMER. “The Naproche system: Proof-checking mathematical texts in controlled natural language”. In: *Sprache und Datenverarbeitung. International Journal for Language Data Processing* 4.1 (2016), pp. 9–33. URL: http://hdl.handle.net/10993/30185.

[27] T. Creutzig, Y. Hikida, and P. ROENNE. “Correspondences between WZNW models and CFTs with W-algebra symmetry”. In: *JHEP* 2 (2016), p. 048. DOI: 10.1007JHEP02(2016)048. URL: http://hdl.handle.net/10993/26831.

[28] G. DANOY, L. Jourdan, E.-G. Talbi, and S. Nesmachnow. “Foreword”. In: *International* (2016). URL: http://hdl.handle.net/10993/29865.

[29] L. I. Daoyuan, T. F. d. A. BISSYANDE, J. KLEIN, and Y. L. TRAON. “Time Series Classification with Discrete Wavelet Transformed Data”. In: *International Journal of Software Engineering & Knowledge Engineering* 6.9 (2016), pp. 1361–1377. DOI: 10.1142/S0218194016400088. URL: http://hdl.handle.net/10993/30509.

[30] B. Dave, S. KUBLER, K. Främling, and L. Koskela. “Opportunities for enhanced lean construction management using Internet of Things standards”. In: *Automation in Construction* 1 (2016), pp. 86–97. DOI: 10.1016/j.autcon.2015.10.009. URL: http://hdl.handle.net/10993/23028.

[31] R.-A. DOBRICAN, G. NEYENS, and D. ZAMPUNIERIS. “A Context-Aware Collaborative Mobile Application for Silencing the Smartphone during Meetings or Important Events”. In: *International Journal On Advances in Intelligent Systems* 9.1 (2016), pp. 171–180. URL: http://hdl.handle.net/10993/27987.

[32] A. R. DURAN, G. Danezis, and M. Kohlweiss. “Privacy-preserving smart metering revisited”. In: *International Journal of Information Security* (2016). URL: http://hdl.handle.net/10993/28952.

[33] S. FAYE and C. Chaudet. “Characterizing the Topology of an Urban Wireless Sensor Network for Road Traffic Management”. In: *IEEE Transactions on Vehicular Technology* 5.7 (2016), pp. 5720–5725. DOI: 10.1109/TVT.2015.2465811. URL: http://hdl.handle.net/10993/21720.

[34] S. FAYE, N. LOUVETON, G. GHEORGHE, and T. ENGEL. “A Two-Level Approach to Characterizing Human Activities from Wearable Sensor Data”. In: *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 7.3 (2016). URL: http://hdl.handle.net/10993/27638.

[35] D. M. Gabbay. “Logical foundations for bipolar and tripolar argumentation networks: preliminary results”. In: *J. Log. Comput.* 6.1 (2016), pp. 247–292. DOI: 10.1093/logcom/ext027. URL: http://hdl.handle.net/10993/26061.

[36] D. M. Gabbay. “The handling of loops in argumentation networks”. In: *J. Log. Comput.* 6.4 (2016), pp. 1065–1147. DOI: 10.1093/logcom/exu007. URL: http://hdl.handle.net/10993/31442.

[37] D. M. Gabbay. “Theory of Semi-Instantiation in Abstract Argumentation”. In: *Logica Universalis* 4 (2016), pp. 431–516. DOI: 10.1007/s11787-015-0133-9. URL: http://hdl.handle.net/10993/31406.

[38] D. M. Gabbay and M. Gabbay. “The attack as intuitionistic negation”. In: *Logic Journal of the IGPL* 4.5 (2016), pp. 807–837. DOI: 10.1093/jigpal/jzw012. URL: http://hdl.handle.net/10993/31404.

[39] D. M. Gabbay and M. Gabbay. “Theory of disjunctive attacks, Part I”. In: *Logic Journal of the IGPL* 4.2 (2016), pp. 186–218. DOI: 10.1093/jigpal/jzv032. URL: http://hdl.handle.net/10993/31443.

[40] D. M. Gabbay and O. Rodrigues. “Introducing Bayesian Argumentation Networks”. In: *The IfColog Journal of Logics and their Applications (FLAP)* (2016). URL: http://hdl.handle.net/10993/31410.

[41] Y. GENG, N. O. H. JungHyun, I. Drevensek-Olenik, R. Rupp, G. LENZINI, and J. LAGERWALL. “High-fidelity spherical cholesteric liquid crystal Bragg reflectors generating unclonable patterns for secure authentication”. In: *Scientific Reports* 6.26840 (2016), pp. 1–8. DOI: 10.1038/srep26840. URL: http://hdl.handle.net/10993/27540.

[42] I. Gonzalez-Herrera, J. Bourcier, E. Daubert, W. Rudametkin, O. Barais, F. FOUQUET, J.-M. Jézéquel, and B. Baudry. “ScapeGoat: Spotting abnormal resource usage in component-based reconfigurable software systems”. In: *Journal of Systems and Software* (2016). URL: http://hdl.handle.net/10993/26821.

[43] S. Gottmann, N. NACHTIGALL, C. Ermel, F. Hermann, and T. ENGEL. "Towards the Propagation of Model Updates along different Views in Multi-View Models". In: *Proceedings of the 5th International Workshop on Bidirectional Transformations* 1 (2016), pp. 45–60. URL: http://hdl.handle.net/10993/26582.

[44] H. Hamann, Y. Khaluf, J. BOTEV, M. D. Soorati, E. Ferrante, O. Kosak, J.-M. Montanier, S. Mostaghim, R. Redpath, J. Timmis, F. Veenstra, M. Wahby, and A. Zamuda. "Hybrid Societies: Challenges and Perspectives in the Design of Collective Behavior in Self-Organizing Systems". In: *Frontiers in Robotics and AI* 3.14 (2016). DOI: 10.3389/frobt.2016.00014. URL: http://hdl.handle.net/10993/26593.

[45] C. HAMMERSCHMIDT, S. Verwer, Q. Lin, and R. STATE. "Interpreting Finite Automata for Sequential Data". In: *Interpretable Machine Learning for Complex Systems: NIPS 2016 workshop proceedings* (2016). URL: http://hdl.handle.net/10993/29386.

[46] S. Khaled, M. Deaconu, A. Lejay, N. Champagnat, and N. NAVET. "Regime switching model for financial data: empirical risk analysis". In: *Physica A: Statistical Mechanics and its Applications* 1 (2016), pp. 148–157. DOI: 10.1016/j.physa.2016.05.002. URL: http://hdl.handle.net/10993/21249.

[47] S. Kim and K. I. M. Dongsun. "Automatic Identifier Inconsistency Detection Using Code Dictionary". In: *Empirical Software Engineering* 1.2 (2016), pp. 565–604. URL: http://hdl.handle.net/10993/20131.

[48] D. KLIAZOVICH, J. E. Pecero, A. Tchernykh, P. BOUVRY, S. U. khan, and A. Y. Zomaya. "CA-DAG: Modeling Communication-Aware Applications for Scheduling in Cloud Computing". In: *Journal of Grid Computing* 4.1 (2016), pp. 23–39. DOI: 10.1007/s10723-015-9337-8. URL: http://hdl.handle.net/10993/21041.

[49] S. KUBLER, J. ROBERT, D. William, V. Alexandre, and Y. L. TRAON. "A state-of the-art survey & testbed of Fuzzy AHP (FAHP) applications". In: *Expert Systems with Applications* 5 (2016), pp. 398–422. DOI: 10.1016/j.eswa.2016.08.064. URL: http://hdl.handle.net/10993/28568.

[50] P. R. Lewis, K. Bellman, J. BOTEV, H. Hildmann, S. Marsh, J. Pitt, I. Scholtes, and S. Tomforde. "Socially-Sensitive Systems Design – Working Group on "Understanding Social Concepts in Self-Organising Systems"". In: *Dagstuhl Reports* 5.11 (2016), pp. 142–147. URL: http://hdl.handle.net/10993/29509.

[51] M. L. Loces, J. Musial, J. Pecero, H. Fraire, J. Blazewicz, and P. BOUVRY. "Exact and heuristic approaches to solve the Internet shopping optimization problem with delivery costs". In: *International Journal of Applied Mathematics and Computer Science* 6 (2016), pp. 391–406. DOI: 10.1515/amcs-2016-0028. URL: http://hdl.handle.net/10993/30189.

[52] N. LOUVETON, R. MCCALL, V. Koenig, T. AVANESOV, and T. ENGEL. "Driving while using a smartphone-based mobility application: Evaluating the impact of three multi-choice user interfaces on visual-manual distraction". In: *Applied Ergonomics* 4 (2016), pp. 196–204. DOI: 10.1016/j.apergo.2015.11.012. URL: http://hdl.handle.net/10993/24740.

[53] M. Madhikermi, S. KUBLER, J. ROBERT, A. Buda, and K. Främling. "Data Quality Assessment of Maintenance Reporting Procedures". In: *Expert Systems with Applications* (2016). DOI: 10.1016/j.eswa.2016.06.043. URL: http://hdl.handle.net/10993/28081.

[54] A. D. MAIO, M. R. PALATTELLA, R. Soua, L. Lamorte, X. Vilajosana, J. Alonso-Zarate, and T. ENGEL. "Enabling SDN in VANETs: What is the Impact on Security?" In: *Sensors* 6.12 (2016), p. 2077. DOI: 10.3390/s16122077. URL: http://hdl.handle.net/10993/29382.

[55] D. Marosin, Z. E. E. M. VAN, and S. Ghanavati. "Formalizing and Modeling Enterprise Architecture (EA) Principles with Goal-oriented Requirements Language (GRL)". In: *Proceedings of the 28th International Conference on Advanced Information System Engineering (CAiSE16)* (2016). URL: http://hdl.handle.net/10993/29391.

[56] S. Merz, J. PANG, and J. S. Dong. *Editorial (ICFEM 14 special issue, part I)*. 2016. URL: http://hdl.handle.net/10993/27340.

[57] S. Merz, J. PANG, and J. S. Dong. "Editorial (ICFEM 14 special issue, part II)". In: *Formal Aspects of Computing* 8.5 (2016), pp. 723–724. URL: http://hdl.handle.net/10993/28257.

[58] S. NESHVAD, H. MARGOSSIAN, and J. SACHAU. "Topology and Parameter Estimation in Power Systems through Inverter Based Broadband Stimulations". In: *IET Generation, Transmission & Distribution* (2016). URL: http://hdl.handle.net/10993/24924.

[59] M. R. PALATTELLA, M. Dohler, L. A. Grieco, G. Rizzo, J. Torsen, T. ENGEL, and L. LADID. "Internet of Things in the 5G Era: Enablers, Architecture and Business Models". In: *IEEE Journal on Selected Areas In Communications* (2016). URL: http://hdl.handle.net/10993/24796.

[60] J. PANG and M. Stoelinga. *Selected and extended papers from ACM SVT 2014*. 2016. URL: http://hdl.handle.net/10993/27341.

[61] A. Perovi, D. DODER, Z. Ognjanovi, and M. Ra\vskovi. "On evaluations of propositional formulas in countable structures". In: *Filomat* 1 (2016), pp. 1–13. URL: http://hdl.handle.net/10993/31053.

[62] G. Piro, S. SIGNORELLO, M. R. PALATTELLA, L. A. Grieco, G. Boggia, and T. ENGEL. "Understanding the Social impact of ICN: between myth and reality". In: *Springer AI & Society: Journal of Knowledge, Culture and Communication* (2016). URL: http://hdl.handle.net/10993/23782.

[63] J. L. T. POZO, D. P. González, and F. V. Mesa. "Limpieza de ruido para clasificación basado en vecindad y cambios de concepto en el tiempo". In: *Revista Cubana de Ciencias Informaticas* 2 (2016), pp. 1–13. URL: http://hdl.handle.net/10993/28389.

[64] R. T. RASUA and I. G. Yero. "Characterizing 1-metric antidimensional trees and unicyclic graphs". In: *Computer Journal* 9.8 (2016), pp. 1264–1273. URL: http://hdl.handle.net/10993/28762.

[65] E. Rogstad and L. BRIAND. "Clustering Deviations for Black Box Regression Testing of Database Applications". In: *IEEE Transactions on Reliability* 5.1 (2016), pp. 4–18. URL: http://hdl.handle.net/10993/19454.

[66] E. Rogstad and L. BRIAND. “Cost-effective Strategies for the Regression Testing of Database Applications: Case study and Lessons Learned”. In: *Journal of Systems and Software* 3 (2016), pp. 257–274. URL: http://hdl.handle.net/10993/22772.

[67] P. Y. A. RYAN, P. ROENNE, and V. IOVINO. “Selene: Voting with Transparent Verifiability and Coercion-Mitigation”. In: *IACR Cryptology ePrint Archive || Abstract book of 1st Workshop on Advances in Secure Electronic Voting* 5 (2016), p. 1105. URL: http://hdl.handle.net/10993/24802%20%7C%7C%20http://hdl.handle.net/10993/26832.

[68] Y. Salgueiro, J. L. T. POZO, R. Bello, and R. Falcon. “Multiobjective variable mesh optimization”. In: *Annals of Operations Research* (2016). DOI: 10.1007/s10479-016-2221-5. URL: http://hdl.handle.net/10993/28187.

[69] S. SIGNORELLO, R. STATE, J. François, and O. Festor. “NDN.p4: Programming Information-Centric data-planes”. In: *Proceedings of the IEEE International Workshop on Open-Source Software Networking at NetSoft2016* (2016). DOI: 10.1109/NETSOFT.2016.7502472. URL: http://hdl.handle.net/10993/28007.

[70] D. P. B. SPAGNUELO and G. LENZINI. “Patient-Centred Transparency Requirements for Medical Data Sharing Systems”. In: *Proceedings of the 4th World Conference on Information Systems and Technologies* (2016). URL: http://hdl.handle.net/10993/23569.

[71] D. P. B. SPAGNUELO and G. LENZINI. “Transparent Medical Data Systems”. In: *Journal of Medical Systems* (2016). DOI: 10.1007/s10916-016-0653-8. URL: http://hdl.handle.net/10993/28698.

[72] A. Tchernykh, L. Lozano, U. Schwiegelshohn, P. BOUVRY, J. Pecero, S. Nesmachnow, and A. Drosdov. “Online Bi-Objective Scheduling for IaaS Clouds Ensuring Quality of Service”. In: *Journal of Grid Computing* 4 (2016). DOI: 10.1007/s10723-015-9340-0. URL: http://hdl.handle.net/10993/30190.

[73] D. Teubner, A.-K. Wesslein, P. ROENNE, M. Veith, C. Frings, and M. Paulus. “Is a visuo-haptic differentiation of zebra mussel and quagga mussel based on a single external morphometric shell character possible?” In: *Aquatic Invasions* (2016). URL: http://hdl.handle.net/10993/27989.

[74] L. V. D. TORRE, M. Giacomin, B. Liao, and D. M. Gabbay. “Present and Future of Formal Argumentation”. In: *Dagstuhl Reports* (2016). DOI: 10.4230/DagRep.5.8.74. URL: http://hdl.handle.net/10993/26041.

[75] A. Tretakiova, F. Seredynski, and P. BOUVRY. “Online Bi-Objective Scheduling for IaaS Clouds Ensuring Quality of Service”. In: *Simulation* 2 (2016). DOI: 10.1177/0037549715612579. URL: http://hdl.handle.net/10993/30191.

[76] Q. YUAN, H. Qu, J. PANG, and A. MIZERA. “Improving BDD-based attractor detection for synchronous Boolean networks.” In: *SCIENCE CHINA Information Sciences* 9.8 (2016), 080101:1–080101:16. URL: http://hdl.handle.net/10993/28348.

[77] P. Zarnowiec, A. MIZERA, M. Chrapek, M. Urbaniak, and W. Kaca. “Chemometric analysis of attenuated total reflectance infrared spectra of Proteus mirabilis strains with defined structures of LPS.” In: *Innate Immunity* 2.5 (2016), pp. 325–335. URL: http://hdl.handle.net/10993/28347.

[78] L. I. U. Zhe, H. Seo, J. GROSZSCHÄDL, and H. Kim. “Efficient Implementation of NIST-Compliant Elliptic Curve Cryptography for 8-bit AVR-Based Sensor Nodes”. In: *IEEE Transactions on Information Forensics and Security* 1.7 (2016), pp. 1385–1397. DOI: 10.1109/TIFS.2015.2491261. URL: http://hdl.handle.net/10993/27839.

[79] M. Zotkiewicz, M. GUZEK, D. KLIAZOVICH, and P. BOUVRY. “Minimum Dependencies Energy-Efficient Scheduling in Data Centers”. In: *IEEE Transactions on Parallel & Distributed Systems* (2016). DOI: 10.1109/TPDS.2016.2542817. URL: http://hdl.handle.net/10993/26585.

A.4 Thesis

[80] D. APPELT. “Automated Security Testing of Web-Based Systems Against SQL Injection Attacks”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/27947.

[81] C. ARORA. “AUTOMATED ANALYSIS OF NATURAL-LANGUAGE REQUIREMENTS USING NATURAL LANGUAGE PROCESSING”. PhD thesis. University of Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/28922.

[82] L. CODECA. “Dynamic Vehicular Routing in Urban Environments”. PhD thesis. University of Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/29015.

[83] R.-A. DOBRICAN. “COLLABORATIVE RULE-BASED PROACTIVE SYSTEMS: MODEL, INFORMATION SHARING STRATEGY AND CASE STUDIES”. PhD thesis. University of Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/29093.

[84] C. FIANDRINO. “Energy-efficient Communications in Cloud, Mobile Cloud and Fog Computing”. PhD thesis. University of Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/28841.

[85] T. HARTMANN. “Enabling Model-Driven Live Analytics For Cyber-Physical Systems: The Case of Smart Grids”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/28924.

[86] S. HÖHN. “Data-driven Repair Models for Text Chat with Language Learners”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/27057.

[87] J.-L. HUYNEN. “Socio-Technical Aspects of Security Analysis”. PhD thesis. University of Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/29006.

[88] M. KRACHEEL. “Changing Commuter Behaviour through Gamification”. PhD thesis. University of Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/28849.

[89] L. I. Li. “Boosting Static Security Analysis of Android Apps through Code Instrumentation”. PhD thesis. University of Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/29387.

[90] J. MARTINEZ. “Mining Software Artefact Variants for Product Line Migration and Analysis”. PhD thesis. University of Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/28675.

[91] R. MATINNEJAD. “AUTOMATED TESTING OF SIMULINK/STATEFLOW MODELS IN THE AUTOMOTIVE DOMAIN”. PhD thesis. University of Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/28688.

[92] A. MOAWAD. “Towards Ambient Intelligent Applications Using Models@run.time And Machine Learning For Context-Awareness”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/23746.

[93] N. NACHTIGALL. “Domain Completeness of Model Transformations and Synchronisations”. PhD thesis. University of Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/29181.

[94] D. D. NARDO. “Model-Based Test Automation Strategies for Data Processing Systems”. PhD thesis. University of Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/26911.

[95] S. NESHVAD. “Topology and Parameter Estimation in Power Systems Though Inverter Based Broadband Stimulations”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/27964.

[96] S. S. NIELSEN. “Diversity Preserving Genetic Algorithms - Application to the Inverted Folding Problem and Analogous Formulated Benchmarks”. PhD thesis. University of Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/28226.

[97] M. TABATABAEI. “GAMES AND STRATEGIES IN ANALYSIS OF SECURITY PROPERTIES”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/29502.

[98] D. O. U. Wei. “A Model-Driven Approach to Offline Trace Checking of Temporal Properties”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2016. URL: http://hdl.handle.net/10993/29184.

A.5 Conference

[99] M. Abraham, I. Belfer, U. J. Schild, and D. M. Gabbay. “Identity Merging and Identity Revision in Talmudic Logic: An Outline Paper”. In: *Computational Models of Rationality, Essays dedicated to Gabriele Kern-Isberner on the occasion of her 60th birthday*. 2016. URL: http://hdl.handle.net/10993/31412.

[100] K. Adebayo, L. D. Caro, L. ROBALDO, and G. Boella. “Textual Inference with Deep Learning Technique”. In: *Proc. of the 28th Annual Benelux Conference on Artificial Intelligence (BNAIC2016)*. (2016). URL: http://hdl.handle.net/10993/29463.

[101] K. ALLIX, T. F. d. A. BISSYANDE, J. KLEIN, and Y. L. TRAON. “AndroZoo: Collecting Millions of Android Apps for the Research Community”. In: *Proceedings of the 13th International Workshop on Mining Software Repositories*. ACM, 2016, pp. 468–471. ISBN: 978-1-4503-4186-8. DOI: 10.1145/2901739.2903508. URL: http://hdl.handle.net/10993/27396.

[102] L. Amgoud, J. Ben-Naim, D. DODER, and S. Vesic. “Ranking Arguments With Compensation-Based Semantics”. In: *Principles of Knowledge Representation and Reasoning: Proceedings of the Fifteenth International Conference, KR 2016, Cape Town, South Africa, April 25-29, 2016*. 2016. URL: http://hdl.handle.net/10993/31054.

[103] C. ARORA, M. SABETZADEH, L. BRIAND, and F. Zimmer. “Extracting Domain Models from Natural-Language Requirements: Approach and Industrial Evaluation”. In: *19th International Conference on Model Driven Engineering Languages and Systems, Saint-Malo 2-7 October 2016*. 2016. URL: http://hdl.handle.net/10993/28067.

[104] A. D. ARRIAGA, M. Barbosa, and P. Farshim. “Private Functional Encryption: Indistinguishability-Based Definitions and Constructions from Obfuscation”. In: *Progress in Cryptology – INDOCRYPT 2016: 17th International Conference on Cryptology in India, Kolkata, India, December 11-14, 2016, Proceedings*. Springer, 2016. ISBN: 978-3-319-49890-4. DOI: 10.1007/978-3-319-49890-4_13. URL: http://hdl.handle.net/10993/29144.

[105] A. D. ARRIAGA, V. IOVINO, and Q. Tang. “Updatable Functional Encryption”. In: *Paradigms in Cryptology - Mycrypt 2016. Malicious and Exploratory Cryptology, Second International Conference, Mycrypt 2016, Kuala Lumpur, Malaysia, December 1-2, 2016, Revised Selected Papers*. Springer, 2016. ISBN: 978-3-319-61272-0. URL: http://hdl.handle.net/10993/29145.

[106] A. ATASHPENDAR, B. Dorronsoro, G. DANOY, and P. BOUVRY. “A Parallel Cooperative Coevolutionary SMPSO Algorithm for Multi-objective Optimization”. In: *IEEE International Conference on High Performance Computing Simulation (HPCS)*. 2016, pp. 713–720. DOI: 10.1109/HPCSim.2016.7568405. URL: http://hdl.handle.net/10993/29925.

[107] C. Atten, L. Chanouf, G. DANOY, and P. BOUVRY. “UAV Fleet Mobility Model with Multiple Pheromones for Tracking Moving Observation Targets”. In: *19th European Conference on Applications of Evolutionary Computation (EvoApplications)*. Springer, 2016. URL: http://hdl.handle.net/10993/26850.

[108] C. BARTOLINI, A. GIURGIU, G. LENZINI, and L. ROBALDO. “A Framework to Reason about the Legal Compliance of Security Standards”. In: *Proceedings of the Tenth International Workshop on Juris-informatics (JURISIN)*. 2016. URL: http://hdl.handle.net/10993/28786.

[109] C. BARTOLINI, G. LENZINI, and L. ROBALDO. “Towards legal compliance by correlating Standards and Laws with a semi-automated methodology”. In: *Proceedings of the 28 Benelux Conference on Artificial Intelligence (BNAIC)*. 2016. URL: http://hdl.handle.net/10993/28957.

[110] B. Behringer and S. ROTHKUGEL. “Integrating feature-based implementation approaches using a common graph-based representation”. In: *ACM Symposium on Applied Computing, Pisa, Italy, April 4-8, 2016*. 2016, pp. 1504–1511. URL: http://hdl.handle.net/10993/29046.

[111] M. M. Bersani, D. BIANCULLI, C. Ghezzi, S. Krstic, and P. S. Pietro. “Efficient Large-scale Trace Checking Using MapReduce”. In: *Proceedings of the 38th International Conference on Software Engineering (ICSE 2016)*. 2016, pp. 888–898. DOI: 10.1145/2884781.2884832. URL: http://hdl.handle.net/10993/20110.

[112] L. I. U. Bing, L. LUCIA, S. NEJATI, L. BRIAND, and T. Bruckmann. “Localizing Multiple Faults in Simulink Models.” In: *23rd IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER 2016)*. 2016. URL: http://hdl.handle.net/10993/23993.

[113] A. BIRYUKOV, D.-D. DINU, and J. GROSZSCHÄDL. “Correlation Power Analysis of Lightweight Block Ciphers: From Theory to Practice”. In: *Applied Cryptography and Network Security - 14th International Conference, ACNS 2016, Guildford, UK, June 19-22, 2016. Proceedings*. Springer Verlag, 2016, pp. 537–557. DOI: 10.1007/978-3-319-39555-5_29. URL: http://hdl.handle.net/10993/27849.

[114] A. BIRYUKOV, D.-D. DINU, and D. KHOVRATOVICH. “Argon2: New Generation of Memory-Hard Functions for Password Hashing and Other Applications”. In: *IEEE European Symposium on Security and Privacy*. 2016, pp. 292–302. URL: http://hdl.handle.net/10993/31652.

[115] A. BIRYUKOV and D. KHOVRATOVICH. “Equihash: asymmetric proof-of-work based on the Generalized Birthday problem”. In: *Proceedings of NDSS 2016*. 2016, p. 13. URL: http://hdl.handle.net/10993/22277.

[116] A. BIRYUKOV, G. Leurent, and L. P. PERRIN. “Cryptanalysis of Feistel Networks with Secret Round Functions”. In: *Selected Areas in Cryptography – SAC 2015, 21st International Conference, Sackville, NB, Canada, August 12-14, 2015, Revised Selected Papers*. Springer International Publishing, 2016, pp. 102–121. URL: http://hdl.handle.net/10993/22278.

[117] A. BIRYUKOV, L. P. PERRIN, and A. UDOVENKO. “Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1”. In: *Advances in Cryptology – EUROCRYPT 2016*. Springer Berlin Heidelberg, 2016, pp. 372–402. ISBN: 978-3-662-49890-3. DOI: 10.1007/978-3-662-49890-3_15. URL: http://hdl.handle.net/10993/23895.

[118] A. BIRYUKOV, V. VELICHKOV, and Y. L. CORRE. “Automatic Search for the Best Trails in ARX: Application to Block Cipher Speck”. In: *Fast Software Encryption - FSE 2016*. 2016. URL: http://hdl.handle.net/10993/29482.

[119] J. BOTEV. “Demonstrating the CollaTrEx Framework for Collaborative Context-Aware Mobile Training and Exploration”. In: *Proceedings of the International Conference on Educational Technologies (ICEduTech)*. 2016. URL: http://hdl.handle.net/10993/29508.

[120] J. BOTEV, R. Marschall, and S. ROTHKUGEL. “CollaTrEx – Collaborative Context-Aware Mobile Training and Exploration”. In: *Proceedings of the International Conference on Design, Learning & Innovation (DLI)*. 2016. URL: http://hdl.handle.net/10993/26596%20%7C%7C%20http://hdl.handle.net/10993/30044.

[121] P. BOUVRY, S. Chaumette, G. DANOY, G. Guerrini, G. Jurquet, A. Kuwertz, W. Müller, M. ROSALIE, and J. Sander. “Using Heterogeneous Multilevel Swarms of UAVs and High-Level Data Fusion to Support Situation Management in Surveillance Scenarios”. In: *2016 IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems, MFI 2016*. 2016. URL: http://hdl.handle.net/10993/28474.

[122] L. BRIAND, S. NEJATI, M. SABETZADEH, and D. BIANCULLI. “Testing the Untestable: Model Testing of Complex Software-Intensive Systems”. In: *Proceedings of the 38th International Conference on Software Engineering (ICSE 2016) Companion*. ACM, 2016, pp. 789–792. DOI: 10.1145/2889160.2889212. URL: http://hdl.handle.net/10993/23840.

[123] W. BRONZI, T. DERRMANN, G. CASTIGNANI, and T. ENGEL. “Towards Characterizing Bluetooth Discovery in a Vehicular Context”. In: *Vehicular Networking Conference (VNC), 2016 IEEE*. 2016. URL: http://hdl.handle.net/10993/28801.

[124] J. Camenisch, M. Dubovitskaya, and A. R. DURAN. “UC Commitments for Modular Protocol Design and Applications to Revocation and Attribute Tokens”. In: *Advances in Cryptology – CRYPTO 2016*. Springer Berlin Heidelberg, 2016, pp. 208–239. ISBN: 978-3-662-53014-6. URL: http://hdl.handle.net/10993/28276.

[125] A. CAPPONI, C. FIANDRINO, C. FRANCK, U. SORGER, D. KLIAZOVICH, and P. BOUVRY. “Assessing Performance of Internet of Things-based Mobile Crowdsensing Systems for Sensing as a Service Applications in Smart Cities”. In: *8th IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. 2016. URL: http://hdl.handle.net/10993/28784.

[126] A. D. caro, V. IOVINO, and A. O’Neill. “Deniable Functional Encryption”. In: *Public-key Cryptography - PKC 2016, 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part I*. Springer, 2016, p. 27. ISBN: 978-3-662-49384-7. URL: http://hdl.handle.net/10993/24801.

[127] G. CASINI and T. Meyer. “Using Defeasible Information to Obtain Coherence”. In: *Proceedings of the 15th International Conference on Principle of Knowledge Representation and Reasoning (KR-16)*. AAAI Press, 2016. ISBN: 978-1-57735-755-1. URL: http://hdl.handle.net/10993/30341.

[128] G. CASINI and T. Meyer. “Using Defeasible Information to Obtain Coherence”. In: *BNAIC 2016 - Proceedings of the 28th Benelux Conference on Artificial intelligence*. 2016, pp. 124–125. URL: http://hdl.handle.net/10993/30348.

[129] M. Ceccato, D. C. NGUYEN, D. APPELT, and L. BRIAND. “SOFIA: An Automated Security Oracle for Black-Box Testing of SQL-Injection Vulnerabilities”. In: *Proceedings of the 31th IEEE/ACM International Conference on Automated Software Engineering*. 2016. URL: http://hdl.handle.net/10993/28150.

[130] H. Coles, T. Laurent, C. Henard, M. PAPADAKIS, and A. Ventresque. “PIT a Practical Mutation Testing Tool for Java”. In: *International Symposium on Software Testing and Analysis, ISSTA 2016*. 2016. URL: http://hdl.handle.net/10993/28928.

[131] M. CRAMER, P. V. Hertum, R. Lapauw, I. Dasseville, and M. Denecker. “Resilient Delegation Revocation with Precedence for Predecessors is NP-Complete”. In: *IEEE 29th Computer Security Foundations Symposium*. 2016, pp. 432–442. URL: http://hdl.handle.net/10993/30186.

[132] L. I. Daoyuan, T. F. d. A. BISSYANDE, J. KLEIN, and Y. L. TRAON. “DSCo-NG: A Practical Language Modeling Approach for Time Series Classification”. In: *The 15th International Symposium on Intelligent Data Analysis*. 2016. URL: http://hdl.handle.net/10993/27942.

[133] L. I. Daoyuan, T. F. d. A. BISSYANDE, J. KLEIN, and Y. L. TRAON. “Time Series Classification with Discrete Wavelet Transformed Data: Insights from an Empirical Study”. In: *The 28th International Conference on Software Engineering and Knowledge Engineering (SEKE 2016)*. 2016. URL: http://hdl.handle.net/10993/26842.

[134] L. I. Daoyuan, T. F. d. A. BISSYANDE, S. KUBLER, J. KLEIN, and Y. L. TRAON. “Profiling household appliance electricity usage with n-gram language modeling”. In: *The 2016 IEEE International Conference on Industrial Technology (ICIT 2016)*. 2016. URL: http://hdl.handle.net/10993/24163.

[135] L. I. Daoyuan, L. I. Li, T. F. d. A. BISSYANDE, J. KLEIN, and Y. L. TRAON. “DSCo: A Language Modeling Approach for Time Series Classification”. In: *12th International Conference on Machine Learning and Data Mining (MLDM 2016)*. 2016. URL: http://hdl.handle.net/10993/26733.

[136] T. DERRMANN, R. FRANK, S. FAYE, G. CASTIGNANI, and T. ENGEL. “Towards Privacy-Neutral Travel Time Estimation from Mobile Phone Signalling Data”. In: *Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2)*. 2016. URL: http://hdl.handle.net/10993/28013.

[137] X. Devroey, G. Perrouin, M. PAPADAKIS, A. Legay, P.-Y. Schobbens, and P. Heymans. “Featured model-based mutation analysis”. In: *38th International Conference on Software Engineering (ICSE’16)*. 2016. URL: http://hdl.handle.net/10993/28926.

[138] D.-D. DINU, L. P. PERRIN, A. UDOVENKO, V. VELICHKOV, J. GROSZSCHÄDL, and A. BIRYUKOV. “Design Strategies for ARX with Provable Bounds: SPARX and LAX”. In: *Advances in Cryptology - ASIACRYPT 2016*. Springer Berlin Heidelberg, 2016, pp. 484–513. ISBN: 978-3-662-53887-6. URL: http://hdl.handle.net/10993/29917.

[139] R.-A. DOBRICAN and D. ZAMPUNIERIS. “A Proactive Solution, using Wearable and Mobile Applications, for Closing the Gap between the Rehabilitation Team and Cardiac Patients”. In: *Proceedings of the IEEE International Conference on Healthcare Informatics 2016 (ICHI 2016)*. IEEE, 2016, pp. 146–155. ISBN: 978-1-5090-6117-4. DOI: 10.1109/ICHI.2016.23. URL: http://hdl.handle.net/10993/28427.

[140] L. DOLBERG, J. François, S. R. Chowdhury, R. Ahmed, R. Boutaba, and T. ENGEL. “A Generic Framework to Support Application-Level Flow Management in Software-Defined Networks”. In: *Conference on Network Softwarization (Netsoft)*. 2016. URL: http://hdl.handle.net/10993/28051.

[141] A. R. DURAN. “On the Insecurity of a Method for Providing Secure and Private Fine-Grained Access to Outsourced Data”. In: *Abstract book of 2016 IEEE 8th International Conference on Cloud Computing Technology and Science (CloudCom)* (2016). URL: http://hdl.handle.net/10993/29285.

[142] J. Emeras, X. BESSERON, S. VARRETTE, P. BOUVRY, and B. PETERS. “HPC or the Cloud: a cost study over an XDEM Simulation”. In: *Proc. of the 7th International Supercomputing Conference in Mexico (ISUM 2016)*. 2016. URL: http://hdl.handle.net/10993/29825.

[143] J. EMERAS, S. VARRETTE, and P. BOUVRY. “Amazon Elastic Compute Cloud (EC2) vs. in-House HPC Platform: a Cost Analysis”. In: *Proc. of the 9th IEEE Intl. Conf. on Cloud Computing (CLOUD 2016)*. IEEE Computer Society, 2016. URL: http://hdl.handle.net/10993/27837.

[144] A. B. FADHEL, D. BIANCULLI, and L. BRIAND. “GemRBAC-DSL: a High-level Specification Language for Role-based Access Control Policies”. In: *21st ACM Symposium on Access Control Models and Technologies (SACMAT 2016)*. ACM, 2016. DOI: 10.1145/2914642.2914656. URL: http://hdl.handle.net/10993/26814.

[145] A. B. FADHEL, D. BIANCULLI, L. BRIAND, and B. Hourte. “A model-driven approach to representing and checking RBAC contextual policies.” In: *Proceedings of the 6th ACM Conference on Data and Application Security and Privacy (CODASPY 2016)*. 2016, pp. 243–253. DOI: 10.1145/2857705.2857709. URL: http://hdl.handle.net/10993/22759.

[146] S. FAYE and T. ENGEL. “Understanding User Daily Mobility Using Mobile and Wearable Sensing Systems”. In: *Proceedings of the 2016 International Conference on Information and Communications Technology Convergence - ICTC 2016*. 2016. URL: http://hdl.handle.net/10993/28245.

[147] S. FAYE, N. LOUVETON, G. GHEORGHE, and T. ENGEL. “Toward a Characterization of Human Activities using Smart Devices: A Micro/Macro Approach”. In: *Proceedings of the 7th IEEE INFOCOM International Workshop on Mobility Management in the Networks of the Future World*. 2016. DOI: 10.1109/INFCOMW.2016.7562162. URL: http://hdl.handle.net/10993/24896.

[148] S. FAYE, I. Tahirou, and T. ENGEL. “Demo Abstract: Human Mobility Profiling Using Privacy-Friendly Wi-Fi and Activity Traces”. In: *Proceedings of the 14th ACM Conference on Embedded Networked Sensor Systems (SenSys 2016)*. 2016. DOI: 10.1145/2994551.2996530. URL: http://hdl.handle.net/10993/28400.

[149] A. Ferreira and G. LENZINI. “Comparing and Integrating Break-the-Glass and Delegation in Role-based Access Control for Healthcare”. In: *Proc. of the nd Int. Conference on International Conference in Information Systems Security and Privacy (ICISSP)*. Springer, 2016. URL: http://hdl.handle.net/10993/23568.

[150] C. FIANDRINO, B. Kantarci, F. Anjomshoa, D. KLIAZOVICH, P. BOUVRY, and J. Matthews. “Sociability-Driven User Recruitment in Mobile Crowdsensing Internet of Things Platforms”. In: *IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 2016*. 2016. URL: http://hdl.handle.net/10993/27843.

[151] C. FIANDRINO, D. KLIAZOVICH, P. BOUVRY, and A. Y. Zomaya. “Network Coding-based Content Distribution in Cellular Access Networks”. In: *IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 2016*. 2016. URL: http://hdl.handle.net/10993/24605.

[152] M. Fraile, M. Ford, O. GADYATSKAYA, R. Kumar, M. Stoelinga, and R. T. RASUA. “Using attack-defense trees to analyze threats and countermeasures in an ATM: a case study”. In: *IFIP Working Conference on The Practice of Enterprise Modeling*. 2016, pp. 326–334. DOI: 10.1007/978-3-319-48393-1_24. URL: http://hdl.handle.net/10993/28979.

[153] D. M. Gabbay and M. Gabbay. “Argumentation as Information Input: A Position Paper”. In: *Computational Models of Argument - Proceedings of COMMA 2016, Potsdam Germany, 12-16 September, 2016.* 2016. DOI: 10.3233/978-1-61499-686-6-311. URL: http://hdl.handle.net/10993/31411.

[154] D. M. Gabbay and O. Rodrigues. “Degrees of ”in”, ”out” and ”undecided” in Argumentation Networks”. In: *Computational Models of Argument - Proceedings of COMMA 2016, Potsdam Germany, 12-16 September, 2016.* 2016. DOI: 10.3233/978-1-61499-686-6-319. URL: http://hdl.handle.net/10993/31403.

[155] O. GADYATSKAYA. “How to Generate Security Cameras: Towards Defence Generation for Socio-Technical Systems”. In: *Proc. of GraMSec 2015*. Springer, 2016. URL: http://hdl.handle.net/10993/23814.

[156] O. GADYATSKAYA, R. R. Hansen, K. G. Larsen, A. Legay, M. C. Olesen, and D. B. Poulsen. “Modelling Attack-defense Trees Using Timed Automata”. In: *Proc. of FORMATS*. Springer, 2016. DOI: 10.1007/978-3-319-44878-7_3. URL: http://hdl.handle.net/10993/29225.

[157] O. GADYATSKAYA, C. Harpes, S. MAUW, C. Muller, and S. Muller. “Bridging two worlds: Reconciling practical risk assessment methodologies with theory of attack trees”. In: *Proc. of GraMSec*. Springer, 2016. DOI: 10.1007/978-3-319-46263-9_5. URL: http://hdl.handle.net/10993/29224.

[158] O. GADYATSKAYA, R. JHAWAR, P. KORDY, K. LOUNIS, S. MAUW, and R. T. RASUA. "Attack trees for practical security assessment: ranking of attack scenarios with ADTool 2.0". In: *Quantitative Evaluation of Systems - 13th International Conference*. Springer, 2016, pp. 159–162. URL: http://hdl.handle.net/10993/28763.

[159] O. GADYATSKAYA, K. Labunets, and F. Paci. "Towards Empirical Evaluation of Automated Risk Assessment Methods". In: *Risks and Security of Internet and Systems*. Springer, 2016. DOI: 10.1007/978-3-319-54876. URL: http://hdl.handle.net/10993/29928.

[160] O. GADYATSKAYA, A.-L. Lezza, and Y. Zhauniarovich. "Evaluation of Resource-based App Repackaging Detection in Android". In: *Proc. of NordSec*. Springer, 2016. DOI: 10.1007/978-3-319-47560-8_9. URL: http://hdl.handle.net/10993/29223.

[161] L. GAMMAITONI and N. Hochgeschwender. "RPSL meets lightning: A model-based approach to design space exploration of robot perception systems". In: *RPSL meets lightning: A model-based approach to design space exploration of robot perception systems*. 2016. URL: http://hdl.handle.net/10993/30976.

[162] L. GAMMAITONI, P. KELSEN, and Q. Ma. "Agile Validation of Higher Order Transformations Using F-Alloy". In: *Agile Validation of Higher Order Transformations Using F-Alloy*. 2016. URL: http://hdl.handle.net/10993/28977.

[163] G. GHEORGHE, N. LOUVETON, B. Martin, B. Viraize, L. Mougin, S. FAYE, and T. ENGEL. "Heat is in the Eye of the Beholder: Towards Better Authenticating on Smartglasses". In: *Proceedings of the 9th International Conference on Human System Interaction (HSI'16)*. 2016. URL: http://hdl.handle.net/10993/27383.

[164] R. Giustolisi, V. IOVINO, and P. Rønne. "On the Possibility of Non-Interactive E-Voting in the Public-key Setting". In: *Financial Cryptography and Data Security, FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers*. Springer, 2016. ISBN: 978-3-662-53356-7. URL: http://hdl.handle.net/10993/24799.

[165] P. GLAUNER. "Deep Learning For Smile Recognition". In: *Proceedings of the 12th International FLINS Conference (FLINS 2016)*. 2016. URL: http://hdl.handle.net/10993/28367.

[166] P. GLAUNER, A. Boechat, L. Dolberg, R. STATE, F. Bettinger, Y. Rangoni, and D. Duarte. "Large-Scale Detection of Non-Technical Losses in Imbalanced Data Sets". In: *Proceedings of the Seventh IEEE Conference on Innovative Smart Grid Technologies (ISGT 2016)*. 2016. URL: http://hdl.handle.net/10993/28370.

[167] P. GLAUNER, J. A. MEIRA, L. Dolberg, R. STATE, F. Bettinger, Y. Rangoni, and D. Duarte. "Neighborhood Features Help Detecting Non-Technical Losses in Big Data Sets". In: *Proceedings of the 3rd IEEE/ACM International Conference on Big Data Computing Applications and Technologies (BDCAT 2016)*. 2016. URL: http://hdl.handle.net/10993/28594.

[168] A. GÖKNIL, I. Kurtev, and K. van den Berg. “A Rule-based Approach for Evolution of AADL Models based on Changes in Functional Requirements”. In: *The workshop on Sustainable Architecture: Global Collaboration, Requirements, Analysis (SAGRA) at the 10th European Conference on Software Architecture (ECSA)*. 2016. DOI: 10.1145/2993412.3004846. URL: http://hdl.handle.net/10993/29021.

[169] I. Gonzalez-Herrera, J. Bourcier, W. Rudametkin, O. Barais, and F. FOUQUET. “Squirrel: Architecture Driven Resource Management”. In: *31st Annual ACM Symposium on Applied Computing (SAC’16)*. 2016. URL: http://hdl.handle.net/10993/26860.

[170] C. GREVISSE. “Adaptive Literacy-Aware Integration of Learning Material”. In: *UMAP 2016 Extended Proceedings*. 2016. URL: http://hdl.handle.net/10993/27846.

[171] N. GUELFI, B. JAHIC, and B. RIES. “TESMA : Towards the Development of a Tool for Specification, Management and Assessment of Teaching Programs”. In: *Proceeding of the 2nd International Conference on Applications in Information Technology*. The University of Aizu Press, 2016, pp. 5–8. ISBN: 978-4-900721-04-3. URL: http://hdl.handle.net/10993/28607.

[172] I. HAJRI. “Supporting Change in Product Lines within the Context of Use Case-Driven Development and Testing”. In: *24th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (DS@FSE 2016)*. 2016. URL: http://hdl.handle.net/10993/28260.

[173] I. HAJRI, A. GÖKNIL, L. BRIAND, and T. Stephany. “PUMConf: A Tool to Configure Product Specific Use Case and Domain Models in a Product Line”. In: *24th ACM SIGSOFT International Symposium on the Foundations of Software Engineering*. 2016. URL: http://hdl.handle.net/10993/28261.

[174] S. Hamadi, K. Blaiech, P. VALTCHEV, O. Cherkaoui, and R. STATE. “Compiling packet forwarding rules for switch pipelined architecture”. In: *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*. 2016. URL: http://hdl.handle.net/10993/28415.

[175] T. HARTMANN, A. MOAWAD, F. FOUQUET, Y. Reckinger, J. KLEIN, and Y. L. TRAON. “Near Real-Time Electric Load Approximation in Low Voltage Cables of Smart Grids with Models@run.time”. In: *31st Annual ACM Symposium on Applied Computing (SAC’16)*. 2016, pp. 2119–2126. URL: http://hdl.handle.net/10993/27073.

[176] A. Hefnawy, T. Elhariri, A. Bouras, C. Cherifi, J. ROBERT, S. KUBLER, and K. Främling. “Lifecycle Management in the Smart City Context: Smart Parking Use-Case”. In: *13th IFIP International Conference on Product Lifecycle Management, Columbia SC 10-13 July 2016*. Springer, 2016. URL: http://hdl.handle.net/10993/28166.

[177] R. B. A. (HELALI), S. NEJATI, L. BRIAND, and T. Stifter. “Testing Advanced Driver Assistance Systems using Multi-objective Search and Neural Networks”. In: *International Conference on Automated Software Engineering (ASE 2016)*. ACM, 2016, pp. 63–74. DOI: 10.1145/2970276.2970311. URL: http://hdl.handle.net/10993/28071.

[178] C. HENARD, M. PAPADAKIS, M. Harman, Y. Jia, and Y. L. TRAON. “Comparing White-box and Black-box Test Prioritization”. In: *38th International Conference on Software Engineering (ICSE'16)*. 2016. URL: http://hdl.handle.net/10993/25175.

[179] P. V. Hertum, M. CRAMER, B. Bogaerts, and M. Denecker. “Distributed Autoepistemic Logic and its Application to Access Control”. In: *Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence*. 2016, pp. 1286–1292. URL: http://hdl.handle.net/10993/30187.

[180] W. HÖHN. “Georeferencing, Annotation, and Analysis Tools for Old Maps: an overview”. In: *Proceedings International Workshop Exploring Old Maps 2016*. 2016. URL: http://hdl.handle.net/10993/29411.

[181] M. HURIER, K. ALLIX, T. F. d. A. BISSYANDE, J. KLEIN, and Y. L. TRAON. “On the Lack of Consensus in Anti-Virus Decisions: Metrics and Insights on Building Ground Truths of Android Malware”. In: *Detection of Intrusions and Malware, and Vulnerability Assessment - 13th International Conference*. Springer, 2016, pp. 142–162. ISBN: 978-3-319-40666-4. DOI: 10.1007/978-3-319-40667-1_8. URL: http://hdl.handle.net/10993/27845.

[182] A. A. Z. A. IBRAHIM, P. BOUVRY, D. KLIAZOVICH, and A. OLEKSIAK. “Virtual Desktop Infrastructures: architecture, survey and green aspects proof of concept”. In: *7th INTERNATIONAL GREEN and SUSTAINABLE COMPUTING CONFERENCE (1st RE-HPC workshop), Hangzhou, China (November 2016)*. 2016. URL: http://hdl.handle.net/10993/28844.

[183] A. A. Z. A. IBRAHIM, D. KLIAZOVICH, and P. BOUVRY. “On Service Level Agreement Assurance in Cloud Computing Data Centers”. In: *IEEE 9th International Conference on Cloud Computing (CLOUD), San Francisco, USA (June 2016)*. 2016, pp. 921–926. DOI: 10.1109/CLOUD.2016.135. URL: http://hdl.handle.net/10993/27945.

[184] A. A. Z. A. IBRAHIM, D. KLIAZOVICH, and P. BOUVRY. “Service Level Agreemnet Assurance between Cloud Services Providers and CLoud Customers”. In: *Proceedings of 16th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing CCGrid 2016*. IEEE Computer Society, 2016, pp. 588–591. ISBN: 978-1-5090-2453-7. DOI: 10.1109/CCGrid.2016.56. URL: http://hdl.handle.net/10993/27390.

[185] A. A. Z. A. IBRAHIM, D. KLIAZOVICH, P. BOUVRY, and A. OLEKSIAK. “Using Virtual Desktop Infrastructure to Improve Power Efficiency in Grinfy System”. In: *IEEE 8th International Conference on Cloud Computing Technology and Science(CloudCom), Luxembourg 2016*. 2016, pp. 85–89. DOI: 10.1109/CloudCom.2016.25. URL: http://hdl.handle.net/10993/29123.

[186] V. IOVINO, Q. TANG, and K. Zebrowski. “On the power of Public-key Function-Private Functional Encryption”. In: *15th International Conference on Cryptology and Network Security*. Springer Seciurity and Cryptology, 2016. ISBN: 978-3-319-48964-3. DOI: 10.1007/978-3-319-48965-0. URL: http://hdl.handle.net/10993/28648.

[187] W. Jamroga and M. TABATABAEI. “Information Security as Strategic (In)effectivity”. In: *12th International Workshop on Security and Trust Management (STM), 2016.* 2016. URL: http://hdl.handle.net/10993/29312.

[188] W. Jamroga and M. TABATABAEI. “Preventing Coercion in E-Voting: Be Open and Commit”. In: *Proceedings of the 12th International Joint Conference on Electronic Voting (E-Vote-ID)*. 2016. URL: http://hdl.handle.net/10993/29251.

[189] R. JHAWAR, K. LOUNIS, and S. MAUW. “A Stochastic Framework for Quantitative Analysis of Attack-Defense Trees”. In: *12th International Workshop on Security and Trust Management*. 2016. URL: http://hdl.handle.net/10993/29397.

[190] R. JHAWAR, S. Mauw, and I. Zakiuddin. “Automating Cyber Defense Response Using Attack-Defence Trees and Game Theory”. In: *The 15th European Conference on Cyber Warfare and Security*. 2016, pp. 163–172. URL: http://hdl.handle.net/10993/29847.

[191] M. JIMENEZ, M. PAPADAKIS, T. F. d. A. BISSYANDE, and J. KLEIN. “Profiling Android Vulnerabilities”. In: *2016 IEEE International Conference on Software Quality, Reliability and Security (QRS 2016)*. IEEE Computer Society, 2016, pp. 222–229. ISBN: 978-1-5090-4127-5. DOI: 10.1109/QRS.2016.34. URL: http://hdl.handle.net/10993/28093.

[192] M. JIMENEZ, M. PAPADAKIS, and Y. L. TRAON. “An Empirical Analysis of Vulnerabilities in OpenSSL and the Linux Kernel”. In: *2016 Asia-Pacific Software Engineering Conference (APSEC)*. 2016. URL: http://hdl.handle.net/10993/28628.

[193] M. JIMENEZ, M. PAPADAKIS, and Y. L. TRAON. “Vulnerability Prediction Models: A case study on the Linux Kernel”. In: *16th IEEE International Working Conference on Source Code Analysis and Manipulation, SCAM 2016, Raleigh, US, October 2-3, 2016*. 2016. DOI: 10.1109/SCAM.2016.15. URL: http://hdl.handle.net/10993/28259.

[194] E. KIEFFER, G. DANOY, P. BOUVRY, and A. Nagih. “Co-evolutionary approach based on constraint decomposition”. In: *Co-evolutionary approach based on constraint decomposition*. 2016. URL: http://hdl.handle.net/10993/28914.

[195] E. KIEFFER, G. DANOY, P. BOUVRY, and A. Nagih. “Hybrid mobility model with pheromones for UAV detection task”. In: *Hybrid mobility model with pheromones for UAV detection task*. 2016. DOI: 10.1109/SSCI.2016.7850104. URL: http://hdl.handle.net/10993/30387.

[196] E. KIEFFER, M. GUZEK, G. DANOY, P. BOUVRY, and A. Nagih. “A Novel Co-evolutionary Approach for Constrained Genetic Algorithms”. In: *Proceedings of the 2016 on Genetic and Evolutionary Computation Conference Companion*. ACM, 2016, pp. 47–48. ISBN: 978-1-4503-4323-7. DOI: 10.1145/2908961.2908969. URL: http://hdl.handle.net/10993/28196.

[197] M. KINTIS, M. PAPADAKIS, A. Papadopoulos, E. Valvis, and N. Malevris. “Analysing and Comparing the Effectiveness of Mutation Testing Tools: A Manual Study”. In: *International Working Conference on Source Code Analysis and Manipulation (SCAM'16)*. 2016. URL: http://hdl.handle.net/10993/28929.

[198] N. KOLBE, A. Zaslavsky, S. KUBLER, and J. ROBERT. “Reasoning over Knowledge-based Generation of Situations in Context Spaces to Reduce Food Waste”. In: *Reasoning over Knowledge-based Generation of Situations in Context Spaces to Reduce Food Waste*. Springer, 2016. URL: http://hdl.handle.net/10993/28567.

[199] S. KUBLER, A. Buda, J. ROBERT, and K. Främling. “Building Lifecycle Management System for Enhanced Closed Loop Collaboration”. In: *13th IFIP International Conference on Product Lifecycle Management (PLM16)*. Springer, 2016. URL: http://hdl.handle.net/10993/28080.

[200] S. KUBLER, J. ROBERT, A. Hefnawy, C. Cherifi, A. Bouras, and K. Främling. “IoT-based Smart Parking System for Sporting Event Management”. In: *Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. ACM New York, 2016, pp. 104–114. ISBN: 978-1-4503-4750-1. DOI: 10.1145/2994374.2994390. URL: http://hdl.handle.net/10993/29742.

[201] S. KUBLER, J. ROBERT, Y. L. TRAON, J. Umbrich, and S. Neumaier. “Open Data Portal Quality Comparison using AHP”. In: *Proceedings of the 17th International Digital Government Research Conference on Digital Government Research*. ACM, 2016, pp. 397–407. ISBN: 978-1-4503-4339-8. DOI: 10.1145/2912160.2912167. URL: http://hdl.handle.net/10993/27952.

[202] J. LANCRENON. “On Password-Authenticated Key Exchange Security Modeling”. In: *Technology and practice of passwords: 9th International Conference, PASSWORDS 2015, Cambridge, UK, December 7-9, 2015, Proceedings*. Springer, 2016. ISBN: 978-3-319-29937-2. URL: http://hdl.handle.net/10993/25745.

[203] G. LENZINI, S. MAUW, and S. OUCHANI. “Analysing the Efficacy of Security Policies in Cyber-Physical Socio-Technical Systems”. In: *Security and Trust Management - STM 2016*. Springer-Verlag, 2016. URL: http://hdl.handle.net/10993/28328.

[204] L. I. Li. “Boosting Static Analysis of Android Apps through Code Instrumentation”. In: *The Doctoral Symposium of 38th International Conference on Software Engineering (ICSE-DS 2016)*. 2016. URL: http://hdl.handle.net/10993/26823.

[205] L. I. Li, T. F. d. A. BISSYANDE, J. KLEIN, and Y. L. TRAON. “An Investigation into the Use of Common Libraries in Android Apps”. In: *The 23rd IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER 2016)*. 2016, p. 12. URL: http://hdl.handle.net/10993/26634.

[206] L. I. Li, T. F. d. A. BISSYANDE, J. KLEIN, and Y. L. TRAON. “Parameter Values of Android APIs: A Preliminary Study on 100,000 Apps”. In: *The 23rd IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER 2016)*. 2016, p. 5. URL: http://hdl.handle.net/10993/26633.

[207] L. I. Li, T. F. d. A. BISSYANDE, D. Octeau, and J. KLEIN. “DroidRA: Taming Reflection to Support Whole-Program Analysis of Android Apps”. In: *The 2016 International Symposium on Software Testing and Analysis*. 2016. URL: http://hdl.handle.net/10993/27761.

[208] L. I. Li, T. F. d. A. BISSYANDE, D. Octeau, and J. KLEIN. “Reflection-Aware Static Analysis of Android Apps”. In: *The 31st IEEE/ACM International Conference on Automated Software (ASE)*. 2016, p. 6. URL: http://hdl.handle.net/10993/28287.

[209] L. I. Li, T. F. d. A. BISSYANDE, Y. L. TRAON, and J. KLEIN. “Accessing Inaccessible Android APIs: An Empirical Study”. In: *The 32nd International Conference on Software Maintenance and Evolution (ICSME)*. 2016, p. 12. URL: http://hdl.handle.net/10993/28304.

[210] L. I. Li, L. I. Daoyuan, A. Bartel, T. F. d. A. BISSYANDE, J. KLEIN, and Y. L. TRAON. “Towards a Generic Framework for Automating Extensive Analysis of Android Applications”. In: *The 31st ACM/SIGAPP Symposium on Applied Computing (SAC 2016)*. 2016. URL: http://hdl.handle.net/10993/26632.

[211] L. I. Li, J. MARTINEZ, T. Ziadi, T. F. d. A. BISSYANDE, J. KLEIN, and Y. L. TRAON. “Mining Families of Android Applications for Extractive SPL Adoption”. In: *The 20th International Systems and Software Product Line Conference (SPLC 2016)*. 2016. URL: http://hdl.handle.net/10993/27764.

[212] Y. Li, K. Duan, L. Lv, J. PANG, and S. Cai. “A novel approach to parameterized verification of cache coherence protocols”. In: *Proceedings of the 34th IEEE International Conference on Computer Design*. IEEE Computer Society, 2016, pp. 560–567. URL: http://hdl.handle.net/10993/29070.

[213] B. Liao, N. Oren, L. V. D. TORRE, and S. Villata. “Prioritized Norms and Defaults in Formal Argumentation”. In: *Deontic Logic and Normative Systems (2016)*. 2016. URL: http://hdl.handle.net/10993/30765.

[214] A. C. LIMA, F. ROCHA, M. VOLP, and P. E. VERISSIMO. “Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems”. In: *Proceedings of the Second ACM Workshop on Cyber-Physical Systems Security and PrivaCy*. 2016. ISBN: 978-1-4503-4568-X. DOI: 10.1145/2994487.2994489. URL: http://hdl.handle.net/10993/28773.

[215] D. U. Manxing, R. STATE, M. Brorsson, and T. Avanesov. “Behavior Profiling for Mobile Advertising”. In: *Proceedings of the 3rd IEEE/ACM International Conference on Big Data Computing, Applications and Technologies*. ACM, 2016, pp. 302–307. ISBN: 9781450346177. URL: http://hdl.handle.net/10993/29373.

[216] J. MARTINEZ, T. Ziadi, T. F. d. A. BISSYANDE, J. KLEIN, and Y. L. TRAON. “Name Suggestions during Feature Identification: The VariClouds Approach”. In: *20th International Systems and Software Product Line Conference (SPLC 2016) proceedings*. 2016. URL: http://hdl.handle.net/10993/27766.

[217] J. MARTINEZ, T. Ziadi, M. PAPADAKIS, T. F. d. A. BISSYANDE, J. KLEIN, and Y. L. TRAON. “Feature Location Benchmark for Software Families using Eclipse Community Releases”. In: *Software Reuse: Bridging with Social-Awareness, ICSR 2016 Proceedings*. 2016. URL: http://hdl.handle.net/10993/27765.

[218] R. MATINNEJAD, S. NEJATI, L. BRIAND, and T. Bruckamnn. “SimCoTest: A Test Suite Generation Tool for Simulink/Stateflow Controllers”. In: *Proceedings of the 38th International Conference on Software Engineering* (2016). URL: http://hdl.handle.net/10993/23828.

[219] R. MATINNEJAD, S. NEJATI, L. BRIAND, and t. Bruckmann. “Automated Test Suite Generation for Time-Continuous Simulink Models”. In: *proceedings of the 38th International Conference on Software Engineering* (2016). URL: http://hdl.handle.net/10993/23411.

[220] S. MAUW, J. L. T. POZO, and R. T. RASUA. “A Class of Precomputation-based Distance-bounding Protocols”. In: *1st IEEE European Symposium on SECURITY and PRIVACY*. 2016. DOI: 10.1109/EuroS&P.2016.19. URL: http://hdl.handle.net/10993/28202.

[221] S. MAUW, R. T. RASUA, and B. Xuan. “Counteracting active attacks in social network graphs”. In: *Proceedings of Data and Applications Security and Privacy - 30th Annual IFIP WG 11.3 Conference (DBSec 2016)*. Springer, 2016, pp. 233–248. URL: http://hdl.handle.net/10993/28978.

[222] J. A. MEIRA, E. C. de Almeira, K. I. M. Dongsun, E. R. L. Filho, and Y. L. TRAON. ““Overloaded!” — A Model-based Approach to Database Stress Testing”. In: *International Conference on Database and Expert Systems Applications, Porto 5-8 September 2016*. 2016. URL: http://hdl.handle.net/10993/28616.

[223] A. MIZERA, J. PANG, and Q. YUAN. “ASSA-PBN 2.0: A software tool for probabilistic Boolean networks.” In: *Proceedings of 14th International Conference on Computational Methods in Systems Biology*. Springer, 2016, pp. 309–315. URL: http://hdl.handle.net/10993/28350.

[224] A. MIZERA, J. PANG, and Q. YUAN. “Fast simulation of probabilistic Boolean networks.” In: *Proceedings of 14th International Conference on Computational Methods in Systems Biology*. Springer, 2016, pp. 216–231. URL: http://hdl.handle.net/10993/28349.

[225] A. MIZERA, J. PANG, and Q. YUAN. “Parallel Approximate Steady-state Analysis of Large Probabilistic Boolean Networks”. In: *Proceedings of the 31st ACM Symposium on Applied Computing*. ACM, 2016. URL: http://hdl.handle.net/10993/25935.

[226] J. MUSZYNSKI, S. VARRETTE, and P. BOUVRY. “Reducing Efficiency of Connectivity-Splitting Attack on Newscast via Limited Gossip”. In: *Proc. of the 19th European Event on Bio-Inspired Computation, EvoCOMNET 2016*. Springer Verlag, 2016. URL: http://hdl.handle.net/10993/23759.

[227] R. Muthuri, G. Boella, J. Hulstijn, and L. HUMPHREYS. “Argumentation-Based Legal Requirements Engineering: The Role of Legal Interpretation in Requirements Acquisition”. In: *Requirements Engineering Conference Workshops (REW), IEEE International*. 2016. DOI: 10.1109/REW.2016.048. URL: http://hdl.handle.net/10993/31072.

[228] N. NAVET and L. Fejoz. “CPAL: High-Level Abstractions for Safe Embedded Systems”. In: *DSM 2016: Proceedings of the International Workshop on Domain-Specific Modeling*. ACM, 2016, pp. 35–41. ISBN: 978-1-4503-4894-2. URL: http://hdl.handle.net/10993/30019.

[229] S. NEJATI, M. SABETZADEH, C. ARORA, L. BRIAND, and F. Mandoux. “Automated Change Impact Analysis between SysML Models of Requirements and Design”. In: *24th ACM SIGSOFT International Symposium on the Foundations of Software Engineering, Seattle 13-18 November 2016*. 2016. URL: http://hdl.handle.net/10993/28046.

[230] M. Ni, Y. Zhang, W. Han, and J. PANG. “An Empirical Study on User Access Control in Online Social Networks”. In: *Proceedings of the 21st ACM Symposium on Access Control Models and Technologies (SACMAT’16)*. ACM, 2016, pp. 13–23. DOI: 10.1145/2914642.2914644. URL: http://hdl.handle.net/10993/27677.

[231] S. S. NIELSEN, C. F. Torres, G. DANOY, and P. BOUVRY. “Tackling the IFP Problem with the Preference-Based Genetic Algorithm”. In: *Proceedings of the Genetic and Evolutionary Computation Conference 2016*. ACM, 2016, pp. 965–972. ISBN: 978-1-4503-4206-3. DOI: 10.1145/2908812.2908954. URL: http://hdl.handle.net/10993/28197.

[232] D. Octeau, S. Jha, M. Dering, P. McDaniel, A. Bartel, L. I. Li, J. KLEIN, and Y. L. TRAON. “Combining Static Analysis with Probabilistic Models to Enable Market-Scale Android Inter-component Analysis”. In: *The 43rd Symposium on Principles of Programming Languages (POPL 2016)*. 2016. URL: http://hdl.handle.net/10993/26631.

[233] A. PANCHENKO, F. LANZE, A. Zinnen, M. Henze, J. Pennekamp, K. Wehrle, and T. ENGEL. “Website Fingerprinting at Internet Scale”. In: *Proceedings of the 23rd Internet Society (ISOC) Network and Distributed System Security Symposium (NDSS 2016)*. 2016. URL: http://hdl.handle.net/10993/24117.

[234] J. PANG, P. Zablotskaia, and Y. Zhang. “On impact of weather on human mobility in cities”. In: *Proceedings of the 17th International Conference on Web Information System Engineering*. Springer Science & Business Media B.V., 2016, pp. 247–256. URL: http://hdl.handle.net/10993/29071.

[235] M. PAPADAKIS, C. Henard, M. Harman, Jia, and Y. L. TRAON. “Threats to the validity of mutation-based test assessment”. In: *International Symposium on Software Testing and Analysis, ISSTA 2016*. 2016. URL: http://hdl.handle.net/10993/28927.

[236] I. Pecci, B. Martin, I. Kacem, I. Maamria, S. FAYE, N. LOUVETON, G. GHEORGHE, and T. ENGEL. “Not a Tile Out of Place: Toward Creating Context-Dependent User Interfaces on Smartglasses”. In: *Proceedings of the 9th International Conference on Human System Interaction (HSI’16)*. 2016. URL: http://hdl.handle.net/10993/27384.

[237] L. P. PERRIN and A. UDOVENKO. “Algebraic Insights into the Secret Feistel Network”. In: *Fast Software Encryption - 23rd International Workshop, FSE 2016, Bochum, March 20-23, 2016*. Springer-Verlag Berlin Heidelberg, 2016, pp. 378–398. ISBN: 978-3-662-52992-8. URL: http://hdl.handle.net/10993/26935.

[238] L. P. PERRIN, A. UDOVENKO, and A. BIRYUKOV. “Cryptanalysis of a Theorem: Decomposing the Only Known Solution to the Big APN Problem”. In: *Advances in Cryptology – CRYPTO 2016*. Springer Berlin Heidelberg, 2016, pp. 93–122. ISBN: 978-3-662-53007-8. DOI: 10.1007/978-3-662-53008-5_4. URL: http://hdl.handle.net/10993/28414.

[239] A. POPLETEEV. “HIPS: Human-based indoor positioning system”. In: *Proceedings of the 7th International Conference on Indoor Positioning and Indoor Navigation (IPIN-2016)*. 2016. URL: http://hdl.handle.net/10993/29079.

[240] A. POPLETEEV. “Indoor positioning and floor plan based ground truth: Can you really click where you are?” In: *15th International Conference on Mobile and Ubiquitious Multimedia (MUM-2016)*. 2016. DOI: 10.1145/3012709.3012737. URL: http://hdl.handle.net/10993/29186.

[241] A. POPLETEEV. “Indoor positioning using ambient radio signals: Data acquisition platform for a long-term study”. In: *Proceedings of the IEEE 13th Workshop on Positioning, Navigation and Communications (WPNC-2016)*. IEEE, 2016. URL: http://hdl.handle.net/10993/29080.

[242] A. POPLETEEV, H. Arshadaghghaleh, and V. Lutkovski. “Small-scale positioning using digital compasses”. In: *International Congress on Computer Science: Information Systems and Technologies (CSIST-2016)*. BSU, 2016. URL: http://hdl.handle.net/10993/29082.

[243] M. Pouryazdan, C. FIANDRINO, B. Kantarci, D. KLIAZOVICH, T. Soyata, and P. BOUVRY. “Game-Theoretic Recruitment of Sensing Service Providers for Trustworthy Cloud-Centric Internet-of-Things (IoT) Applications”. In: *IEEE Global Communications Conference (GLOBECOM) Workshops: Fifth International Workshop on Cloud Computing Systems, Networks, and Applications (CCSNA)*. 2016. URL: http://hdl.handle.net/10993/28587.

[244] M. A. Qin and S. de Kinderen. “Goal-Based Decision Making Using Goal-Oriented Problem Structuring and Evaluation Visualization for Multi Criteria Decision Analysis”. In: *Lecture Notes in Computer Science (LNCS) 9619*. 2016. URL: http://hdl.handle.net/10993/30398.

[245] G. Rens, T. Meyer, and G. CASINI. “On Revision of Partially Specified Convex Probabilistic Belief Bases”. In: *Proceedings of the 22nd European Conference on Artificial Intelligence (ECAI-16)*. 2016. ISBN: 978-1-61499-671-2. URL: http://hdl.handle.net/10993/30950.

[246] G. Rens, T. Meyer, and G. CASINI. “Revising Incompletely Specified Convex Probabilistic Belief Bases”. In: *Proceedings of the 16th International Workshop on Non-Monotonic Reasoning (NMR 2016)*. Technische Universität Dortmund, 2016, pp. 133–142. URL: http://hdl.handle.net/10993/30343.

[247] G. Rizzo, M. R. PALATTELLA, T. Braun, and T. ENGEL. “Content and Context Aware Strategies for QoS Support in VANETs”. In: *Proc. of Int. Conf. on Advanced Information Networking and Applications (AINA-2016)*. 2016. URL: http://hdl.handle.net/10993/24638.

[248] L. ROBALDO and S. U. N. Xin. “Reified Input/Output logic - a position paper”. In: *proceedings of Workshop on Artificial Intelligence for Justice (AI4J), collocated at the 22nd European Conference on Artificial Intelligence (ECAI 2016)* (2016). URL: http://hdl.handle.net/10993/29525.

[249] J. ROBERT, S. KUBLER, and Y. L. TRAON. “Micro-billing framework for IoT: Research & Technological foundations”. In: *International Conference on Future Internet of Things and Cloud, 22-24 August 2016, Vienna, Austria*. 2016. URL: http://hdl.handle.net/10993/28314.

[250] J. ROBERT, S. KUBLER, Y. L. TRAON, and K. Främling. “O-MI/O-DF Standards as Interoperability Enablers for Industrial Internet: a Performance Analysis”. In: *O-MI/O-DF Standards as Interoperability Enablers for Industrial Internet: a Performance Analysis*. 2016. URL: http://hdl.handle.net/10993/28313.

[251] M. ROSALIE, G. DANOY, P. BOUVRY, and S. Chaumette. “UAV Multilevel Swarms for Situation Management”. In: *Proceedings of the 2Nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*. ACM, 2016, pp. 49–52. ISBN: 978-1-4503-4405-0. DOI: 10.1145/2935620.2935631. URL: http://hdl.handle.net/10993/27794.

[252] M. ROSALIE, G. DANOY, S. Chaumette, and P. BOUVRY. “From Random Process to Chaotic Behavior in Swarms of UAVs”. In: *DIVANet ’16 Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications*. ACM, 2016, pp. 9–15. ISBN: 978-1-4503-4506-4. DOI: 10.1145/2989275.2989281. URL: http://hdl.handle.net/10993/28921.

[253] P. Ruiu, A. Bianco, C. FIANDRINO, P. Giaccone, and D. KLIAZOVICH. “Power Comparison of Cloud Data Center Architectures”. In: *IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 2016*. 2016. URL: http://hdl.handle.net/10993/24606.

[254] J. A. N. Sadeeq, D. C. NGUYEN, and L. BRIAND. “Automated and Effective Testing of Web Services for XML Injection Attacks”. In: *ISSTA’16-The International Symposium on Software Testing and Analysis, Saarbrücken 18-20 July 2016*. 2016, pp. 12–23. URL: http://hdl.handle.net/10993/27070.

[255] N. SANNIER, M. Adedjouma, M. SABETZADEH, and L. BRIAND. "Automated Classification of Legal Cross References Based on Semantic Intent". In: *22nd International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ'16)*. 2016. URL: http://hdl.handle.net/10993/23176.

[256] C. Santos, V. R. Doncel, P. Casanovas, and L. V. D. TORRE. "Modeling relevant legal information for consumer disputes". In: *EGOVIS 2016: Electronic Government and the Information Systems Perspective*. Springer, 2016, pp. 150–165. URL: http://hdl.handle.net/10993/30681.

[257] C. Santos, C. Pruski, M. d. Silveira, V. Rodriguez-Doncel, A. Gangemi, L. V. D. TORRE, and P. Casanovas. "Complaint Ontology Pattern - COP". In: *Workshop on Ontology and Semantic Web Patterns, Kobe 18 October 2016*. 2016. URL: http://hdl.handle.net/10993/30682.

[258] A. Sciarrone, C. FIANDRINO, I. Bisio, F. Lavagetto, D. KLIAZOVICH, and P. BOUVRY. "Smart Probabilistic Fingerprinting for Indoor Localization over Fog Computing Platforms". In: *IEEE 5th International Conference on Cloud Networking (CloudNet), Pisa, Italy*. 2016. URL: http://hdl.handle.net/10993/28039.

[259] S. SIGNORELLO, M. R. PALATTELLA, and L. A. Grieco. "Security Challenges in future NDN-Enabled VANETs". In: *In the Proceedings of the 3rd International Workshop on the Emerging Future Internet and Network Security (EFINS 2016) - IEEE TrustCom-16*. 2016. URL: http://hdl.handle.net/10993/28387.

[260] M. SKROBOT, J. LANCRENON, and Q. TANG. "Two More Efficient Variants of the J-PAKE Protocol". In: *ACNS 2016*. 2016. ISBN: 978-3-319-39555-5. URL: http://hdl.handle.net/10993/26452.

[261] G. SOLTANA, M. SABETZADEH, and L. BRIAND. "Model-Based Simulation of Legal Requirements: Experience from Tax Policy Simulation". In: *24th IEEE International Requirements Engineering Conference, Beijing 12-16 September 2016*. 2016. URL: http://hdl.handle.net/10993/27798.

[262] R. Soua, E. Kalogeiton, G. Manzo, J. M. Duarte, M. R. PALATTELLA, A. D. MAIO, T. Braun, T. ENGEL, L. A. Villas, and G. A. Rizzo. "SDN coordination for CCN and FC content dissemination in VANETs". In: *Proceedings of the 8th International Conference on Ad Hoc Networks (ADHOCNETS), Ottawa, ON, Canada*. Springer, 2016, pp. 26–27. URL: http://hdl.handle.net/10993/29094.

[263] D. P. B. SPAGNUELO, C. BARTOLINI, and G. LENZINI. "Metrics for Transparency". In: *Proceedings of DPM 2016 and QASA 2016*. 2016. URL: http://hdl.handle.net/10993/28240.

[264] S. M. SUNDHARAM, S. ALTMEYER, and N. NAVET. "Poster Abstract: An Optimizing Framework for Real-Time Scheduling". In: *Proceedings of 22nd IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS 2016)*. 2016. URL: http://hdl.handle.net/10993/24827.

[265] S. M. SUNDHARAM, S. Altmeyer, and N. NAVET. “Model Interpretation for an AUTOSAR compliant Engine Control Function”. In: *7th International Workshop on Analysis Tools and Methodologies for Embedded and Real-time Systems (WATERS)*. 2016. URL: http://hdl.handle.net/10993/27711.

[266] S. M. SUNDHARAM, L. Fejoz, and N. NAVET. “Connected Motorized Riders - A Smart Mobility System to Connect Two and Three-wheelers”. In: *Proceedings of 6th Intentional Symposium on Embedded computing & system Design (ISED 2016)*. 2016. URL: http://hdl.handle.net/10993/29400.

[267] S. M. SUNDHARAM, L. Havet, S. Altmeyer, and N. NAVET. “A Model-Based Development Environment for Rapid-Prototyping of Latency-Sensitive Automotive Control Software”. In: *Proceedings of 6th Intentional Symposium on Embedded computing & system Design (ISED 2016)*. 2016. URL: http://hdl.handle.net/10993/28774.

[268] M. TABATABAEI, W. Jamroga, and P. Y. A. RYAN. “Expressing Receipt-Freeness and Coercion-Resistance in Logics of Strategic Ability: Preliminary Attempt”. In: *The International Workshop on AI for Privacy and Security (PrAISe), 2016*. 2016. URL: http://hdl.handle.net/10993/29250.

[269] Q. Tang and J. WANG. “Privacy-preserving Friendship-based Recommender Systems”. In: *IEEE Transactions on Dependable and Secure Computing* (2016). URL: http://hdl.handle.net/10993/29366.

[270] L. V. D. TORRE. “Norms and Arguments”. In: *Proceedings of the 1st Chinese Conference on Logic and Argumentation (CLAR 2016), Hangzhou, China, April 2-3, 2016*. 2016. URL: http://hdl.handle.net/10993/31153.

[271] C. F. Torres and R. T. RASUA. “The Fréchet/Manhattan distance and the trajectory anonymisation problem”. In: *Proceedings of Data and Applications Security and Privacy - 30th Annual IFIP WG 11.3 Conference (DBSec 2016)*. Springer, 2016. URL: http://hdl.handle.net/10993/28770.

[272] M. Tricoire, O. Barais, M. Leduc, J. Bourcier, F. FOUQUET, G. NAIN, L. MOULINE, G. Sunyé, and B. Morin. “KevoreeJS: Enabling dynamic software reconfigurations in the Browser”. In: *WICSA/CompArch 2016 Proceedings*. 2016. URL: http://hdl.handle.net/10993/26822.

[273] J. M. P. URQUIDI, J. LANCRENON, D. Khader, and L. Chen. “Attribute-Based Signatures with Controllable Linkability”. In: *Trusted Systems: 7th International Conference, INTRUST 2015, Beijing, China, December 7-8, 2015, Revised Selected Papers*. Springer, 2016, pp. 114–129. ISBN: 978-3-319-31549-2. URL: http://hdl.handle.net/10993/26453.

[274] Z. E. E. M. VAN, F. Bex, and S. Ghanavati. “RationalGRL: A Framework for Rationalizing Goal Models Using Argument Diagrams”. In: *35th International Conference on Conceptual Modeling (ER’2016)*. 2016. URL: http://hdl.handle.net/10993/29393.

[275] Z. E. E. M. VAN and D. DODER. “AGM-Style Revision of Beliefs and Intentions”. In: *Proceedings of the 22nd European Conference on Artificial Intelligence (ECAI’16)*. 2016. URL: http://hdl.handle.net/10993/29389.

[276] Z. E. E. M. VAN and D. DODER. “AGM-Style Revision of Beliefs and Intentions from a Database Perspective (Preliminary Version)”. In: *Proceedings of the 16th International Workshop on Non-Monotonic Reasoning*. 2016. URL: http://hdl.handle.net/10993/29392.

[277] Z. E. E. M. VAN, D. Marosin, F. Bex, and S. Ghanavati. “The RationalGRL toolset for Goal Models and Argument Diagrams”. In: *Proceedings of the 6th International Conference on Computational Models of Argument (COMMA'16)*. 2016. URL: http://hdl.handle.net/10993/29390.

[278] J. WANG and Q. Tang. “A Probabilistic View of Neighborhood-based Recommendation Methods”. In: *ICDM 2016 - IEEE International Conference on Data Mining series (ICDM) workshop CLOUDMINE*. 2016. URL: http://hdl.handle.net/10993/29142.

[279] S. U. N. Xin and L. ROBALDO. “Norm Creation in Proposition Control Games”. In: *Proceedings of the 1st Chinese Conference on Logic and Argumentation (CLAR 2016), Hangzhou, China, April 2-3, 2016*. 2016. URL: http://hdl.handle.net/10993/31055.

[280] Y. Zhauniarovich and O. GADYATSKAYA. “Small changes, big changes: an updated view on the Android permission system”. In: *Research in Attacks, Intrusions, and Defenses - 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings*. Springer, 2016, pp. 346–367. ISBN: 978-3-319-45718-5. DOI: 10.1007/978-3-319-45719-2_16. URL: http://hdl.handle.net/10993/28908.

[281] L. I. U. Zhe, J. GROSZSCHÄDL, L. Li, and Q. Xu. “Energy-Efficient Elliptic Curve Cryptography for MSP430-Based Wireless Sensor Nodes”. In: *Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I*. Springer Verlag, 2016, pp. 94–112. DOI: 10.1007/978-3-319-40253-6_6. URL: http://hdl.handle.net/10993/27841.

[282] L. ZHOU, Y. Zhang, J. PANG, and C.-T. Li. “Modeling city locations as complex networks: An initial study”. In: *Proceedings of the 5th International Workshop on Complex Networks and their Applications*. Springer Science & Business Media B.V., 2016, pp. 735–747. URL: http://hdl.handle.net/10993/29072.

A.6 Technical Report

[283] S. ALTMEYER, S. M. SUNDHARAM, and N. NAVET. *The Case for FIFO Real-Time Scheduling*. University of Luxembourg > Faculty of Science, Technology, Communication (FSTC) > Computer Science, and Communications Research Unit (CSC), 2016. URL: http://hdl.handle.net/10993/24935.

[284] D. A. AMBROSSIO, X. PARENT, and L. V. D. TORRE. *A Representation Theorem for Abstract Cumulative Aggregation*. University of Luxembourg > Interdisciplinary Centre for Security, Reliability et al., 2016. URL: http://hdl.handle.net/10993/27364.

[285] D. APPELT, D. C. NGUYEN, and L. BRIAND. *Automated Testing of Web Application Firewalls*. University of Luxembourg > Interdisciplinary Centre for Security, Reliability and Trust (SNT), 2016. URL: http://hdl.handle.net/10993/26231.

[286] L. I. Daoyuan, L. I. Li, K. I. M. Dongsun, T. F. d. A. BISSYANDE, D. Lo, and Y. L. TRAON. *Watch out for This Commit! A Study of Influential Software Changes*. University of Luxembourg > Interdisciplinary Centre for Security, Reliability et al., 2016. URL: http://hdl.handle.net/10993/27742.

[287] A. B. FADHEL, D. BIANCULLI, and L. BRIAND. *GemRBAC-DSL: a High-level Specification Language for Role-based Access Control Policies*. University of Luxembourg > Interdisciplinary Centre for Security, Reliability and Trust (SNT), 2016. URL: http://hdl.handle.net/10993/27171.

[288] M. Haus, K. A. A. E.-S. EMARA, and J. Ott. *Privacy-Preserving Proximity Services*. University of Luxembourg > Interdisciplinary Centre for Security, Reliability and Trust (SNT), 2016. DOI: 10.14459/2016md1324021. URL: http://hdl.handle.net/10993/29096.

[289] B. JAHIC. *TESMA : Requirements, Design and Implementation of a Teaching Specification, Management and Assessment tool*. University of Luxembourg > Faculty of Science, Technology, Communication (FSTC) > Computer Science, and Communications Research Unit (CSC), 2016. URL: http://hdl.handle.net/10993/29884.

[290] L. I. Li, T. F. d. A. BISSYANDE, M. PAPADAKIS, S. Rasthofer, A. Bartel, D. Octeau, J. KLEIN, and Y. L. TRAON. *Static Analysis of Android Apps: A Systematic Literature Review*. University of Luxembourg > Interdisciplinary Centre for Security, Reliability et al., 2016. URL: http://hdl.handle.net/10993/26879.

[291] L. I. Li, L. I. Daoyuan, T. F. d. A. BISSYANDE, D. Lo, J. KLEIN, and Y. L. TRAON. *Ungrafting Malicious Code from Piggybacked Android Apps*. University of Luxembourg > Interdisciplinary Centre for Security, Reliability et al., 2016. URL: http://hdl.handle.net/10993/26880.

[292] L. E. H. Thanh, D. C. NGUYEN, and L. BRIAND. *ReACP: A Semi-Automated Framework for Reverse-engineering and Testing of Access Control Policies of Web Applications*. University of Luxembourg > Interdisciplinary Centre for Security, Reliability and Trust (SNT), 2016. URL: http://hdl.handle.net/10993/27699.

A.7 Miscellaneous

[293] M. BRÜHL, D. U. Sauer, and J.-R. HADJI-MINAGLOU. *Experimental Lifetime Investigation of Series Connected Li-ion Cells at Different Operation Strategies*. 2016. URL: http://hdl.handle.net/10993/31504.

[294] S. Bustan, A. M. Gonzalez-Roldan, C. SCHOMMER, S. Kamping, M. Loeffler, M. Brunner, H. Flor, and F. Anton. *Facteurs psychologiques, cognitifs et les influences contextuelles dans la douleur et la souffrance liée à la douleur*. 2016. URL: http://hdl.handle.net/10993/28990.

[295] T. DERRMANN, S. FAYE, R. FRANK, and T. ENGEL. *LuST-LTE: A Simulation Package for Pervasive Vehicular Connectivity*. 2016. URL: http://hdl.handle.net/10993/28106.

[296] T. DERRMANN, S. FAYE, R. FRANK, and T. ENGEL. *Poster: LuST-LTE: A Simulation Package for Pervasive Vehicular Connectivity*. 2016. URL: http://hdl.handle.net/10993/28800.

[297] K. A. A. E.-S. EMARA. *Poster: PREXT: Privacy Extension for Veins VANET Simulator*. 2016. URL: http://hdl.handle.net/10993/29073.

[298] K. A. A. E.-S. EMARA, W. Woerndl, and J. Schlichter. *Context-based Pseudonym Changing Scheme for Vehicular Adhoc Networks*. 2016. URL: http://hdl.handle.net/10993/29075.

[299] L. Fejoz, N. NAVET, S. M. SUNDHARAM, and S. ALTMEYER. *Applications of the CPAL language to model, simulate and program Cyber-Physical Systems*. 2016. URL: http://hdl.handle.net/10993/24833.

[300] C. FRANCK and U. SORGER. *Some Properties of Homogenous Trellis-Constrained Codes*. 2016. URL: http://hdl.handle.net/10993/29882.

[301] C. FRANCK and U. SORGER. *Untraceable VoIP Communication based on DC-nets*. 2016. URL: http://hdl.handle.net/10993/29881.

[302] G. Gallegos-Garcia, V. IOVINO, P. ROENNE, and P. Y. A. RYAN. *(Universal) Unconditional Verifiability in E-Voting without Trusted Parties*. 2016. URL: http://hdl.handle.net/10993/31726.

[303] P. GLAUNER. *Detecting Electricity Theft*. 2016. URL: http://hdl.handle.net/10993/28368.

[304] C. HAMMERSCHMIDT, S. Marchal, G. Pellegrino, R. STATE, and S. Verwer. *Efficient Learning of Communication Profiles from IP Flow Records*. 2016. URL: http://hdl.handle.net/10993/28374.

[305] C. HAMMERSCHMIDT, S. Marchal, R. STATE, and S. Verwer. *Behavioral Clustering of Non-Stationary IP Flow Record Data*. 2016. URL: http://hdl.handle.net/10993/28375.

[306] W. HÖHN and C. SCHOMMER. *Annotating and Georeferencing of Digitized Early Maps*. 2016. URL: http://hdl.handle.net/10993/29409.

[307] Q. Lin, C. HAMMERSCHMIDT, G. Pellegrino, and S. Verwer. *Short-term Time Series Forecasting with Regression Automata*. 2016. URL: http://hdl.handle.net/10993/28623.

[308] S. MAUW, J. L. T. POZO, and R. T. RASUA. *A class of precomputation-based distance-bounding protocols*. 2016. URL: http://hdl.handle.net/10993/26836.

[309] A. MITSEVA, A. PANCHENKO, F. Lanze, M. Henze, K. Wehrle, and T. ENGEL. *POSTER: Fingerprinting Tor Hidden Services*. 2016. URL: http://hdl.handle.net/10993/28223.

[310] A. MIZERA, J. PANG, and Q. YUAN. *GPU-accelerated steady-state analysis of probabilistic Boolean networks*. 2016. URL: http://hdl.handle.net/10993/28545.

[311] B. PEJO and Q. Tang. *Game-Theoretic Framework for Integrity Verification in Computation Outsourcing*. 2016. URL: http://hdl.handle.net/10993/29089.

[312] x. sun and L. ROBALDO. *Ali Baba and Thief, Norm Emergence in Games*. 2016. URL: http://hdl.handle.net/10993/29183.

A.8 Unpublished

[313] R. J. BISDORFF. "A sparse outranking digraph model for HPC-ranking of big performance tableaux". 2016. URL: http://hdl.handle.net/10993/28393.

[314] R. J. BISDORFF. "Computing linear rankings from trillions of pairwise outranking situations". 2016. URL: http://hdl.handle.net/10993/28613.

[315] R. J. BISDORFF. "Ranking big performance tableaux with multiple incommensurable criteria and missing data". 2016. URL: http://hdl.handle.net/10993/23921.

[316] M. Boyer, H. Daigmorte, N. NAVET, and J. Migge. "Performance impact of the interactions between time -triggered and rate-constrained transmissions in TTEthernet". 2016. URL: http://hdl.handle.net/10993/23845.

[317] L. Ciarletta, L. Fejoz, A. Guenard, and N. NAVET. "Development of a safe CPS component: the hybrid parachute, a remote termination add-on improving safety of UAS". 2016. URL: http://hdl.handle.net/10993/23406.

[318] P. GLAUNER and R. STATE. "Deep Learning Concepts from Theory to Practice". 2016. URL: http://hdl.handle.net/10993/28369.

[319] P. GLAUNER and R. STATE. "Deep Learning on Big Data Sets in the Cloud with Apache Spark and Google TensorFlow". 2016. URL: http://hdl.handle.net/10993/28807.

[320] P. GLAUNER and R. STATE. "Load Forecasting with Artificial Intelligence on Big Data". 2016. URL: http://hdl.handle.net/10993/28619.

[321] N. GUELFI, A. CAPOZUCCA, and B. RIES. "Measuring the SWEBOK Coverage: An Approach and a Tool". 2016. URL: http://hdl.handle.net/10993/31407.

[322] C. HAMMERSCHMIDT, B. L. Loos, S. Verwer, and R. STATE. "Flexible State-Merging for learning (P)DFAs in Python". 2016. URL: http://hdl.handle.net/10993/28376.

[323] W. HÖHN and C. SCHOMMER. "RAT: A Referencing and Annotation Tool for Digitized Early Maps". 2016. URL: http://hdl.handle.net/10993/29410.

[324] E. KIEFFER, G. DANOY, and P. BOUVRY. "On Bi-level approach for Scheduling problems". 2016. URL: http://hdl.handle.net/10993/28915.

[325] A. MACHALEK and D. DUNLOP. "Collaboration Web - Social Computing Technology for Emergency Data Interoperability". 2016. URL: http://hdl.handle.net/10993/29078.

[326] A. MACHALEK, D. DUNLOP, Z. Balogh, E. Gatial, and L. Hluchy. "REDIRNET – Emergency Responder Data Interoperability Network". 2016. URL: http://hdl.handle.net/10993/29108.

[327] A. MACHALEK, D. DUNLOP, C. Simon, and R. Hoben. “Visual Public Protection Disaster Relief and Critical Infrastructure”. 2016. URL: http://hdl.handle.net/10993/29110.

[328] N. NAVET. “The use of simulation in the design of critical embedded systems”. 2016. URL: http://hdl.handle.net/10993/27703.

[329] N. NAVET. “Timing Analysis of Automotive Architectures and Software”. 2016. URL: http://hdl.handle.net/10993/26004.

[330] N. NAVET, L. Fejoz, L. Havet, and S. ALTMEYER. “Lean Model-Driven Development through Model-Interpretation: the CPAL design flow”. 2016. URL: http://hdl.handle.net/10993/23414.

[331] N. NAVET, J. Seyler, and J. Migge. “Timing verification of realtime automotive Ethernet networks: what can we expect from simulation?” 2016. URL: http://hdl.handle.net/10993/23457.

[332] B. PEJO, Q. Tang, and H. Wang. “Protect both Integrity and Confidentiality in Outsourcing Collaborative Filtering Computations”. 2016. URL: http://hdl.handle.net/10993/29388.

[333] G. Pellegrino, C. HAMMERSCHMIDT, Q. Lin, and S. Verwer. “Learning Deterministic Finite Automata from Infinite Alphabets”. 2016. URL: http://hdl.handle.net/10993/28373.

[334] P. ROENNE. “JCJ with Improved Verifiability Guarantees”. 2016. URL: http://hdl.handle.net/10993/29212.

[335] P. E. VERISSIMO and J. DECOUCHANT. “The big data deluge in biomedicine: addressing the privacy vs. sharing dilemma”. 2016. URL: http://hdl.handle.net/10993/27448.

[336] M. VOLP, A. Lackorzynski, J. DECOUCHANT, V. RAHLI, F. ROCHA, and P. E. VERISSIMO. “Avoiding Leakage and Synchronization Attacks through Enclave-Side Preemption Control”. 2016. URL: http://hdl.handle.net/10993/28964.

Appendix B

Research Projects

This chapter lists CSC research projects that were ongoing during 2016, and is structured to summarize the projects by funding source.

Note: the 2016 CSC activity report lists only projects whose principal investigator is a CSC member, while previous reports listed all projects in which a CSC member participated in any capacity.

- COST Action Projects
- Directorate-General for Education and Culture (EC) Projects
- EC - FP7 Projects
- ESA Projects
- European Defence Agency - EDA Projects
- External organisation funding Projects
- FNR - AFR Projects
- FNR - AFR PhD Projects
- FNR - AFR PostDoc Projects
- FNR - AFR Projects
- FNR - CORE Projects
- FNR - INTER Projects
- FNR - Luxembourg (AFR - PHD) Projects
- FNR - Other Projects
- Horizon 2020 (EU) Projects
- International call ANR - FNR Luxembourg () Projects
- UL (PUL) Projects
- UL Funding Projects
- Undefined Funding Projects
- Unfunded Projects

B.1 COST Action Projects

High-Performance Modelling and Simulation for Big Data Applications

http://chipset-cost.eu

Acronym:	cHiPSet
PI:	Dzmitry KLIAZOVICH
Funding:	COST Action
Duration:	April 8, 2015 – April 7, 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.

Network for Sustainable Ultrascale Computing

http://www.nesus.eu

Acronym:	NESUS
PI:	Pascal BOUVRY
Funding:	COST Action
Duration:	March 28, 2014 – March 27, 2018
Members:	• Pascal BOUVRY (Principal Investigator) • Sébastien VARRETTE (Researcher)
Partners:	• Alexandru Ioan Cuza University of Iasi • INRIA • Jozef Stefan Institute • Norwegian University of Science and Technology • Politecnico di Torino • Technical Unversity of Denmark • Technische Universitaet Wien • Universidad de Extremadura • Universidad de Murcia

- Universidad de Valladolid
- Universität Wien
- Université de Mons, Belgique
- University of Amsterdam
- University of Bergen
- University of Calabria
- University of Cyprus
- University of Innsbruck
- University of La Laguna
- University of Malta
- University of Sarajevo
- University of Tartu
- University Ss Cyril & Methodiuous, Skopje

Description

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

- First, the current state-of-the-art on sustainability in large-scale systems will be studied. The Action will strive for continuous learning by looking for synergies among HPC, distributed systems, and big data communities in cross cutting aspects like programmability, scalability, resilience, energy efficiency, and data management.
- Second, the Action will explore new programming paradigms, runtimes, and middlewares to increase the productivity, scalability, and reliability of parallel and distributed programming.
- Third, as failures will be more frequent in ultrascale systems, the Action will explore approaches of continuous running in the presence of failures. The Action plans to find synergies between resilient schedulers that handle errors reactively or proactively, monitoring and assessment of failures, and malleable applications that can adapt their resource usage at runtime.
- Fourth, future scalable systems will require sustainable data management for addressing the predicted exponential growth of digital information. The Action plans to explore synergistic approaches from traditionally separated communities to reform the handling of the whole data life cycle, in particular: restructure the Input/Output (I/O) stack, advance predictive and adaptive data management, and improve data locality.
- Fifth, as energy is a major limitation for the design of ultrascale infrastructures, the Action will address energy efficiency of ultrascale systems by investigating, promoting, and potentially standardizing novel metrics for energy monitoring and profiling, modelling, and simulation of energy consumption and CO2 emission, eco-design of ultrascale components and applications, energy-aware resource management, and hardware/software codesign.
- Finally, the Action will identify applications, high-level algorithms, and services amenable to ultrascale systems and investigate the redesign and reprogramming efforts needed for applications to efficiently exploit ultrascale plat-

forms, while providing sustainability.

B.2 Directorate-General for Education and Culture (EC) Projects

Future Education and Training in Computing: How to meet our students where they are

http://fetch.ecs.uni-ruse.bg/index.php?cmd=gsIndex

Acronym:	FETCH
Reference:	I2R-NET-PEU-13FTCH
PI:	Thomas ENGEL
Funding:	Directorate-General for Education and Culture (EC)
Budget:	1,127,000.00 €
Duration:	Oct. 1, 2013 – Sept. 30, 2016
Members:	• Thomas ENGEL (Principal Investigator) • Stefanie OESTLUND (Project Coordinator)
Area:	Communicative Systems
Partners:	• Aalborg University • Academy of Economic Studies • BIKEMA • Comhard Gesellschaft für Computer Kommunikation Bildung mbH • Czech Technical University • Dublin City University • GFai tech GmBH • Heriot-Watt University • HTW Berlin • IEEE Bulgaria Section • IIEF Integrierte Informationssysteme für Engineering und Facility Management GmbH • Institute of Mathematics and Informatics • Izmir University of Economics • Kaunas University of Technology • Lappeenranta University of Technology • Linnaeus University • Liverpool John Moores University • Molde University College • Musala Soft

- Ostfold University College
- Polytechnic University of Tirana
- Reykjavik University
- Riga Technical University
- Selcuk University
- Slovak University of Technology
- Sofia University “St. Kliment Ohridski”
- South East European University
- Tallinn University of Technology
- Technical University of Gabrovo
- Technical University of Sofia
- Technical University of Varna
- Technische Universitaet Wien
- Technische Universität Ilmenau
- Tellus Ltd
- Temida Ltd
- University of Bahcesehir
- University of Calabria
- University of Coimbra
- University of Cyprus
- University of Delft
- University of Ioannina
- University of La Laguna
- University of Library Science and Information Technologies
- University of Liechtenstein
- University of Luxembourg
- University of Malaga
- University of Malta
- University of Napoli Parthenope
- University of Nova Gorica
- University of Novi Sad
- University of Palermo
- University of Pavia
- University of Pitesti
- University of Plovdiv
- University of Rijeka
- University of Russe
- University of Szeged
- University of Tampere
- University of Veliko Turnovo
- University of Versailles
- University Ss Cyril & Methodiuous, Skopje
- VARTEC NV
- Vilnius Gediminas Technical University
- Vilnius University
- Warsaw University of Technology

Description

Future Education and Training in Computing: How to support learning at anytime anywhere?

The project aims at the achievement of intelligent growth, and building a knowledge and innovation based computer society through raising the quality of computing education, introducing modern innovative technologies in education, sharing knowledge, discussing methodologies, promoting exchange of good practice between all parties.

In order to respond to:

- ET2020 - the consortium will develop a European Strategic Framework for Computing Education and Training 2020 (ESFCET 2020), which will form a solid, global strategic framework that leverages local and transnational competences to enhance Computing Education in Europe.
- European Qualification Framework - ETN FETCH will develop a European Evaluation Framework in Computing Education and Training 2020 (EEFCET 2020), which will evaluate the three factors: Knowledge, Skills and Competences gained from Computing Education and Training.
- The Tuning Methodology - the project will prepare recommendations for future Digital Curricula in Computing Education and Training 2020 (DCCET 2020).
- Introducing modern innovative technologies in education - new didactical theories and learning models for using social media in education will be developed.

Main project outcomes and products:

- ETN FETCH "Future Education and Training in Computing: How to support learning at anytime anywhere".
- European Strategic Framework for Computing Education and Training 2020 (ESFCET 2020).
- European Evaluation Framework in Computing Education and Training 2020 (EEFCET 2020).
- A set of recommendations for future Digital curricula in Computing Education and Training 2020.
- New didactical theories and learning models for using social media in education.
- Six conferences with co-event workshops in the field of computing.
- Publications of the results in journals, newspapers, magazines, brochures and web sites.
- Internal and external evaluation reports.

Impact:

- The project products will be of benefit for all actors in Computing education like
  - University and national policy-makers in the field of Computing education;
  - University academic staff who are lecturers/trainers in Computing;
  - Bachelor, Master & Doctoral Students;
  - Research institutes and centres in Computing;

  - Companies and SMEs in the field of Computing.
- The project will change the methodology of training computer specialists, will apply most modern technologies in education, and will promote closer cooperation between universities, research institutes and industry.

Results

The main project outcomes of the FETCH project are the following:

- European Strategic Framework for Computing Education and Training 2020
- European Evaluation Framework in Computing Education and Training 2020
- set of recommendations for future digital curricula in Computing Education and Training 2020
- New didactical theories and learning models for use social media in educational
- Six conferences and six workshops as co-events to the conferences in the field of computing.

B.3 EC - FP7 Projects

Emergency responder data interoperability network

http://www.redirnet.eu/

Acronym:	ReDIRNET
Reference:	I2R-NET-PEU-14RNET
PI:	Thomas ENGEL
Funding:	EC - FP7
Budget:	4,311,000.00 €
Duration:	March 1, 2014 – Aug. 30, 2016
Members:	• Thomas ENGEL (Principal Investigator) • Aurel MACHALEK (Researcher) • Stefanie OESTLUND (Project Coordinator)
Area:	Communicative Systems
Partners:	• Ardaco • British Association of Public Safety Communication Officers • ITTI Sp. z o.o. • Ministère d'Etat • Ministry of Interior of the Slovak Republic

- Nadony bezpecnostny urad
- NEXTEL S.A.
- Pramacom Prague spol. s r.o.
- World Consult

Description

Over the past 5 years the majority of the REDIRNET consortia have participated in Projects SECRICOM and FREESIC; this has involved partners engaging significantly with a wide range of public safety officers across the EU. A benefit of this engagement has been the recognition that in addition to agency interoperability of communications a pressing need exists for agency interoperability of additional IT systems such as databases, sensor systems and cameras. REDIRNET provides a framework for addressing this need with detailed mapping of user preferences and related legal requirements using innovative technologies.

The consortium is aware that frequently it is non-technical issues that hinder agency interoperability regardless of the quality of technical solutions. Consequently user engagement across a range of agencies EU-wide will be ongoing throughout the duration of REDIRNET. This will lead to the first of two elements of the REDIRNET framework - a quality repository of user identified interoperability issues and proposals for their resolution.

The second element of REDIRNET will be technology. REDIRNET will provide a decentralized framework for interoperability for first responders' systems based on a public meta-data gateway controlled by the agencies themselves via a REDIRNET socio-professional web. Agencies will be able link up to partner agencies of their choice and operational need; they will also be able to manage the scope of such interoperability. To help set up these link-up arrangements REDIRNET will be enhanced with semantic web methods in accordance with the vocabulary and processes of the user community. Inter-operating agencies will need only to develop one gateway (to REDIRNET) leading to a cost effective solution; agent technologies will also be developed to facilitate the integration of user systems into REDIRNET.

Aspects of REDIRNET will address not only current but future challenges. Published project results being timely for 2016 development.

Results

REDIRNET proposes an agile platform, as well as the adoption of a set of tools and web service sets, aimed at developing a repository of public safety user identified needs and proposals for their resolution providing a decentralized framework for interoperability of first responders' systems.

In particular the REDIRNET project offers an interoperability solution to First Responder agencies, based on meta-data exchange and a socio-professional web relationship paradigm, aiming at greater cooperation and interoperability between the emergency services agencies. While it has built on the previously EC-funded project FREESIC, it advances the state-of-the-art by transitioning

Command and Control technology towards IP-based communications networks in the Strategic and Coordinating Level of operations (not Field Command).

REDIRNET in fact has been very strong in the implementation phase of the second and final stage in 2016. It has delivered prototypes of the main platform, configuration interfaces and generic system gateway that facilitate cross-border communication of public safety agencies after adaptation of their specific systems into the common interoperable system. The relevant legal framework has been analysed and carefully considered in the design. Especially the final part of the activities has been characterised by a clear evidence for the creation of a framework on how manage interoperability capabilities and contribute in responding to global challenges.

Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security

http://www.trespass-project.eu/

Acronym:	TREsPASS
Reference:	FP7 Grant Agreement No. 318003
PI:	Sjouke MAUW
Funding:	EC - FP7
Budget:	13,568,381.00 €
Duration:	Nov. 1, 2012 – Oct. 31, 2016
Members:	• Sjouke MAUW (Principal Investigator) • Olga GADYATSKAYA (Researcher) • Rolando TRUJILLO RASUA (Researcher) • Barbara Kordy (Collaborator) • Gabriele LENZINI (Collaborator) • Yunior RAMIREZ CRUZ (Collaborator)
Partners:	• Aalborg University • BiZZdesign • Consult Hyperion • Cybernetica • Deloitte Netherlands • GMVIS SKYSOFT • GMV SGI • Goethe-Universität • Hamburg University of Technology • IBM Switzerland • itrust Luxembourg • LUST

- Royal Holloway University London
- Technical Unversity of Denmark
- University of Delft
- University of Twente

Description

Information security threats to organizations have changed completely over the last decade, due to the complexity and dynamic nature of infrastructures and attacks. Successful attacks cost society billions a year, impacting vital services and the economy. Examples include StuxNet, using infected USB sticks to sabotage nuclear plants, and the DigiNotar attack, using fake certificates to spy on website traffic. New attacks cleverly exploit multiple organizational vulnerabilities, involving physical security and human behavior. Defenders need to make rapid decisions regarding which attacks to block, as both infrastructure and attacker knowledge are constantly evolving. Current risk management methods provide descriptive tools for assessing threats by systematic brainstorming. In today's dynamic attack landscape, however, this process is too slow and exceeds the limits of human imaginative capability. Emerging security risks demand an extension of established methods with an analytical approach to predict, prioritize, and prevent complex attacks. The TREsPASS project develops quantitative and organization- specific means to achieve this in complex socio-technical environments. The iterative, tool-supported framework:

- Represents the structure of complex organizations as socio-technical security models, integrating social and technical viewpoints;
- Predicts socio-technical attacks, prioritizes them based on their risk, and assesses the aggregated effect of preventive measures;
- Presents results to enable quick understanding and updating of the current security posture.

By integrating European expertise on socio-technical security into a widely applicable and standardized framework, TREsPASS will reduce security incidents in Europe, and allow organizations and their customers to make informed decisions about security investments. This increased resilience of European businesses both large and small is vital to safeguarding the social and economic prospects of Europe. All public information about the project can be found at http://www.trespass-project.eu/. TREsPASS is executed jointly by members of SnT and CSC.

Results

- We have developed a stochastic framework for attack-defense trees quantitative analysis. This thrive in security risk assessment area have been reported in the following paper: A Stochastic Framework for Quantitative Analysis of Attack-Defense Trees. R. Jhawar, K. Lounis, and S. Mauw. In Security and Trust Management, Springer International
  Publishing, pp. 138153, 2016.
- We have added more features to the ADTool, such as ranking and support to

sequential gates. Such improvements have been reported in the following paper. Attack Trees for Practical Security Assessment: Ranking of Attack Scenarios with ADTool 2.0. O. Gadyatskaya, R. Jhawar, P. Kordy, K. Lounis, S. Mauw and R. Trujillo-Rasua. In Proc. of QEST, Springer, LNCS 9826, pp. 159-162, 2016.

- We gave support to the GramSec 2016 workshop.
- Using attackdefense trees to analyze threats and countermeasures in an ATM: A case study. M. Ford, M. Fraile, O. Gadyatskaya, R. Kumar, M. Stoellinga and R. Trujillo-Rasua. In Proc. of PoEM, Springer, 2016.
- Modelling Attack-defense Trees Using Timed Automata. O. Gadyatskaya, R.R. Hansen, K.G. Larsen, A. Legay, M.C. Olesen and D.B. Poulsen. In Proc. of FORMATS, Springer, LNCS 9884, pp. 35-50, 2016.
- Towards Empirical Evaluation of Automated Risk Assessment Methods. O. Gadyatskaya, K. Labunets and F. Paci. In Proc. of CRiSIS, Springer, 2016.
- Bridging two worlds: Reconciling practical risk assessment methodologies with theory of attack trees. O. Gadyatskaya, C. Harpes, S. Mauw, C. Muller and S. Muller. In Proc. of GraMSec, Springer, 2016.

B.4 ESA Projects

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

Acronym:	M2MSAT
PI:	Thomas ENGEL
Funding:	ESA
Budget:	500,000.00 €
Duration:	Oct. 3, 2016 – Jan. 2, 2018
Members:	• Thomas ENGEL (Principal Investigator) • Luca LAMORTE (Researcher) • Ridha SOUA (Researcher) • Stefanie OESTLUND (Project Coordinator)
Area:	Communicative Systems
Partner:	SES Techcom Services

Description

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

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

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

Results

In the first months of the project, we investigated lightweight application and transport protocols for Machine-to-machine (M2M) / Internet of Things (IoT) applications, namely Constrained Application Protocol (CoAP), MQTT and MQTT-SN. The future purpose is to understand how they work and then carry out a comparison analysis. In addition, we studied several IoT and satellite simulators that can be integrated and used to efficiently simulate the IoT/Satellite network.

B.5 European Defence Agency - EDA Projects

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

Acronym:	ASIMUT
Reference:	R-AGR-0548-10-Z
PI:	Pascal BOUVRY
Funding:	European Defence Agency - EDA
Budget:	640,000.00 €
Duration:	March 5, 2015 – March 4, 2017
Members:	• Pascal BOUVRY (Principal Investigator) • Matthias BRUST (Researcher) • Grégoire DANOY (Researcher)

	• Martin ROSALIE (Researcher)
Area:	Intelligent and Adaptive Systems
Partners:	• FLY-N-SENSE • FRAUNHOFER IOSB • THALES SYSTEMES AEROPORTES SAS • Université de Bordeaux I

Description

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

Results

For 2016, in the context of the ASIMUT project, the UL/SnT has contributed in the field of UAV swarms. One of the aspects of the ASIMUT project is the use of multilevel swarms of UAVs: a High Level Coordination Swarm of UAVs manages several Low Level Swarms of UAVs in charge of area surveillance or tracking.

We have first proposed a model to autonomously manage a swarm of UAVs [251]. This model can handle the tasking of UAVs with different missions and is usable by both types of swarms used in the ASIMUT project. In a second phase, we focused our attention on mobility models for such swarms. As the trajectories have to be unpredictable, we proposed novel nature inspired mobility models (i.e., ant colony based) including a chaotic behavior. We obtained outstanding results in terms of coverage (coverage rate, fairness of the coverage, recent coverage) which led to one publication in an international conference [252]. In addition, a second paper presenting all ASIMUT contributions has been authored by all ASIMUT partners and published in a second international conference [121].

B.6 External organisation funding Projects

CREOS

Acronym:	CREOS
PI:	Thomas ENGEL
Funding:	External organisation funding
Budget:	841,679.00 €

Duration:	May 1, 2012 – June 30, 2020
Members:	• Thomas ENGEL (Principal Investigator) • Florian ADAMSKY (Researcher) • Raimondas SASNAUSKAS (Researcher) • Emilia TANTAR (Researcher)
Area:	Communicative Systems
Partner:	CREOS

Description

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

Results

In 2016, together with the energy company CREOS, we started to build a Supervisory Control and Data Acquisition (SCADA) laboratory for research purposes. This includes real hardware and software from CREOS, such as IP/MPLS routers and switches and several servers with specialist software. Additionally, we documented the whole setup and prepared it for future security investigations.

Huawei Security Magazine

Acronym:	Huawei
PI:	Sjouke MAUW
Funding:	External organisation funding
Budget:	56,295.00 €
Duration:	April 1, 2015 – March 30, 2016
Members:	• Sjouke MAUW (Principal Investigator) • Olga GADYATSKAYA (Collaborator) • Ravi JHAWAR (Collaborator) • Jun PANG (Collaborator)
Area:	Information Security

Description

This project aims for establishment of a joint bimonthly magazine of Huawei and the University of Luxembourg. The goal of this magazine is to serve as a comprehensive reference guide which will not only allow Huawei to kick-start its security research but also design both short and long term security research strategies. To achieve this goal, the magazine will provide a succinct review of the on-going academic and industrial research, and identify the latest technological advancements and provide useful insights on their bene ts and potential future impact on ICT security. The review of the state-of-the-art and analysis of promising technological trends will be performed on the topics that might be of interest to Huawei.

Partners: Huawei Technologies Co. Ltd., China

MOTION: Exploring human mobility and optimizing the usage of the transportation network using vehicular network technologies In order to understand individual mobility on a countrywide scale, it is important to reply on large scale mobility datasets.

https://secan-lab.uni.lu/projects/national-funded-projects/274-motion

Acronym:	Motion
Reference:	R-AGR-0426-12
PI:	Thomas ENGEL
Funding:	External organisation funding
Budget:	390,000.00 €
Duration:	Jan. 1, 2010 – Dec. 31, 2016
Members:	• Thomas ENGEL (Principal Investigator) • German CASTIGNANI (Researcher) • Karim Ahmed Awad El-Sayed EMARA (Researcher) • Sébastien FAYE (Researcher) • Raphaël FRANK (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator)
Area:	Communicative Systems
Partner:	Post

Description

Suitable datasets that would allow such an analysis are Call Detail Records (CDR) that are available at mobile phone operators. CDRs provide details on incoming and outgoing calls with the main goal of building network usage reports. In the MOTION project, we plan to extend the usage of CDR to study individual mobility. It is clear that before the data can be made available, all privacy-related information must be removed. The resulting anonymised dataset will provide important information on how people move from one cellular base station to another. Please note that those datasets only provide information on how people move (not personally identifiable information). However, if aggregated on a large-scale, it provides valauble information on the socioeconomic mobility patterns that can be exploited from a large number of applications and services including transportation optimization. Another advantage of this dataset is that it includes cross-border commuters, as their mobile phones register with the Luxembourgian mobile phone network (even those not covered by a Luxembourg contract).

Results

The main objective of the project was to study the relationship that may exist between a dataset from POST – which is specific to cellular networks – and metrics to estimate the situation of road traffic at a certain place and time, with the aim of developing a concrete application both for POST and SECAN-Lab. This application has been developped successfully as a service able to estimate the traffic situation at a certain place and time based on aggregated and privacy-friendly data from POST.

The service is fully controllable through a web interface. The user can add GPS points as he wishes, either by means of a map or by requesting a latitude and a longitude via a form. Once the GPS point is registered in the database, the user can request an instantaneous estimate of the speed on the road closest to this GPS point. Subsequently, the application computes, at regular intervals (by default, every 15 minutes) the evolution of the speed estimates and records the results in a database for further analysis. In addition, the service also records contextual and concurrent data from external services. This data can serve as a good basis for calibrating the estimates.

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

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

Acronym: BluVeC

PI:	Thomas ENGEL
Funding:	External organisation funding
Duration:	April 1, 2013 – April 1, 2017
Members:	• Thomas ENGEL (Principal Investigator) • Walter BRONZI (Doctoral Candidate) • Raphaël FRANK (Scientific Contact)
Area:	Communicative Systems
Partner:	Telindus

Description

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

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

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

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

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

Results

We developed and internally tested the SECAN-Lab BlueScanner app. The scope of the application is to collect Bluetooth beacons whilst in a driving scenario and send them to a sever. In this context was performed a 2-month collection campaign within University of Luxembourg. More than 20 participants where collected for this stage.

TelMe

Acronym:	TelMe
Reference:	R-AGR-0426-13-Z
PI:	Thomas ENGEL
Funding:	External organisation funding
Budget:	390,000.00 €
Duration:	Jan. 1, 2010 – Dec. 31, 2016
Members:	• Thomas ENGEL (Principal Investigator) • Gabriela GHEORGHE (Researcher) • Nicolas LOUVETON (Researcher) • Roderick MCCALL (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator)
Area:	Communicative Systems
Partners:	• Roderick McCall (LIST) • Post

Description

The Telecom Museum Experiences (TelMe) project is funded by POST Luxembourg. The project will explore new serious gaming approaches which are designed to improve public understanding of telecoms research and development.

Results

This project is a collaboration with Post and more precisely the Post Museum. This project aims at exploring new interactive approaches to museum experience, particularly with the possibility to interact with museums from across Europe. The project ended in 2016 with the delivery of a complete content management system and a range of games to be used with a large Multitouch table in a museum. Software has been documented, tested and packaged for future deployment.

B.7 FNR - AFR Projects

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

PI:	Juergen SACHAU
Funding:	FNR - AFR
Duration:	March 1, 2013 – March 31, 2017
Members:	• Juergen SACHAU (Principal Investigator) • David NORTA (Doctoral Candidate)
Area:	Communicative Systems
Partner:	RWTH Aachen University

Description

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

B.8 FNR - AFR PhD Projects

Coevolutionary HybRid Bi-level Optimization

Acronym:	CARBON
Reference:	I2R-DIR-PFN-11AFRT
PI:	Pascal BOUVRY
Funding:	FNR - AFR PhD
Duration:	Jan. 3, 2015 – Jan. 3, 2018
Members:	• Pascal BOUVRY (Principal Investigator) • Grégoire DANOY (Collaborator) • Emmanuel KIEFFER (Doctoral Candidate)
Area:	Intelligent and Adaptive Systems

Description

Multi-level problems are problems involving several different decision makers. In particular, bi-level problems engage two types of decision makers “playing” iteratively. The first decision maker is referred to as the leader while the second is the follower. Bi-level programs found their root in Game theory (Stakelberg equilibrium) and have a wide range of applications. They have been proved NP-hard even for convex leader and follower problems. Convexity gave us resolution tools in the single-level case but now we have to face this problem without

this set of tools. When convexity cannot be assumed, metaheuristics are employed. Coevolutionary algorithms are well adapted to the structure of bi-level problems. They are a special kind of evolutionary metaheuristics designed to use collaborative or competitive metatheurisrtics working in parallel to find the optimal solution. We propose a novel approach which consists of hybridizing coevolutionary algorithms with exact approaches to take advantage of the research results made in exact decomposition techniques. According to these new hybrid and coevolutionary algorithms, we want to tackle the Cloud Pricing Problem. The latter is nowadays a real need for Cloud providers (and brokers) where optimal prices could be deduced by applying bi-level models.

The research will thus focus on:

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

Results

On Bi-level approach for Scheduling problems [324]: Hierarchical optimization is concerned with several nested levels of optimization problems binding decision makers. Bi-level optimization is a particular case involving two nested problems representing two decision makers who control their own set of decision variables. The first decision maker referred to as the leader takes the first decision which restricts the second decision maker referred to as the follower. In response to it, the follower will try to react optimally to the leader's decision. This modelling pattern may lead to collaboration or competition between them. Closely related to Game Theory (Stackelberg games), bi-level strategies are more realistic since they do not overestimate the objective fitness when decision makers may have an impact on each other. Bi-levels modelling has been proposed for different kinds of problems (e.g. supply-chain management, network optimization, structural optimization). One of the most studied bi-level problems is the Toll setting problem which consists in finding optimal toll locations knowing that network users try to minimize their travel cost. By considering the possible reactions of the network users, the authority operating tolls is able to maximize its revenue and avoid a situation discouraging network users to take highways. Despite the fact that the literature on scheduling is very rich, few scheduling problems have been modelled using bi-level representations. We propose here a survey on scheduling using bi-level models and show the necessity to develop new optimization tools to solve them.

Co-evolutionary approach based on constraint decomposition [194]: Practical optimization problems are often large constrained problems in which the generation of feasible solutions still represent an important challenge. Population-based algorithms (e.g. genetic algorithm) are natured-inspired methods which experience a real success when solving free optimization problems. Nevertheless when some decision variables are strongly linked through constraints, it may be very difficult to generate feasible solutions with standard evolutionary operators (e.g crossover, mutation). The initialization of the first population

might also be a brainteaser and often rely on some random procedures. It is obvious that it is not possible to guaranty feasibility in these conditions. Penalty factors are thus added to the tness function to disadvantage non-feasible solutions. Nevertheless, they are hard to define and strongly depend on the considered instance. A large penalty factor will definitely drive solutions to the feasible decision set while a small factor will not be enough to discriminate non-feasible solutions. Penalty factors do not solve the problem of generating feasible solutions, they only penalize non-feasible ones. If the evolutionary operators are not able to generation new valid solutions, the penalty factor will not help. In some cases, one can also observe that a feasible solution with poor fitness can be rejected in favor of a non-feasible one which are particularly closed to the feasible decision set. In this paper, we are going to describe a new approach to fix this issue. This method is based on two phases. The first one consists in ensuring a minimum rate of feasible solutions in the initial population while the second one adds a mechanism which is triggered when feasibility falls below this rate during the evolution.

A novel co-evolutionary approach for constrained genetic algorithms [196]: Standard evolutionary algorithms are very efficient on unconstrained optimisation problems since evolutionary operators do not generate values outside the decision set. However constrained problems add a new level of difficulty. Various constraints handling techniques have been proposed, such as static or dynamic penalties, but few of them have attempted to handle constraints separately. Indeed, in many combinatorial problems, the conjunction of some groups of constraints makes them very hard. In this paper, a novel type of co-evolutionary algorithm based on constraints decomposition (CHCGA) is proposed. Its principle consists in dividing an initial constrained problem into a sucient number of sub-problems with weak constrained domains. Generally at this stage, it is trivial to obtain feasible solutions. Then, each of these sub-problems is evolved in order to increase their compatibility with another sub-population. When two sub-populations are compatible, i.e. they contain enough mutually feasible solutions, these two sub-populations merge and the process continues until reaching a single population representing the initial, globally constrained domain. Then, this population is used as initial population for one selected metaheuristic, a genetic algorithm in this work. Experimental results on the Cloud Brokering optimization problem have demonstrated a strong solution quality gain compared to a standard genetic algorithm.

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

mergy. Experimental results demonstrate the ability of H3MP to rapidly detect and keep watch on targets compared to random and pheromone based models.

Evaluation of Authenticated Ciphers

Acronym:	EAC
Reference:	I2R-DIR-AFR-090000
PI:	Alexei BIRYUKOV
Funding:	FNR - AFR PhD
Duration:	May 1, 2015 – March 31, 2019
Members:	• Alexei BIRYUKOV (Principal Investigator) • Aleksei UDOVENKO (Collaborator)
Area:	Information Security

Description

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

Results

Aleksei has attended the CRYPTO 2016 conference (one of the main events in the field of cryptography) and presented the paper "Cryptanalysis of a Theorem: Decomposing the Only Known Solution to the Big APN Problem" (submitted in the beginning of 2016, joint work with Alex Biryukov and Léo Perrin). He also co-authored a follow-up work on reverse-engineering of S-Boxes, which was accepted at IACR Transactions on Symmetric Cryptology 2016 (a hybrid journal/conference venue which replaces FSE). The paper is called "Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog" and is a joint work with Léo Perrin. The candidate presented this work at the ESC 2017 workshop (Luxembourg). Another work was on the design of a new lightweight block cipher called SPARX. The paper "Design Strategies for ARX with Provable Bounds: Sparx and LAX" was accepted at ASIACRYPT 2016. It is a joint work with Daniel Dinu, Léo Perrin, Vesselin Velichkov, Johahn Großschädl, Alex Biryukov. The candidate also presented this work at the GRSRD 2017 workshop (Luxembourg). Aleksei works on cryptanalysis of the authenticated cipher

NORX, which is a part of the CAESAR competition. A report with preliminary results is uploaded to an online archive. It shows particular weaknesses of the NORX permutation. The report is called ”Analysis of the NORX Core Permutation”.

Model Translation and Model Visualisation

PI:	Thomas ENGEL
Funding:	FNR - AFR PhD
Budget:	111,000.00 €
Duration:	Jan. 15, 2012 – Jan. 14, 2016
Members:	• Thomas ENGEL (Principal Investigator) • Susann GOTTMANN (Doctoral Candidate) • Raimondas SASNAUSKAS (Scientific Contact)
Area:	Communicative Systems
Partner:	SES

Description

Model transformations define how to transform a model into another model. Model transformation is executed using transformation rules. A transformation rule consists of the following parts: A left-hand-side (LHS) which defines a pattern, which shall be found in a model and a right-hand side (RHS) which defines the target pattern. During rule application, it is checked if the LHS of the rule can be found in the model. Then, this pattern is replaced by the pattern of the RHS in the model, i.e., the model is transformed according to the specification of the transformation rule. Model transformations can be executed either unidirectional, i.e., from a model to another model, or bidirectional, which includes also the backward direction. Model synchronisations describe a bidirectional model transformation approach. In this case, particular problems arise with regard to concurrency.

In this thesis, we applied formal concepts on model transformations on an industrial prototype case study with our partner company SES in the field of generating a visual representation (which we call SPELL-Flow) of satellite control procedures written in the language SPELL. The source code of the satellite control procedures and also the concrete visual representation are called concrete syntax. We also discovered new theoretical research problems and solved them formally.

Results

Driven by an industrial problem of transforming satellite control source code into visual flow charts, a formal methodology was developed within the project generalising model transformations based on triple graph grammars. We showed the ability to combine and extend complex theoretical frameworks in a consistent way. In particular, this concerns the concepts: Preservation, model synchronization, automated conflict resolution, and propagation of model updates between multiple views. The initial technical demonstration of the theoretical methods showed first potential.

Refactoring and Semantical Correctness

PI:	Thomas ENGEL
Funding:	FNR - AFR PhD
Budget:	111,000.00 €
Duration:	Jan. 15, 2012 – Jan. 14, 2016
Members:	• Thomas ENGEL (Principal Investigator) • Stefanie OESTLUND (Project Coordinator) • Nico NACHTIGALL (Doctoral Candidate) • Raimondas SASNAUSKAS (Scientific Contact)
Area:	Communicative Systems
Partner:	SES

Results

The intrinsic question of most activities in information science, in practice or science, is “Does a given system satisfy the requirements regarding its application?” Commonly, requirements are expressed and accessible by means of models, mostly in a diagrammatic representation by visual models. The requirements may change over time and are often defined from different perspectives and within different domains. This implies that models may be transformed either within the same domain-specific visual modelling language or into models in another language. Furthermore, model updates may be synchronised between different models. Most types of visual models can be represented by graphs where model transformations and synchronisations are performed by graph transformations. The theory of graph transformations emerged from its origins in the late 1960s and early 1970s as a generalisation of term and tree rewriting systems to an important field in (theoretical) computer science with applications particularly in visual modelling techniques, model transformations, synchronisations and behavioural specifications of models. Its formal foundations but likewise visual notation enable both precise definitions and proofs of important properties of model transformations and synchronisations from a theoretical point of view and an intuitive approach for specifying

transformations and model updates from an engineer's point of view. The recent results were presented in the EATCS monographs "Fundamentals of Algebraic Graph Transformation" (FAGT) in 2006 and its sequel "Graph and Model Transformation: General Framework and Applications" (GraMoT) in 2015. This project concentrated on one important property of model transformations and synchronisations, i.e., syntactical completeness. Syntactical completeness of model transformations means that given a specification for transforming models from a source modelling language into models in a target language, then all source models can be completely transformed into corresponding target models. In the same given context, syntactical completeness of model synchronisations means that all source model updates can be completely synchronised, resulting in corresponding target model updates. This work is essentially based on the GraMoT book and mainly extends its results for model transformations and synchronisations based on triple graph grammars by a new more general notion of syntactical completeness, namely domain completeness, together with corresponding verification techniques. Furthermore, the results are instantiated to the verification of the syntactical completeness of software transformations and synchronisations. The well-known transformation of UML class diagrams into relational database models and the transformation of programs of a small object-oriented programming language into class diagrams serve as running examples. The existing AGG tool is used to support the verification of the given examples in practice.

Stream Mining for Predictive Authentication Under Adversarial Influence

PI:	Radu STATE
Funding:	FNR - AFR PhD
Budget:	138,000.00 €
Duration:	Nov. 11, 2014 – Nov. 14, 2017
Members:	• Radu STATE (Principal Investigator) • Stefanie OESTLUND (Project Coordinator) • Christian HAMMERSCHMIDT (Doctoral Candidate) • Thomas ENGEL (Scientific Contact)
Area:	Communicative Systems
Partner:	neXus

Symbolic verification of distance-bounding and multiparty authentication protocols

Acronym:	DBMP

PI:	Sjouke MAUW
Funding:	FNR - AFR PhD
Budget:	119,943.00 €
Duration:	June 1, 2015 – May 31, 2018
Members:	• Sjouke MAUW (Principal Investigator) • Rolando TRUJILLO RASUA (Collaborator) • Jorge Luis TORO POZO (Doctoral Candidate)
Area:	Information Security

Description

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

Transparent Yet Private Access to Medical Data

Acronym:	TYPAMED
Reference:	FNR/AFR project 7842804
PI:	Peter Y. A. RYAN
Funding:	FNR - AFR PhD
Duration:	Dec. 1, 2014 – Nov. 30, 2017

Members:
- Peter Y. A. RYAN (Principal Investigator)
- Dayana PIERINA BRUSTOLIN SPAGNUELO (Doctoral Candidate)
- Gabriele LENZINI (Co-Investigator)

Description

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

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

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

Urban Travel Time Estimation from Cooperative Data Gathering

Acronym:	OUTREACH
Reference:	I2R-DIR-AFR-090000
PI:	Thomas ENGEL
Funding:	FNR - AFR PhD
Budget:	120,000.00 €
Duration:	June 5, 2013 – Dec. 18, 2016
Members:	• Thomas ENGEL (Principal Investigator) • Stefanie OESTLUND (Project Coordinator) • Lara CODECA (Doctoral Candidate) • Raphaël FRANK (Scientific Contact)
Area:	Communicative Systems
Partner:	UCLA (non contracting)

Description

Over recent decades, traffic density has continuously increased. In many metropolitan areas, the road network has reached its limit and cannot easily be extended to meet the growing traffic demand. Consequently more and more drivers are stuck in traffic, causing billions of dollars worth of economic damage. Recently, a new monitoring paradigm has drawn the attention of the research community: floating car data directly retrieved from private vehicles. Anonymous information on the current speed and position is sent at regular intervals to a centralized server where it is aggregated to obtain a global picture of the traffic conditions in real time. It is important to take in account that the literature provides a lot of different methods to estimate the travel time in an extra-urban environment (e.g. highway) but unfortunately all these methods are not directly applicable in an urban setting due to the complexity of the environment itself. The aim of this project is to exploit the collected data (discovering new models applicable in the urban environment) and design dynamic routing algorithms, which take into account changing traffic conditions and predictable traffic patterns to provide the best possible equilibrium for the traffic and thus reduce individual and global traffic delays in urban environments.

Results

Within the project, Lara Codecà has been defended her doctoral thesis in November 2016. The thesis was evaluated as excellent from the members of the jury. In the research project, she presented a selfish traffic optimisation approach based on dynamic rerouting, able to mitigate the impact of traffic congestion

in urban environments on a global scale. The research areas are traffic flow models on urban and extra-urban environments, and intelligent transportations systems. The main contribution to the scientific community is ”Luxembourg SUMO Traffic (LuST) Scenario”, an open source traffic scenario built for SUMO and compatible with Veins. The project is hosted on GitHub (https://github.com/lcodeca/LuSTScenario).

The Luxembourg SUMO Traffic (LuST) Scenario is based on the mobility derived from the City of Luxembourg. The scenario is built for the Simulator of Urban MObiltiy (SUMO) and it is compatible with Vehicles in Network Simulation (VEINS) and Objective Modular Network Testbed in C++ (OMNet++), allowing it to be used in VANET simulations. The scenario has been presented at the IEEE VNC 2015 conference, where the publication received the Best Paper Award.

B.9 FNR - AFR PostDoc Projects

Probabilistic reliability management and its applications in argumentation theory and tracking objects

Acronym:	PRIMAT
PI:	Dragan DODER
Funding:	FNR - AFR PostDoc
Duration:	June 1, 2014 – June 1, 2016
Members:	• Dragan DODER (Principal Investigator) • Leon VAN DER TORRE (Scientific Contact)
Areas:	• Information Security • Intelligent and Adaptive Systems

Description

The project proposes two applications of probabilistic logic, one in the field of probabilistic argumentation, and the other in the field of probabilistic spatio-temporal reasoning. My first goal is to provide uniform logical formalization for different semantics for probabilistic argumentation frameworks in terms of probabilistic logic. The second goal is to develop a formal system in which one can interpret uncertainty of some systems for tracking moving objects. The central issue is to develop a complete axiomatic system for the appropriate spatio-temporal logic

Results

Development of a general propositional framework for reasoning about F-valued evaluations of propositional formulas of various probability logics, fuzzy logics and possibility and necessity logics, where F is a recursive L-structure, with L a countable first-order language. The central technical result is the proof of the strong completeness theorem for the introduced system (paper 1).

Development of a broad class of ranking semantics for abstract argumentation, which can compensate between the number of attackers and their strength (paper 2).

Development of a temporal logic for revision of strong beliefs and intentions. The main results are Katsuno-Mendelzon representation theorem and a complete axiomatization for this logic (papers 3,4).

1. On Evaluations of Propositional Formulas in Countable Structures, Aleksandar Perović, Dragan Doder, Zoran Ognjanović, Miodrag Rašković, FILOMAT, Volume 30, Number 1, pp 1-13, 2016
2. Ranking Arguments With Compensation-Based Semantics, Leila Amgoud, Jonathan Ben-Naim, Dragan Doder, Srdjan Vesic in KR 2016, Fifteenth International Conference on the Principles of Knowledge Representation and Reasoning, 12-21.
3. AGM-Style Revision of Beliefs and Intentions from a Database Perspective (Preliminary Version), Marc van Zee, Dragan Doder in NMR 2016, 16th International Workshop on Non-Monotonic Reasoning
4. AGM-Style Revision of Beliefs and Intentions, Van Zee, Marc; Doder, Dragan, in Proceedings of the 22nd European Conference on Artificial Intelligence (ECAI'16) (2016)

Subjective and Objective Uncertainty in Description Logics

Acronym:	SOUL
PI:	Giovanni CASINI
Funding:	FNR - AFR PostDoc
Duration:	July 1, 2015 – June 30, 2017
Member:	Giovanni CASINI (Principal Investigator)
Area:	Intelligent and Adaptive Systems

Description

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

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

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

Results

The semantic characterisation of strict and defeasible inference relations for the TBox and definition of implementable decision procedures for such inference relations in ALC is quite mature. We have reformulated for Description Logic some main semantic constructions based on ranked interpretations. Here we should take under consideration also the extension to DLs of other relevant constructions in the field.

We have been able to readapt the formulations for the language ALC also for the EL family, preserving the low computational complexity for some of them.

The addition of defeasible reasoning with classical ABoxes has been fulfilled w.r.t. the different entailment relations developed for the TBox. Two methods of applying defeasible reasoning to the ABox have been developed: one for expressive Description Logics, and another one for the EL family, that preserves the computational complexity of the decision problem, but is not applicable to more expressive logics.

The extension of the ABox-reasoning to ABoxes with parametrised conditionals still needs to be developed.

Publications:

- Rens G., Meyer T., Casini G. (2016) 'On revision of partially specified convex probabilistic belief bases' in Proceedings of the 22nd European Conference on Artificial Intelligence (ECAI-16), IOS Press, pp. 921-929.
- Casini G., Meyer T. (2016) 'Using defeasible information to obtain coherence', in Proceedings of the 15th International Conference on Principle of Knowledge Representation and Reasoning (KR-16), pp. 537-540, AAAI Press.
- Rens G., Meyer T., Casini G. (2016) 'Revising incompletely specified convex probabilistic belief bases' in Proceedings of the 16th International Workshop on Non-Monotonic Reasoning (NMR-16), pp. 133-142.

B.10 FNR - AFR Projects

Topology and Parameter Estimation in Power Systems through Inverter Based Broadband Stimulations

Acronym:	TPEPSIBBS
PI:	Juergen SACHAU
Funding:	FNR - AFR
Duration:	Nov. 1, 2012 – June 30, 2016
Members:	• Juergen SACHAU (Principal Investigator) • Surena NESHVAD (Doctoral Candidate)
Area:	Communicative Systems
Partner:	CREOS

Description

This thesis will propose a solution several power network challenges encountered with increasing Distributed Generation (DG) penetration. The three problems that will be addressed are islanding detection, online transmission line parameter identification and system topology identification. These tasks will be performed by requesting the DGs to provide ancillary services to the network operator. A novel and intelligent method will be developed for reprogramming the DGs Pulse Width Modulator, requesting each DG to inject a uniquely coded Pseudo-Random Binary Sequence along with the fundamental.

B.11 FNR - CORE Projects

A Theory of Matching Sessions

Acronym:	AtoMS
PI:	Peter Y. A. RYAN
Funding:	FNR - CORE
Duration:	March 1, 2015 – Feb. 28, 2019
Members:	• Peter Y. A. RYAN (Principal Investigator) • Jean LANCRENON (Researcher)
Area:	Information Security

Description

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

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

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

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

authentication mechanism used (PKI-based, password-based, attribute-based, etc...) and 2) independently the underlying intractability assumption (group-based, lattice-based, quantum-based etc.).

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

Applied Cryptography for the Internet of Things

Acronym:	ACRYPT
PI:	Alexei BIRYUKOV
Funding:	FNR - CORE
Duration:	June 30, 2013 – Dec. 31, 2016
Members:	• Alexei BIRYUKOV (Principal Investigator) • Johann GROSZSCHÄDL (Researcher) • Yann LE CORRE (Collaborator) • Dumitru-Daniel DINU (Doctoral Candidate) • Léo Paul PERRIN (Doctoral Candidate)
Area:	Information Security
Partner:	Fonds National de la Recherche

Description

The project ACRYPT aims at securing the so-called Internet of Things (IoT) by researching the design and implementation of lightweight cryptographic primitives for RFID tags, wireless sensor nodes, and other ”smart” objects.

Attack-Defence Trees: Theory Meets Practice

Acronym:	ADT2P
Reference:	C13/IS/5809105
PI:	Sjouke MAUW
Funding:	FNR - CORE
Budget:	494,000.00 €
Duration:	Sept. 1, 2014 – Aug. 31, 2017

Members:
- Sjouke MAUW (Principal Investigator)
- Ravi JHAWAR (Collaborator)
- Barbara Kordy (Collaborator)

Area: Information Security

Partners:
- Sintef
- THALES Research & Technology

Description

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

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

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

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

Results

- We have added more features to the ADTool, such as ranking and support to sequential gates. Such improvements have been reported in the following paper. Attack Trees for Practical Security Assessment: Ranking of Attack Scenarios with ADTool 2.0. O. Gadyatskaya, R. Jhawar, P. Kordy, K. Lounis, S. Mauw and R. Trujillo-Rasua. In Proc. of QEST, Springer, LNCS 9826, pp. 159-162, 2016.
- We gave support to the GramSec 2016 workshop.

- A framework for quantitative security analysis was developed. These results have been published in the paper: A Stochastic Framework for Quantitative Analysis of Attack-Defense Trees. R. Jhawar, K. Lounis and S. Mauw, In Proc. of STM, LNCS vol. 9871, 2016.
- A paper on Automating Cyber Defense Responses using Attack{Defense Trees and Game Theory was published in Proc. of ECCWS, pp. 163{172. The results of this paper were a side result of the project with Noumena Research Ventures Ltd., UK (MoD project) thatended in Dec 2015.

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

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

Description

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

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

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

The FIXPATTERN project aims at presenting new approaches to automated program repair. First, the project devises a novel pattern-based repair technique learned from human-written patches. This technique can outperform existing techniques based on random mutation with respect to patch quality and

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

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

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

Description

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

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

The RECOMMEND project aims at designing and building a bug fix recommen-

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

Boosting Security and Efficiency in Recommender Systems

Acronym:	BRAIDS
PI:	Qiang TANG
Funding:	FNR - CORE
Duration:	April 15, 2014 – April 14, 2017
Members:	• Qiang TANG (Principal Investigator) • Jun WANG (Doctoral Candidate)
Areas:	• Information Security • Intelligent and Adaptive Systems
Partners:	• Jiuyong Li (University of South Australia) • Irdeto

Description

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

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

Indoor Navigation with Ambient Radio Signals

Acronym:	INDOORS
Reference:	I2R-NET-PFN-14INDO
PI:	Andrei POPLETEEV
Funding:	FNR - CORE
Budget:	381,000.00 €
Duration:	Jan. 1, 2015 – Dec. 31, 2017
Members:	• Andrei POPLETEEV (Principal Investigator) • Stefanie OESTLUND (Project Coordinator) • Thomas ENGEL (Collaborator) • Foued MELAKESSOU (Doctoral Candidate)
Area:	Communicative Systems
Partner:	Microsoft Research

Description

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

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

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

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

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

Results

During 2016, the INDOORS project made important steps toward globally available indoor localization based on ambient radio signals. The project has developed methods for indoor positioning based on FM radio and DVB-T broadcasts, and produced an extensive dataset of georeferenced radio signals in several testbeds. These milestone achievements were complemented with a number of methodological contributions to the field.

Localised Legacies

Acronym:	LOCALE
Reference:	I2R-NET-PFN-13LOCA
PI:	Thomas ENGEL
Funding:	FNR - CORE
Budget:	815,000.00 €
Duration:	May 1, 2014 – April 30, 2017
Members:	• Thomas ENGEL (Principal Investigator) • Gabriela GHEORGHE (Researcher) • Nicolas LOUVETON (Researcher) • Stefanie OESTLUND (Project Coordinator)
Area:	Communicative Systems
Partners:	• Roderick McCall (LIST) • Amiperas a.s.b.l. • Centre National de l'Audiovisuel • Centre Virtuel de la Connaissance sur l'Europe • konviktsgaart

Description

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

Results

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

MAintaining Driving Skills in Semi-Autonomous Vehicles

Acronym:	MaDSAV
Reference:	I2R-NET-PFN-14MADS
PI:	Thomas ENGEL
Funding:	FNR - CORE
Budget:	903,000.00 €
Duration:	April 1, 2015 – March 31, 2018
Members:	• Thomas ENGEL (Principal Investigator) • Sébastien FAYE (Researcher) • Gabriela GHEORGHE (Researcher) • Nicolas LOUVETON (Researcher) • Stefanie OESTLUND (Project Coordinator)
Area:	Communicative Systems
Partners:	• Roderick McCall (LIST)

- University of Salzburg, Austria

Description

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

Results

In the MadSAV project, we continued our collaboration with the University of Salzburg and LIST in order to better understand how users will cope with semi-autonomous vehicles. This collaboration was embodied through preparatory work for a longitudinal in-home driving simulator study on the topic of driving skills decay. This preparatory work led to the definition of experimental scenarios. In particular, a driving simulation platform has been developped using the Unity game engine. This prototype allows to choose between different track layouts, to control a semi-autonomous vehicle, and to record and send core car telemetry data locally and on a remote server. In 2016, two papers prepared in collaboration have been accepted in one of the most relevant conference of the topic (ACM Automotive UI 2016).

MultimodAl MoBility Assistance

Acronym:	MAMBA
Reference:	I2R-NET-PFN-13MAMB
PI:	Thomas ENGEL
Funding:	FNR - CORE
Budget:	886,000.00 €
Duration:	April 1, 2014 – March 31, 2017

Members:
- Thomas ENGEL (Principal Investigator)
- German CASTIGNANI (Researcher)
- Sébastien FAYE (Researcher)
- Raphaël FRANK (Researcher)
- Marco RINALDI (Researcher)
- Stefanie OESTLUND (Project Coordinator)
- Thierry DERRMANN (Doctoral Candidate)
- Maximilien MOUTON (Doctoral Candidate)

Area: Communicative Systems

Partner: UCLA (non contracting)

Description

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

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

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

Optimizing urban transportation services may be achieved in different ways. For example, by limiting or avoiding unnecessary journeys, one can significantly disencumber the road network. Providing drivers with incentives not to take the car during rush hour, if possible, is currently investigated by a partnering FNR CORE iGear project1. The results of those studies will be used as an input in this project. Similarly, the tangible outputs of the still running FNR CORE MOVE project2 will provide important building blocks to achieve the holistic mobility framework.

By taking into account all those sources of information, we will be able to op-

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

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

Results

We further improved the implementation of the web-based itinerary planner for Luxembourg. The first prototype allowed users to plan trips using several intermediate location points. In particular, users could choose between different modes of transport or a combination of several modes, including those with time-dependent availability (i.e., bike-sharing). The system automatically computed interesting trips and suggested the best ones to the user. Current modes of transportation include car, bicycle, Veloh, public transport and walking.

Privacy Enhancing Techniques for Future Internet

Acronym:	PETIT
PI:	Andriy PANCHENKO
Funding:	FNR - CORE
Budget:	654,000.00 €
Duration:	Sept. 1, 2016 – Aug. 31, 2019
Members:	• Andriy PANCHENKO (Principal Investigator) • Augusto Wladimir DE LA CADENA RAMOS (Doctoral Candidate)
Area:	Communicative Systems
Partner:	University College London

Description

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

The goal of the proposal "Privacy-Enhancing Techniques for Future Internet" (PETIT) is to advance the state-of- the-art in the field of Privacy-Enhancing Techniques (PETs) in order to meet the challenges of the Future Internet and to create solid fundamentals for systems that empower users with tools for strengthening their privacy protection on the Internet. This will be done by analysing existing and developing new methods for privacy-friendly communication and by contributing to a broader understanding of the topic and its primitives within the community of researchers as well as the society. To this end, we will thoroughly analyze the susceptibility of existing PETs with respect to traffic analysis to make them robust against this kind of vulnerability. Afterwards, we will design and analyze methods for network discovery in untrustworthy environments in order to overcome scalability and trustworthiness issues in currently deployed systems. Moreover, we will address the topic of privacy-preserving routing by means of new communication paradigms for emerging protocols and performance-improved path selection metrics for better optimization of available resources and provision of an adequate quality of service.

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

Results

The project has officially started in September 2016 though there was a delay in hiring of researchers working for the project due to an extremely long administration process for getting work permits. The goal of the project is to analyze and improve existing and to develop new techniques for privacy enhancing technologies (PETs) on the Internet. To this end, the project started looking at the vulnerability of existing PETs with respect to traffic analysis. Here, one does not try to break the encryption but rather uses solely metadata such as packet sizes, their direction and sequences to deduce information about the content. The first step to perform an analysis is to collect representative datasets. The

collection of datasets was performed for two different scenarios: regular web browsing using the Tor anonymization network and accessing resources in the dark web (hidden services). These datasets allow evaluation of the strengths and weaknesses of considered PETs with respect to traffic analysis.

iGear

Acronym:	iGear
PI:	Thomas ENGEL
Funding:	FNR - CORE
Budget:	640,670.00 €
Duration:	May 1, 2014 – April 30, 2016
Members:	• Thomas ENGEL (Principal Investigator) • Tigran AVANESOV (Researcher) • Nicolas LOUVETON (Researcher) • Roderick MCCALL (Researcher) • Martin KRACHEEL (Doctoral Candidate)
Area:	Communicative Systems
Partner:	Roderick McCall (LIST)

Description

Traffic congestion is a problem in many countries and with government budgets being squeezed, large road infrastructure projects and roadside assistance systems are no longer feasible. The I-GEAR project specifically addresses these problems by looking at new ways to change driver behaviour through the use of incentives, social networking and pervasive gaming concepts.

Starting with the premise that sitting in a traffic jam is lost time and money, the I-GEAR project will explore how we can best channel the motivations of drivers in a way that will optimize traffic flow. For example, by encouraging counter intuitive driving strategies such as driving more slowly or taking a seemingly longer route. It will also explore social driving approaches such as car sharing or driving in a platoon (or convoy) to specific destinations. Our underlying idea is the people would rather do something else than sit in a traffic jam but that in order to encourage this behaviour we need to provide them with social, economic or personal incentives.

The project raises a number of challenges, which range from identifying the motivations of drivers and relevant incentives though to how to design in-car information systems that do not distract the driver. In order to support these areas the project will utilize a contextual design approach that places the driver from the outset at the very heart of the process which will include extensive fieldwork coupled with detailed laboratory and in-situ studies.

I-GEAR is also developing a testing platform that will allow companies and researchers to conduct human-factors tests under simulation and real world conditions using the same system. The system allows developers to test in-car applications using a range of devices including tablet PCs, mobile phones and eye trackers. The system provides tools to log behaviours and trigger specific interactions.

Results

The project developed an approach known as metaphorical games which involved finding a similar daily problem within a non-traffic context in order to test game design concepts. Following on from this work, the Driver Diaries methodology was developed and implemented. Driver Diaries is an approach using an online questionnaire, mobile application and focus groups in order to identify mobility patterns. The objective of this study was to understand the activities of commuters in Luxembourg and also to gain a better understanding of how possible it may be to alter the commuting habits of the population.

Two gamified applications were developed. LeaveNow, which explored the use of timeshift. This application contained three game formats, individuals, leader boards and teams (two being tested within this project). Here participants were awarded points depending on the deviation in terms of time from their initial plan. In contrast Commutastic combined the use of gamification elements with real world incentives. Its primary aim was to encourage people to undertake alternative activities rather than sitting in traffic. Therefore improving their overall commuting experience and encouraging them to use local facilities. Both applications changed the behaviour of between 13% and 57% of their users.

Three controlled studies have been performed on the topic of driver visual-manual distraction when interacting with In-Vehicle Infotainment System. The first one evaluated the feasibility of two use-cases envisioned for the IGear mobility applications. We found that visual-manual distraction induced by accurate finger pointing interaction was equivalent to that of inaccurate kinetic scrolling gesture. This points the necessity to provide the user with filtering capabilities using easy to reach buttons. In the second study we assessed driver's visual-manual distraction using standard smartphone interfaces in both real world and simulated environments. Additionally, we also measured brain activity using a commercial and affordable brain-computer interface (BCI). We demonstrated that the time spent by user while using the smartphone was equivalent in both simulated and real environment, which mean that this metric is robust enough to be assessed in driving simulator. Finally, we found that the Attention metric measured by the BCI device was sensitive to the two driving environment, participants were more "attentive" in the real-driving context, although we did not succeed to distinguished between the different user interfaces using this tool.

Finally, the last experiment investigated trade-off in the design of multi-screens user interfaces for the driver. We tested a range of trade-offs with the number of pages and the number of items on each screen. We also manipulated the type of

task that the user had to perform. We showed that a linear relationship between the visual times spent on the device and the number of screens when the task is to find a particular item among small groups. However, when the user had to memorize information across screens, the linear relationship disappeared. Those results point to the necessity to design interface taking into account both layout and the nature of the task. The experiments necessitated that we develop a simulator environment for controlling, and analysing the results. The platform called DriveLab that integrated a 3D Physics engine, mobile devices and eye-tracker. This platform is now licensed under the MIT open source license with the agreement of the University.

B.12 FNR - INTER Projects

CONtext and conTent Aware CommunicaTions for QoS support in VANETs

Acronym:	CONTACT
Reference:	I2R-NET-PFN-15CONT
PI:	Thomas ENGEL
Funding:	FNR - INTER
Budget:	1,346,000.00 €
Duration:	April 1, 2016 – March 31, 2019
Members:	• Thomas ENGEL (Principal Investigator) • Maria Rita PALATTELLA (Researcher) • Ridha SOUA (Researcher) • Antonio DI MAIO (Doctoral Candidate)
Area:	Communicative Systems
Partners:	• CarPostalSwiss • HES-SO Valais • University of Bern

Description

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

One of the main drivers of vehicular communications is the support for safety applications (e.g. accident, traffic jam notifications), which together with the more recent autonomous and coordinated driving applications require low end-to-end delay and no packet loss. These applications will share the vehicular

network resources with services with very different QoS requirements, such as infotainment services (e.g. live video streams, tourist information).

Due to the volatility of the vehicular environment, VANETs are characterized by a dynamic topology, short-lived intermittent wireless connectivity, and a cooperative and decentralized communication paradigm. All these features make the provision of high levels of QoS in VANETs a challenging task. Even more challenging is the support of a very diverse set of QoS requirements, due to the high heterogeneity of existing and prospective vehicular applications. The main existing approaches to QoS provisioning in VANETs either tackle this issue by focusing on a single layer of the network architecture, or focus on enabling a single specific QoS class of service. The CONTACT project aims at enabling Quality of Service (QoS) support in VANETs by taking a multi-pronged, cross-layer approach, by developing a set of communication techniques, which efficiently adapt, at the same time to the highly volatile and unstable vehicular environment, to content attributes and properties, and to application performance requirements. For this purpose, CONTACT will investigate the use of three different emerging approaches: Content-Centric Networking (CCN), Software Defined Networking (SDN), and Floating Content (FC). CCN implies introducing (content) name-based addressing instead of host-based addressing. This can be beneficial for communications in highly mobile network scenarios such as vehicular networks, where host addresses are not very meaningful. SDN, with its centralized view of network resources, may help in handling efficiently dynamic (re)allocation of resources/channels, and distribution of content (e.g., by reducing amount of Geobroadcast messages). Finally, FC techniques could be used to improve content availability for delay tolerant communications. The main idea behind CONTACT is to combine and exploit the advantages offered by CCN, SDN and FC, to offer a variety of QoS levels. The improvements in communication reliability, content availability, and end-to-end delay are pursued by adopting strategies based on the type of content (alerts, driving coordination, informational) as well as on its context attributes (such as location of origin, geographical range of interest, time of validity).

Results

In 2016, we identificated reference scenarios where approaches that combine Content centric networking, Floating content and Software Defined Networking (SDN) enable an innovative adaptive VANET architecture. We also investigated main open research challenges to improve content dissemination and reduce traffic by optimizing content replication without affecting content availability.

We designed an SDN based technique to improve Floating content performances by optimizing the geographical zone where the content float. This optimization is performed with the support of Software Defined Networking controller. The controller interacts with moving vehicles, collects relevant mobility data and build estimates of mobility parameters required for optimal Floating content dimensioning.

Cognitive Software Defined Network

https://cosdn.uni.lu/

Acronym:	CoSDN
Reference:	I2R-NET-PFN-12COSD
PI:	Thomas ENGEL
Funding:	FNR - INTER
Budget:	799,000.00 €
Duration:	Jan. 1, 2013 – March 31, 2016
Members:	• Thomas ENGEL (Principal Investigator) • Tigran AVANESOV (Researcher) • Miroslaw KANTOR (Researcher) • Luca LAMORTE (Researcher) • Maria Rita PALATTELLA (Researcher) • Thorsten Ries (Researcher) • Radu STATE (Researcher) • Emilia TANTAR (Researcher) • Stefanie OESTLUND (Project Coordinator) • Quentin Jerome (Doctoral Candidate)
Area:	Communicative Systems
Partner:	Warsaw University of Technology

Description

CoSDN stands for Cognitive Software Defined Networks, whose conceptualization is part of the diverse global activities around the design of the Future Internet. The CoSDN concept exploits the possibility of programming network behaviour that is enabled by the Software Defined Network (SDN) paradigm. It allows personalized network services, uses cognitive algorithms with learning in order to optimize the overall network performance and security. The CoSDN research and implementation is based on autonomic network management and control concepts. Such a combination of SDN with autonomic frameworks and cognitive algorithms is very novel. Even though there were significant research contributions in the past related to mentioned areas, but no research activities have been trying to combine the concepts together, since all the areas individually, are still experiencing a lot of research.

The CoSDN concept has the following novelties:

- exploits the possibility of programming of network behaviour that is enabled by the SDN paradigm;
- using SDN, it enables personalized (personalized QoS and security on per flow

basis) and advanced network services (multicast with QoS, ...);
- uses real-time cognitive algorithms with learning in order to optimize the overall network performance (including energy efficient approach (though this is not likely to be covered)) and to improve security;
- decomposition of network multi-criterion optimization problem into a set of quasi separated single criterion problems by 'cognitive interaction';
- network nodes exhibit some degree of self-configuration, and their re-configuration (including AAA), will be done in real-time during network operations in order to achieve better user experience ability to cope with dynamic topology changes;
- provides proactive fault management based on anomaly detection using machine learning approaches;
- implementations are based on autonomic network management and control frameworks.

The main innovation of the CoSDN concept is integration of SDN with autonomic network management and cognitive algorithms. From the scientific point of view the focus is put on the algorithmic side whereas SDN and Autonomic Network Management (ANM) concepts are used as tools/instruments. We would like to emphasise the seamless integration of security mechanisms and features. The main expected result of the project is a set of innovative algorithms and implementations for the CoSDN networks, with potential impact on standards related to Autonomics and OpenFlow-based SDN.

Results

The research activities carried in the framework of the CoSDN project have significantly contributed to enrich the International state-of-the-art in the field of Software Defined Networks (SDNs), on several aspects, as proved by the numerous papers published in International conferences and journals. First of all, the UL team has contributed to the open source OpenDayLight (ODL) project, as documented on the ODL wiki. The contribution has been twofold: enhance the Defense4all ODL Module, adding machine learning techniques, to detect pattern of attacks and use the topology manager ODL module, in combination with agents-based measurements, to localize issues in the network.

Based on the work performed, UL could provide some useful feedback to the ODL community, to improve future version of the ODL controller. This is only one of the project activity that has increased the international visibility of the PI and the entire UL research group. The integration of the ODL controller with the v6Sonar platform for operating monitoring and automating fault detection, has represented an innovative work, not performed before. The Proof of Concept of SDN-RADAR has been presented at a demo session at IM2015 conference, one of the most prestigious one, in the network management area. Moreover, the v6Sonar company has promoted the solution, which has found interest in several of their customers.

Formal Models for Uncertain Argumentation from Text

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

Description

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

Formal Models for Uncertain Argumentation from Text

Acronym:	FUnArT
PI:	Leon VAN DER TORRE
Funding:	FNR - INTER
Budget:	99,850.00 €
Duration:	May 1, 2015 – April 30, 2018
Member:	Leon VAN DER TORRE (Principal Investigator)
Area:	Intelligent and Adaptive Systems

Description

The topic of this project is formal models for uncertain argumentation from natural language text. Based on Dung's argumentation theory, integrating uncertainty into argumentation is gaining momentum. However, to the best of our knowledge, little attention has been paid to the modelling of uncertain argumentation in which the uncertainty of arguments is obtained mainly from text (e.g. biological papers).

The aim of this project is to develop theory and algorithms to formalize and evaluate the uncertain argumentation from natural language text, such that uncertain arguments represented by natural language can be formalized and their status be properly and efficiently evaluated. The prime objectives (challenges) of this project include:

(O1) to study how verbal and linguistic uncertainty of arguments can be formally modeled by mapping them to (constraints over) numerical values;
(O2) to study how uncertain argumentation is formalized on the basis of O1, by exploiting some existing uncertainty-handling formalisms such as possibility/ranking theory and subjective probability theory, etc. (O3) to study rationality postulates for the uncertain argumentation system formed in O2, and to develop a suitable semantics for it, such that the postulates can be satisfied;

(O4) to develop methods to prioritize the evaluation of arguments and their dynamics;
(O5) to develop algorithms and implement prototype systems based on methods in O4, and use these systems to empirically validate the methods and theories formulated in O1-O3.

The project will be carried out by the cooperation between the Individual and Collective Reasoning (ICR) group at the University of Luxembourg and the group of Beishui Liao of the Center for Study of Language and Cognition (CSLC) at Zhejiang University. The cooperation is founded on complementary researches of the two groups: In Beishui Liao's group, they have developed a series of innovative theories, algorithms and prototype systems for efficient computation of abstract argumentation semantics (both dynamic and static), while in ICR, we are working in the direction of combining logic and natural language, and have already conducted fundamental research on the topic of combining uncertainty and argumentation. In other words, ICR is good at resolving problems related to the objectives O1- O3, while CSLC has successful experience in realizing the objectives O4 and O5. So, the cooperation of our two groups is not only necessary, but also sufficient to implement the project.

ID-based Secure Communications system for unified access in IOT

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

Acronym:	IDSECOM
Reference:	I2R-NET-PFN-13IDSE
PI:	Thomas ENGEL
Funding:	FNR - INTER
Budget:	692,000.00 €
Duration:	April 1, 2014 – March 31, 2017
Members:	• Thomas ENGEL (Principal Investigator) • Miroslaw KANTOR (Researcher) • Luca LAMORTE (Researcher) • Stefanie OESTLUND (Project Coordinator) • Salvatore SIGNORELLO (Doctoral Candidate) • Radu STATE (Scientific Contact)
Area:	Communicative Systems
Partner:	Warsaw University of Technology

Description

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

The following proposal is based on the architecture that we presented mainly in [Mon13], and extends its functionalities by providing a self-managed and secure

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

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

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

Results

Within the project framework, the UL team has been investigating opportunities and security risks of the adoption of two novel network paradigms, namely, Software Defined Networking (SDN) and Information Centric Networking (ICN). In particular, the 3rd-year's research activities done by the UL mainly focused on the identification and evaluation of security risks introduced by leveraging SDN-based and ICN-based solutions via software simulations and experiments on physical and simulated testbed. Among the main outcomes of IDSECOM in 2016, there are publications in international conferences and journals, dissemination activities in third-party academic institutions (a project meeting was hosted by the AGH University in Krakow), a tutorial on cutting-edge technology for the network programmability was given at IEEE-Netsoft, the flagship conference of the IEEE SDN initiative. UL has been also working on the development on two different solutions: an open-source module to implement minimal ICN behavior in programmable software switches, and a Quality of Service (QoS) monitoring tool for SDN-Based network. Last but not least, a workshop related to the IDSECOM's research topics was submitted and accepted at the IEEE-IM held in May 2017 in Lisbon.

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:	FNR - INTER
Budget:	10,000.00 €
Duration:	Jan. 1, 2015 – Dec. 31, 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 (Université Pierre et Marie Curie) • Marc Pirlot (Université de Mons, Belgique) • Bernard Ries (Université Paris-Dauphine) • Fred S. Roberts (DIMACS (USA)) • CNRS

Description

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

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

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

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

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

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

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

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

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

Internet Shopping Optimisation Project

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

Acronym: IShOP

Reference: R-AGR-0453-10-V

PI:	Pascal BOUVRY
Funding:	FNR - INTER
Budget:	1,029,639.00 €
Duration:	March 1, 2014 – Feb. 28, 2017
Members:	• Pascal BOUVRY (Principal Investigator) • Grégoire DANOY (Researcher) • Bernabé Dorronsoro (Researcher) • Mateusz GUZEK (Researcher) • Johnatan Pecero (Researcher) • Sébastien VARRETTE (Researcher) • Raymond Joseph BISDORFF (Collaborator)
Area:	Intelligent and Adaptive Systems
Partners:	• Jacek Blazewicz (Poznan University of Technology) • Maciej Drozdowski (Poznan University of Technology) • Mikhail Kovalyov • Jakub Marszalkowski (Poznan University of Technology) • Jedrzej Musial (Poznan University of Technology) • Kamil Sedlak (Poznan University of Technology) • Malgorzata Sterna (Poznan University of Technology)

Description

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

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

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

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

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

Reasoning about Agreement Technologies

Acronym:	RAT
PI:	Leon VAN DER TORRE
Funding:	FNR - INTER
Duration:	Jan. 1, 2016 – June 30, 2016
Member:	Leon VAN DER TORRE (Principal Investigator)
Area:	Intelligent and Adaptive Systems
Partner:	Stanford University

Description

6 month sabbatical of Prof. van der Torre at CSLI Stanford, 2013.

Security Properties, Process Equivalences, and Automated Verification

Acronym:	SEQUOIA
PI:	Peter Y. A. RYAN
Funding:	FNR - INTER
Duration:	March 1, 2015 – Feb. 28, 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.

Specification logics and Inference tools for verification and Enforcement of Policies

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

Acronym:	SIEP
Reference:	I2R-DIR-PFN-11SIEP
PI:	Leon VAN DER TORRE
Funding:	FNR - INTER

Budget:	450,000.00 €
Duration:	June 1, 2012 – May 31, 2017
Members:	• Leon VAN DER TORRE (Principal Investigator) • Marcos CRAMER (Collaborator) • Diego Agustin AMBROSSIO (Doctoral Candidate)
Areas:	• Information Security • Intelligent and Adaptive Systems • Software and Systems
Partners:	• Guillaume Aucher (Université de Rennes) • Marc Denecker (Katholieke Universiteit Leuven) • Dov Gabbay (King's College) • Pieter van Hertum (Katholieke Universiteit Leuven)

Description

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

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

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

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

Results

We finished and published two papers that we started working on in 2015 (see publications below):

- A paper on a distributed (multi-agent) version of autoepistemic logic that can function as a says-based access control logic [1].
- A paper on the NP-completeness of a certain delegation revocation scheme [2].

We have developed a query-based decision procedure the well-founded semantics of dACL(ID) (distributed autoepistemic logic with inductive definitions). The decision procedure is designed in such way that allows to determine access rights while minimizing the information flow exchanged [3].

We have developed a theory of abstract normative systems capable of handling conjunction of outputs along with the aggregative form of cumulative transitivity, called cumulative aggregation. We provide technical details for the rep-

resentation results linking the semantics and proof theory for such systems [4].

Additionally, Marcos Cramer has written a paper on applying the axiomatic method to revocation schemes [5] and a technical report that contains the proofs of the theorems in that paper [6].

[1] Marcos Cramer, Pieter Van Hertum, Bart Bogaerts and Marc Denecker: Distributed Autoepistemic Logic and its Application to Access Control. International Joint Conference on Artificial Intelligence (IJCAI) 2016.
[2] Marcos Cramer, Pieter Van Hertum, Ruben Lapauw, Ingmar Dasseville: and Marc Denecker: Resilient Delegation Revocation with Precedence for Predecessors is NP-Complete. Computer Security Foundations Symposium (CSF) 2016.
[3] A Query-Driven Decision Procedure for Distributed Autoepistemic Logic with Inductive Definitions (Extended Abstract). (Diego Agustìn Ambrossio, Marcos Cramer.) Submitted to Logic and Ap- plications 2016 - LAP 2016.
[4] Diego Agustìn Ambrossio, Parent Xavier, and van der Torre Leon. Cumulative aggregation. In Olivier Roy, Allard Tamminga, and Malte Willer, editors, Deontic Logic and Normative Systems 13th International Conference, pages 1–15. College Publications, 2016.
[5] Marcos Cramer, Giovanni Casini: Postulates for Revocation Schemes International Conference on Principles of Security and Trust (POST) 2017.
[6] Marcos Cramer, Giovanni Casini: Postulates for Revocation Schemes – Technical Report. Published on ORBilu: http://orbilu.uni.lu/handle/10993/29413

B.13 FNR - Luxembourg (AFR - PHD) Projects

NAPEGRN

Acronym:	NAPEGRN
PI:	Sjouke MAUW
Funding:	FNR - Luxembourg (AFR - PHD)
Duration:	Jan. 15, 2014 – Jan. 14, 2017
Member:	Sjouke MAUW (Principal Investigator)

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

Acronym:	EARLY
PI:	Nicolas NAVET
Funding:	FNR - Luxembourg (AFR - PHD)
Budget:	119,943.00 €

Duration:	Oct. 1, 2015 – Sept. 30, 2018
Member:	Nicolas NAVET (Principal Investigator)
Areas:	• Computational Sciences • Security, Reliability and Trust in Information Technology
Partner:	Sakthivel Manikandan SUNDHARAM (Robert Bosch Engineering)

Description

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

B.14 FNR - Other Projects

Black Swan

Acronym:	Black Swan
Reference:	I2R-NET-PFN-15BLSW
PI:	Thomas ENGEL, Miroslaw KANTOR
Funding:	FNR - Other
Budget:	181,000.00 €
Duration:	July 1, 2015 – Feb. 29, 2016
Members:	• Thomas ENGEL (Principal Investigator) • Miroslaw KANTOR (Principal Investigator) • Emilia TANTAR (Researcher) • Anne OCHSENBEIN (Project Coordinator)
Area:	Communicative Systems
Partner:	Hitec

Description

The scope of this project is to provide a set of tools that allow identifying in what situation decision and disaster management policies fail. Instead of finding what plan fits perfectly a set of designed 'catastrophic events', we construct events that stress and break the perfect plan. This allows understanding how disruptive events, i.e. with respect to what is planed given a specific critical infrastructure, unfold and what additional measures one needs to put in place. Existing solutions, now on the market, do not offer such an option and focus almost exclusively on simulating pre-defined disaster scenarios.

The core of the project is constructed around rare event simulation techniques. Rare event techniques are ways to efficiently construct an out-of-the-charts event. Simulation remains a main component of how events are built and later analyzed. For this particular solution however, rare event techniques are used to construct disaster scenarios, subsequently analyzed via simulation. A set of scenarios is first proposed and simulated. Based on the results, i.e. stress put on a given disaster management plan, most difficult cases are selected and extended. The process is continued until disruptive effects can be observed. These effects are quantified as part of a post-analysis phase and show where and how the given plan fails.

The outcome of such a technique can be expressed in terms of occurrence and pathways. The spread of different (independent) events indicates what are the weak points of, in this case, a critical city infrastructure. Pathways, with respect to a single case, allow understanding how an event starts and subsequently unfolds. This provides, in turn, information about thresholds, critical levels or points where additional specific measures are needed.

Results

Black Swan as Proof-of-concept project resulted in two standalone solutions:

1. A standalone anomaly detection engine capable of running in real-time on the phone, with privacy by design included. The unique value proposition came from two facets: no sensitive data needed to be processed/ stored outside the phone, all processing was done in real time on the phone and no personal data stored on the device, only the personalized stochastic model of the user.
2. A holistic centralized anomaly detection system, dedicated to care facilities (e.g. nursing homes). The integrated SafeLive system englobes 4 components: *(i) Sensors that monitor events in real-time, in particular* built-in smartwatches' sensors; (ii) *(Optional) A scalable data store* (this role was played by the in house located, dedicated server); (iii) Analytics engine, the SafeLive anomaly detection module; *and (iv)* SafeLiveApp Android application, integrated in the study as of Phase 2.

The fully functional and operational centralized system, from the previous point (2) run for more than 5 months at the Residentie Edelweis, part of Senior

Living Group (Korian) in Belgium, with a total of 22 residents being informed and continuously monitored.

The triggered alerts were confirmed as true positives when compared with the nursing staff detailed written logs, at the end of the study. The novelty brought by the study was the detection of emotional distress with a high accuracy, using only the heart rate (non-medical grade) sensor.

As a side remark: one person which was flagged during the study with severe deterioration, after clinical checks was confirmed as having an initial form of Alzheimer. This later result shows the potential of SafeLive in preventive care and requires an in-depth study on its own to substantial support the preventive character. The residents provided a positive feedback and manifested a strong interest in keeping the wearable solution.

Combatting Context-Sensitive Mobile Malware

Acronym:	COMMA
Reference:	C15/IS/10404933
PI:	Olga GADYATSKAYA
Funding:	FNR - Other
Budget:	690,000.00 €
Duration:	April 1, 2016 – March 30, 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 appli-

cation whether it is malicious or not. For example, Google and Apple utilise their own on-market security services for application vetting. There exist also a number of third-party online security services offering to check security of mobile applications, such as VirusTotal and Andrubis.

Security services o ered by antivirus companies often rely on known malware signatures. Therefore these services do not detect zero-day malware samples that rely on new attacks or recently discovered vulnerabilities. This approach is not sufficiently reliable in the context of application market. Indeed, if Apple or Google will distribute zero-day malware, they will face a customer drain. Thus on-market security services typically use a combination of static and dynamic security checks that could reveal malicious behaviour. For example, if such service detects a known root exploit code or a suspicious API calls pattern, it can mark the sample in question as malicious. However, the recent generations of mobile malware that utilise obfuscation and dynamic code updates to thwart the security services pose a big challenge. Such dangerous samples can be often categorised as environment-sensitive or context-sensitive malware: they change their behaviour depending on the context. If they are able to detect that they are executed by a security service, they do not exhibit their malicious payload. If the payload is obfuscated (e.g., encrypted), it can be very challenging to identify malicious code in these samples.

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

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

Results

- The project has started on the 1st April 2016. MR has joined the COMMA team on the 1st November 2016. The project is in the process of hiring a technician.

Distance Bounding: a graph theoretical and formal approach

Acronym:	DIST
Reference:	C15/IS/10428112
PI:	Rolando TRUJILLO RASUA
Funding:	FNR - Other
Budget:	349,000.00 €
Duration:	April 1, 2016 – March 30, 2018
Members:	• Rolando TRUJILLO RASUA (Principal Investigator) • Yunior RAMIREZ CRUZ (Researcher) • Sjouke MAUW (Collaborator) • Jorge Luis TORO POZO (Collaborator)
Areas:	• Communicative Systems • Information Security

Description

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

The purpose of this project is to improve and formally verify the security guarantees of distance bounding protocols. In particular, we will focus on graph-based distance bounding protocols; a prominent family of distance bounding protocols based on random walks in graphs. Graph-based distance bounding protocols are efficient building blocks suitable to be implemented
in low-cost devices such as RFID tags. One based on trees and another one based on a peculiar graph structure named Poulidor, are the two graph-based distance bounding protocols proposed up to now. They remain unbroken, and

no other distance bounding protocol has proven to outperform them. Nevertheless, very little is known about this type of protocols. In this project, we will study the relation between graph properties and the security properties of graph-based distance bounding protocols. Our starting point is an observation that, to the best of our knowledge, has not been made before: the Poulidor graph belongs to the well known family of Cayley graphs. Therefore, understanding and studying the relation between graph-based hash functions (where Cayley graphs are used) and graph-based distance bounding protocols, may lead to better designs of this type of security protocols. We will also develop a symbolic approach for the formal verification of distance bounding protocols, which will be used to verify the security and correctness of our own solutions. The few existing symbolic approaches explicitly introduce either timestamps or a global notion of time to the security model. The novelty of our approach is that we expect to formalize the notion of proximity as an ordering problem instead. This keeps the model simple and more appealing to practitioners.

Results

- Optimality results on the security of lookup-based protocols. S. Mauw, J. Pozo and R. Trujillo-Rasua. In At the 12th Workshop on RFID and IoT Security (RFIDSec 2016), Hong kong, November 29, December 2, 2016, 2016.
- A class of precomputation-based distance-bounding protocols. S. Mauw, J. Toro-Pozo and R. Trujillo-Rasua. In 1st IEEE European Symposium on Security and Privacy (Euro S & P), Saarbrücken, Germany, March 21-24, 2016, 2016.

HotspotID-crowdsourced WiFi security

Acronym:	HotspotID
Reference:	I2C-NET-PFN-15HSID
PI:	Thomas ENGEL, Raimondas SASNAUSKAS
Funding:	FNR - Other
Budget:	271,000.00 €
Duration:	Jan. 15, 2016 – July 31, 2017
Members:	• Thomas ENGEL (Principal Investigator) • Raimondas SASNAUSKAS (Principal Investigator) • Daniel FORSTER (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Andriy PANCHENKO (Scientific Contact)
Area:	Communicative Systems
Partner:	Red Dog Communications s.a.

Description

Today's security solutions do not provide WiFi users with the tools needed to asses the security risks associated with connecting to a WiFi network, in real time. It is impossible to verify that you are connected to the legitimate access point (AP) and not an imposter (Evil Twin). Nor do you have any information about the access point. Likewise the owners of WiFi access points have no means to clearly identify themselves for their users, so they will not be mistaken for an imposter.

Hotspot ID offers WiFi users a FREE mobile app which fingerprints all WiFi connections made and registers this (crowdsourced) data on the central server for analysis & evaluation. The server tracks all the data it receives to generate a reputation score for each registered access point (AP). The server returns to the app all relevant data for the WiFi network and warns the user if connected to an unsafe AP (i.e. Evil Twin). We propose to WiFi owners to certify their Access Points - a subscription based service to register verified network data in the system. This permits better attack detection as the live fingerprints are checked against verified networks, instead of crowdsourced records. This results in better security for the users of Certified AP.

Results

During the year 2016, different aspects of the project advanced. In close collaboration with the CNPD and the university's data protection officer, legal problems with regard to the collection of wireless access point information could be solved. The project has a legal basis now. Additionally, the access point fingerprinting algorithm advanced to reduce the amount of false positives in recognition of fake access points. A complete rework of the Android application went online. The new application exhibits a fresh user interface. With release of the new application, HotspotID's user base grew. Further, the web portal for certification partners was completely refactored. Besides a new user interface, the certification partner portal now offers a variety of visualizations of statistics with regard to the certified access points of a partner. Certification partners now get a comprehensive overview of the usage of their access points, their users, uploaded fingerprints and evil twin alerts.

Security and Privacy for System Protection

Acronym:	PRIDE: SPsquared
PI:	Sjouke MAUW
Funding:	FNR - Other
Duration:	Jan. 1, 2016 – Dec. 31, 2021
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)

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.

The interactive eyeglasses for mobile, perceptual computing

Acronym:	eGlasses
Reference:	I2R-NET-PFN-12CHIS
PI:	Thomas ENGEL

Funding:	FNR - Other
Budget:	344,000.00 €
Duration:	Jan. 1, 2014 – Dec. 31, 2016
Members:	• Thomas ENGEL (Principal Investigator) • Sébastien FAYE (Researcher) • Gabriela GHEORGHE (Researcher) • Nicolas LOUVETON (Researcher) • Roderick MCCALL (Researcher) • Stefanie OESTLUND (Project Coordinator)
Area:	Communicative Systems
Partners:	• Roderick McCall (LIST) • Gdansk University of Technology • University of Applied Sciences Upper Austria

Description

The eGlasses project is focused on the development of an open platform in the form of multisensory electronic glasses and on the integration and designing of new intelligent interaction methods using the eGlasses platform. This is an initial development focused on long-term research and technological innovation in perceptual and super-perceptual (e.g. heart rate, temperature) computing. It is an emerging technology that is also focused on the creation of mobile, perceptual media. Perceptual media refers to multimedia devices with added perceptual user interface capabilities. These devices integrate human-like perceptual awareness of the environment, with the ability to respond appropriately. This can be achieved by using automatic perception of an object's properties and delivering information about the object's status as a result of reasoning operations. For example, using the eGlasses, it will be possible to control a device, which is recognized within the field of view using the interactive menu, associated with the identified device. Other examples include presentation of a recognized person name, recognition of people with abnormal physiological parameters, protection against possible head injuries, etc.

The platform will use currently available user-interaction methods, new methods developed in the framework of this project (e.g. a haptic interface) and will enable further extensions to introduce next generation user-interaction algorithms. Furthermore, the goal of this project is to propose and evaluate new and intelligent user interactions, which are particularly useful for healthcare professionals, people with disabilities or at risk of exclusion, and to create and evaluate behavioural models of these mobile users. The main scientific and technological objectives of the project are to design and evaluate the following:

- eye-tracking hardware and algorithms for a user, who is mobile in a noisy real world environment,
- algorithms for perceptual media and for super perceptual computing,
- methods for locating objects and guiding vision towards the identified objects,
- methods of interactions with users and objects (menu of activities for the

identified person or object),
- a haptic interface in a form of a peripheral proximity radar,
- methods for the recognition of the user's own gestures and recognition of gestures of the observed person,
- methods for context-aware behavioural studies,
- methods for reference applications.

The result of the project will be an open platform in the form of multisensory electronic multimedia glasses and a set of new methods for intelligent user interactions, especially in the context of perceptual media.

Results

We developped a platform able to detect, collect and analyse activity- and context-related metrics. The eGlasses Logger app is entirely customizable and works on traditional Android smartglasses and also on the official project hardware. New experiments were conducted with the aim of using this platform to collect activity- and context-related metrics. The EPSON Moverio BT-200 smartglasses that were used allowed us to collect the following metrics: raw data from gyroscope (x, y, z axes), accelerometer, compass, ambient sound, speech, head gesture and current activity using Android ActivityRecognitionApi method. Using different time series analysis techniques and an activity diary completed by the user, we distinguished two classes of activity, i.e., micro- and macro-activities. On the one side, micro-activities are activities detectable from wearable sensors measurements that relate to activities located in the cognitive or even in the upper-bound biological bands. On the other side, macro-activities are activities located in the rational or in the lower-bound social bands and which need integration of several source of information in order to be understood. Micro-activities give information about plan execution while macro-activity gives information about goal and context, which is particularly important in context-sensitive systems. After a review of concepts underlying authentication methods on smartglasses, we defined and developed four alternative methods: (1) PIN using visual keyboard and touchpad; (2) PIN using Voice recognition; (3) PatternLock using touchpad; and (4) PatternLock using head gesture. Participants have to enter fixed-length passwords using the four methods. Completion time, error rate and subjective assessments are collected. Data are being collected and results will be presented in 2017.

Virtual Security Operation Center as a Service

Acronym:	VSOC
Reference:	I2R-NET-PFN-14VSOC
PI:	Radu STATE
Funding:	FNR - Other
Budget:	122,000.00 €

Duration:	Jan. 15, 2015 – Jan. 14, 2016
Members:	• Radu STATE (Principal Investigator) • Fabian LANZE (Researcher)
Area:	Communicative Systems
Partner:	Telindus

Description

Virtual Security Operation Center as a Service (VSOCS) is the result of a FNR PoC project aiming at an easy-to-deploy, cloud-based security analytics engine. Supporting various data sources, VSOC uses machine learning, big data processing, and integrates existing SIEM with advanced analytical capabilities, which have been developed by the Secan-Lab / ComSys research group. VSOC coexists smoothly with existing technologies and operates at a significantly increased speed with reduced investment requirements.

B.15 Horizon 2020 (EU) Projects

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

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

Acronym:	ATENA
Reference:	R-AGR-3026-10-Z
PI:	Thomas ENGEL
Funding:	Horizon 2020 (EU)
Budget:	6,889,925.00 €
Duration:	May 2, 2016 – May 1, 2019
Members:	• Thomas ENGEL (Principal Investigator) • Florian ADAMSKY (Researcher) • Ridha SOUA (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Andriy PANCHENKO (Scientific Contact)
Area:	Communicative Systems

Partners:
- Crat
- CREOS
- Enea
- Iec
- Institute of Baltic Studies
- itrust Luxembourg
- Multitel
- Sapienza SL
- SES Spa
- Swde
- Uniroma3
- University of Coimbra

Description

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

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

Results

In 2016, we studied industrial Control Systems and specifically SCADA systems: architecture, key components and networks protocols. We identificated main

security challenges faced by SCADA systems nowadays. In particular, SCADA are prone to numerous threats due to the large deployment area, the standardization of communication protocols, the distributed operating mode, complex hardware components and growing interconnectivity (cloud, Internet of things, integration of SDN in SCADA systems). Furthermore, we investigated requirements for the design of Intrusion detection systems based on the inputs from end users (CREOS, SDWE).

Building an IoT OPen innovation Ecosystem for connected smart objects

http://biotope-h2020.eu/

Acronym:	bIoTope
PI:	Yves LE TRAON
Funding:	Horizon 2020 (EU)
Budget:	598,750.00 €
Duration:	Jan. 1, 2016 – Dec. 31, 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-3109-10-Z
PI:	Thomas ENGEL
Funding:	Horizon 2020 (EU)
Budget:	999,547.00 €
Duration:	Nov. 1, 2016 – Oct. 31, 2018
Members:	• Thomas ENGEL (Principal Investigator) • Stefanie OESTLUND (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Latif LADID (Scientific Contact)
Area:	Communicative Systems
Partners:	• BII Group Holdings • Bupt • Caict • Cas • Huawei • Hust • Inno AG • Interinnov • Mandat International • Martel Consulting • Spi • UNIS • Upmc

Description

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

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

EXCITING will produce Best Practice guidelines for establishing and operating practical joint collaborations, in order to stimulate further such co-operations

in the future on IoT and 5G Large Scale Pilots. As a result of the above investigations EXCITING will produce a roadmap showing how research and innovation ecosystems, policy, standardisation, interoperability testing and practical Large Scale Pilots should be addressed during the H2020 timeframe, and make recommendations for optimising collaboration between Europe and China for IoT and 5G.

Results

In November 2016, a kick-off project meeting organised. In addition, the organisation of the Advisory Board of the project was started. We had successful negotiations with the European Commission for the project kick-off.

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

http://www.privacyflag.eu/

Acronym:	Privacy Flag
Reference:	I2R-NET-PEU-15PFLG
PI:	Thomas ENGEL
Funding:	Horizon 2020 (EU)
Budget:	4,000,000.00 €
Duration:	May 1, 2015 – April 30, 2018
Members:	• Thomas ENGEL (Principal Investigator) • Karim Ahmed Awad El-Sayed EMARA (Researcher) • Daniel FORSTER (Researcher) • Fabian LANZE (Researcher) • Stefanie OESTLUND (Project Coordinator) • Andriy PANCHENKO (Scientific Contact)
Area:	Communicative Systems
Partners:	• Archimede Solutions • CTI - Computer Technology Institute and Press ”Diophantus” • Dunavnet • HWC • Internationak Association of IT Lawyers • Istituto Italiano per la Privacy

- Mandat International (International Cooperation Foundation)
- OTE
- University of Lulea
- Velti

Description

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

1. Develop a highly scalable privacy monitoring and protection solution with:
   - Crowd sourcing mechanisms to identify, monitor and assess privacy-related risks;
   - Privacy monitoring agents to identify suspicious activities and applications;
   - Universal Privacy Risk Area Assessment Tool and methodology tailored on European norms on personal data protection;
   - Personal Data Valuation mechanism;
   - Privacy enablers against traffic monitoring and finger printing;
   - User friendly interface informing on the privacy risks when using an application or website.
2. Develop a global knowledge database of identified privacy risks, together with online services to support companies and other stakeholders in becoming privacy-friendly, including: - In-depth privacy risk analytical tool and services; - Voluntary legally binding mechanism for companies located outside Europe to align with and abide to European standards in terms of personal data protection; - Services for companies interested in being privacy friendly; - Labelling and certification process.
3. Collaborate with standardization bodies and actively disseminate towards the public and specialized communities, such as ICT lawyers, policy makers and academics. 11 European partners, including SMEs and a large telco operator, bring their complementary technical, legal, societal and business expertise; strong links with standardization bodies and international fora; and outcomes from over 20 related research projects. It will build a privacy defenders community and will establish a legal entity with a sound business plan to ensure longterm sustainability and growth.

Results

In 2016, Secan-Lab continued its research in analyzing and improving Tor with regard to website fingerprinting, scalability and path selection. A browser ex-

tension is being developed to select Tor relays based on their performance and geographical region compared to the client. This tuned modification will enhance the user experience when using the anonymity network. In addition, we have supported other partners in resolving security and privacy technical problems. We implemented several automatic checks that assess the popular security and privacy vulnerabilities of websites such as the authenticity of the certificate chain, strength of cipher suites and the support for DNSSec, HTTP Strict Transport Security and HTTP Public Key Pinning.

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

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

Acronym:	F-INTEROP
PI:	Thomas ENGEL
Funding:	Horizon 2020 (EU)
Budget:	2,998,000.00 €
Duration:	Nov. 1, 2015 – Sept. 30, 2018
Members:	• Thomas ENGEL (Principal Investigator) • Luca LAMORTE (Researcher) • Maria Rita PALATTELLA (Researcher) • Stefanie OESTLUND (Project Coordinator)
Area:	Communicative Systems
Partners:	• Device Gateway SA • EANTC AG • IMINDS • INRIA • Institut europeen des normes de telecomminication • Mandat International (International Cooperation Foundation) • The connected digital economy catapult limited • Universite Pierre et Marie Curie • University of Luxembourg

Description

F-Interop will develop and provide remotely accessible tools to support and accelerate standardization processes and products developments, by offsetting several cost and time barriers. It will research and develop a new FIRE experi-

mental platform to support the development of new technologies and standards, from their genesis to the market for: online interoperability tests and validation tools, remote compliance and conformance tests, scalability tests, Quality of Service (QoS) tests, SDN/NFV interoperability tools, Online privacy test tools, energy efficiency tools.

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

Results

In September, the project F-INTEROP passed its first review with good remarks from the European commission. During last year, UL worked on several aspects. First of all, we contributed on the definition of Software Defined Network (SDN)-based Quality of Service (QoS) and privacy requirements for the platform and we provided a “Privacy by design” report. Such report contains all the platform requirements for ensuring privacy of the test results, confidentiality of the experiment and other considerations based on the upcoming General Data Protection Regulation (GDPR) framework defined by the European Commission.

UL is currently working on the two different testing tools. A performance and a privacy testing tools. The first one is based on SDN-enabled networks, allowing monitoring the status of network with both active and passive mechanisms. A first implementation of it was already presented during the EuCNC 2016 conference in Athens where F-INTEROP was presented with its first two running demos.

The second testing tools is about privacy aspects. As security is a one of the major consideration for an Internet of Things (IoT) platforms, UL is working on a solution based on two different approach. Firstly, on a tool to search if any personal data is leaked by the tested Implementation Under Test (IUT) IoT device. The tool takes advantage of the F-Interop packet analyzer used for the

conformance and interop tests to look for data string that looks as personal data identifier of information. The second one is investigating how an adversary may get "sensitive" information (e.g., results of a test running on the shared platform) by passively observing patterns of encrypted communication, based for instance on packets size, packet ordering, packet direction, and timing.

Mining and Reasoning with Legal Texts

http://www.mirelproject.eu/

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

Description

The MIREL project will create an international and inter-sectorial network to define a formal framework and to develop tools for MIning and REasoning with Legal texts, with the aim of translating these legal texts into formal representations that can be used for querying norms, compliance checking, and decision support. The development of the MIREL framework and tools will be guided by the needs of three industrial partners, and validated by industrial

case studies. MIREL promotes mobility and staff exchange between SMEs to academies in order to create an inter-continental interdisciplinary consortium in Law and Artificial Intelligence areas including Natural Language Processing, Computational Ontologies, Argumentation, and Logic & Reasoning.

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

Processing legal language for normative Multi-Agent Systems

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

Description

The ProLeMAS project reconnects the textual representation of norms in legal documents with the logical representation of their meaning, in order to improve acceptability by legal practitioners of automatic reasoning on norms. It makes a bridge between deontic logic and natural language semantics, focusing on the modalities and the defeasible conditionals conveyed by norms. More generally, ProLeMAS develops a framework with a natural language processing pipeline able to computationally obtain explicit representations from legal text that is effective and acceptable to lawyers. ProLeMAS opens a new research trend in normative Multi-Agent systems, along three dimensions. First, ProLeMAS enhances the expressive power of deontic logic to formalize the meaning of the phrases constituting sentences, including a wide range of fine-grained intra-sentence linguistic phenomena. Natural language semantics is not part of the NorMAS roadmap, although it has been identified as a critical issue by the current scientific community in deontic logic and normative systems, as witnessed by the special focus on "deontic modalities in natural language" at the DEON 2014 conference. Secondly, ProLeMAS defines a first-order decision

theory able to make inferences on norms from legislation as well as agents' goals and attitudes. Third, ProLeMAS will develop a prototype able to extract obligations from laws and codify them in the chosen object logic. No system developed so far by members of the NorMAS community is capable of processing legal documents available on the Web. The prototype that will be implemented in ProLeMAS will use and extend two specific tools: the TULE parser and the Tacitus system.

Results

In 2016, Livio Robaldo worked on aiming at using reification to fill the gap between the current formalizations in deontic logics and the richness of natural language semantics. He developed a new formalism called 'reified input/output logic' for representing natural language norms in a deontic settings. The full definition of the formalism will appear on the Journal of Logic and Computation; preliminary conference paper about it are: [Robaldo and Sun, 2016], [Sun and Robaldo, 2016b], [Robaldo et al, 2016].

Reified Input/Output logic incorporates main insights of Input/Output logic (defined by prof. van der Torre during his academic career) with techniques coming from the literature in Natural Language Semantics (specifically, reification). Reified Input/Output logic has been proposed as the underlying logical framework of the CORE project DAPRECO, which has been retained for funding on October 2016. The framework that will be developed in DAPRECO is described in [Bartolini et al., 2016a] and [Bartolini et al., 2016b].

In parallel, Livio Robaldo developed NLP procedures for dealing with legal texts: converting legal documents in the Akoma Ntoso standard (www.akomantoso.org) and identifying named entities and other relevant information from legal texts, he worked on NLP statistical procedures for classifying and carrying out textual inferences, legal ontologies, and he investigated reasoning techniques, norm emergence/creation and games in deontic logic. The results of these activities have been published in the papers: [Santos et al., 2016], [Adebayo et al., 2016], [Sun and Robaldo, 2016b], [Sun and Robaldo, 2016b], and [Sun and Robaldo, 2016a]. Those techniques are integrated in the Eunomos system [Boella et al, 2016].

[Boella et al, 2016] G. Boella, L. Di Caro, L. Humphreys, L. Robaldo, P. Rossi, L. van der Torre: **Eunomos, a legal document and knowledge management system for the Web to provide relevant, reliable and up-to-date information on the law**, *Artificial Intelligence and Law*, Vol. 24, Issue 3.
[Santos et al., 2016] C. Santos, V. Doncel, P. Casanovas, L. Robaldo and L. van der Torre: **An Approach for Modelling Relevance in Legal Ontologies**, *in proc. of the VII Workshop on Artificial Intelligence and the Complexity of Legal Systems (AICOL), Nice, France, 2016.*
[Adebayo et al., 2016] K. Adebayo, L. Di Caro, L. Robaldo and G. Boella: **Textual Inference with Deep Learning Technique**, *in proc. of the 28th Annual Benelux Conference on Artificial Intelligence (BNAIC2016). Amsterdam, The Netherlands, 2016.*
[Bartolini et al., 2016a] C. Bartolini, G. Lenzini and L. Robaldo: **Towards legal**

compliance by correlating Standards and Laws with a semi-automated methodology, *in proc. of the 28th Annual Benelux Conference on Artificial Intelligence (BNAIC2016). Amsterdam, The Netherlands, 2016.*
[Bartolini et al., 2016b] C. Bartolini, A. Giorgiu, G. Lenzini and L. Robaldo: **A Framework to Reason about the Legal Compliance of Security Standards**, *in proc. of the 10th International Workshop on Juris-informatic (JURISIN 2016). Tokyo, Japan, 2016.*
[Robaldo and Sun, 2016] L. Robaldo, X. Sun: **Reified Input/Output logic - a position paper**, *in proc. of Workshop on Artificial Intelligence for Justice (AI4J), collocated at the 22nd European Conference on Artificial Intelligence (ECAI 2016), The Hague, The Netherlands.*
[Sun and Robaldo, 2016b] X. Sun, L. Robaldo: **Ali Baba and Thief, Norm Emergence in Games**, *in proc. of International Conference on Principles and Practice of Multi-Agent Systems (PRIMA 2016). Phuket, Thailand, 2016.*
[Robaldo et al, 2016] L. Robaldo, L. Humphreys, X. Sun, L. Cupi, C. Santos and R. Muthuri: **Combining Input/Output logic and Reification for representing real-world obligations**, *in post-proceedings of the 9th International Workshop on Juris-informatic (JURISIN 2015). Lecture Notes in Artificial Intelligence.*
[Sun and Robaldo, 2016b] X. Sun, L. Robaldo: **Logic and games for ethical agents in normative multi-agent systems**, *In Vicente Julian Michael Rovatsos, George Vouros, editor, 13th European Conference on Multi-Agent Systems/3rd International Conference on Agreement Technologies, volume 9571 of Lecture Notes in Computer Science. Springer.*
[Sun and Robaldo, 2016a] X. Sun, L. Robaldo: **Norm Creation in Proposition Control Games**, *proc. of Chinese Conference on Logic and Argumentation.*

Training Augmented Reality Generalized Environment Toolkit

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

Acronym:	TARGET
Reference:	I2R-NET-PEU-15TARG
PI:	Thomas ENGEL
Funding:	Horizon 2020 (EU)
Budget:	6,000,000.00 €
Duration:	May 1, 2015 – April 30, 2018
Members:	• Thomas ENGEL (Principal Investigator) • Nicolas LOUVETON (Researcher) • Aurel MACHALEK (Researcher) • Stefanie OESTLUND (Project Coordinator)

Area: Communicative Systems

Partners:
- Roderick McCall (LIST)
- Arttic
- ATRISc
- Cleveland Fire Authority
- Ecole Nationale Superieure de Police
- Estonian Academy of Security Sciences
- Fachhochschule der Polizei des Landes Brandenburg
- Fraunhofer Institute for Transportation and Infrastructure Systems
- German Police University
- Guardia Civil
- Inconnect
- Institut de Seguretat Pública de Catalunya
- International Security and Emergency management Institute
- ISCC International Security Competence Centre
- Oslo Centre of Science in Society (OCSS)
- VectorCommand LtD

Description

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

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

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

lution will support user-technologist dialogue. The TARGET Ecosystem will enable sustainable impact, commercial uptake and synergies at EU level.

Results

The mission of TARGET is to develop trial and assess a comprehensive open distributed pan-European Platform for serious gaming leveraging state-of-the-art decision support tools, for the training and competence assessment of Security Critical Agents (SCA) including counterterrorism units, border guards and first responders (police, firefighters, ambulance services, civil security agencies or critical infrastructure operators). TARGET favours joint development of serious gaming Training Content (TC) and collaborative transnational training. TARGET triggered the emergence of a marketplace for sharing, licensing and paying for serious TC between SCA, leveraging the existing European wealth of exercises.

Unavailable real-source information was substituted by AVR (Augmented / Virtual Reality - multimedia, synthetic role players). Near-real, all-encompassing and non-linear experiences enabled high degrees of dynamics and variability. The distributed Open TARGET Platform provided extensible standards driven methods to integrate simulation techniques and AVR technology with existing SCA training equipment and be customisable to local languages, national legal contexts, organisational structures, established standard operational procedures and legacy IT systems.

B.16 International call ANR - FNR Luxembourg () Projects

Amber: Towards Fog Environments and Opportunistic Management of converged IoT and Cloud computing

Acronym:	Amber
PI:	Yves LE TRAON
Funding:	International call ANR - FNR Luxembourg ()
Budget:	620,000.00 €
Duration:	Jan. 1, 2016 – Dec. 31, 2018
Members:	• Yves LE TRAON (Principal Investigator) • Jacques KLEIN (Supervisor / Scientific Advisor) • François FOUQUET (Responsible Researcher (in case of a delegation to lead a project))
Partners:	• Olivier Barais (Université de Rennes) • Benoit Baudry (INRIA)

- Johann Bourcier (University of Rennes 1)
- Antoine Cabot (b<>com)

Description

Fog computing has been coined has an answer to the growing success of Cloud computing and the emergence of Internet of Things. The emergence of the Internet of things devices and their integration in cloud environment have raised several concerned around the capacity of the network infrastructure to handle massive data transfer and end user quality of services regarding communication delay and data privacy. Fog computing is characterized by the extension of cloud by the inclusion of user personal devices directly hosted in their private home. The Amber project focuses on the problem of dynamically optimizing the placement and configuration of software processes in fog computing. The AMBER project will leverage software engineering methods, modelling techniques and evolutionary algorithms to build fog elasticity engines to place and configure software while simultaneously optimizing multiple criterion such as privacy, security, energy consumption, cost and performance objectives.

B.17 UL (PUL) Projects

Cognitive Aspects of Formal Argumentation Theory

Acronym:	CAFAT
PI:	Leon VAN DER TORRE
Funding:	UL (PUL)
Budget:	350,000.00 €
Duration:	Oct. 1, 2016 – July 31, 2018
Member:	Leon VAN DER TORRE (Principal Investigator)
Areas:	• Computational Sciences • Educational Sciences

Description

Formal Argumentation Theory is a popular framework for capturing deliberative aspects of reasoning in Artificial Intelligence. While it has been thoroughly studied theoretically and implemented in many systems, its relation to actual human reasoning has not been studied much. This project will conduct an empirical cognitive study that tests assumptions and predictions of Formal Argumentation Theory. In order to minimize the interference with domain-specific knowledge, the arguments used in the study will be on conflicts arising in informal mathematical and metalinguistic reasoning.

The project cost will be 350k€, out of which 306k€ are staff costs.

Scalable External Control of Probabilistic Boolean Networks

Acronym:	SEC-PBN
PI:	Jun PANG
Funding:	UL (PUL)
Budget:	336,000.00 €
Duration:	July 1, 2016 – June 30, 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.

Time Predictable Embedded Systems

Acronym:	TIME
PI:	Nicolas NAVET
Funding:	UL (PUL)
Budget:	156,822.00 €
Duration:	July 1, 2016 – June 30, 2019
Members:	• Nicolas NAVET (Principal Investigator) • Sebastian ALTMEYER (Co-Supervisor)

Area: Security, Reliability and Trust in Information Technology

Description

In our everyday life, we interact with a huge number of computer systems embedded into larger devices. Examples are phones, cars, home and factory appliances, airplanes and many more. Many of these devices are subject to real-time constraints. Real-time means that the correctness of a system is not only a functional (the right result), but also an extra-functional property (the right result at the right time). Currently, the development of such systems is very challenging as high-level modelling tools only capture the functional behaviour, whereas the timing behaviour simply happens: as the exact timing behaviour depends on the precise target architecture, little to no knowledge about the exact timing is available at an early design-phase.

The aim of the project is to re-think the development process of real-time embedded systems and to devise a timing-aware model-driven design process. In stark contrast to the current best-practice approach, we aim at a timing verification already at the modelling level, i.e., right from the start. To lift the timing behaviour from the low-level architecture to the high-level model, we propose to use model interpretation instead of compilation. The model interpreter on the target architecture must provide the same timing behaviour as a model verifier on the host machine, where the high-level model is developed and verified. We refer to this property as timing equivalence. We believe that the strongly simplified and accelerated model development and model verification (including functional verification and timing verification), will outweigh by far the additional overhead due to model interpretation on the target architecture. In the project, we will put this assumption to the test and develop a prototype of the timing-aware model-driven design process.

Unclonable Networks for Identification using Cholesteric Emulsions

Acronym: UNIQUE

PI: Jan LAGERWALL, Gabriele LENZINI

Funding: UL (PUL)

Budget: 397,000.00 €

Duration: April 1, 2015 – March 31, 2018

Members:
- Jan LAGERWALL (Principal Investigator)
- Gabriele LENZINI (Principal Investigator)
- Samir OUCHANI (Collaborator)
- Peter ROENNE (Collaborator)
- Peter Y. A. RYAN (Collaborator)

Description

We live in an era where digital services are offered ubiquitously, with increasingly sensitive and valuable transactions being effectuated on-line. This creates an urgent need to uniquely and safely identify and authenticate persons and goods. At the same time we demand personal integrity and there is a strong - and well-founded - reluctance to allow authorities to register biometric data, challenging many approaches to ensure security and privacy. A promising approach to solving the problem is to introduce an artificial identity pattern (IDP) into the authentication chain. IDPs should be as unique as the fingerprint or iris of a person, unclonable, but allow production at low cost in enormous quantities without risking overlap between IDPs. They should be robust and easy to read out quickly and repeatedly for identification and authentication purposes. UNIQUE aims to develop such a pattern, using microfluidics to produce an emulsion of cholesteric liquid crystal shells in specific 2D arrangement. The spherically symmetric photonic crystal properties of cholesteric shells lead to an intricate pattern of brightly colored and circularly polarized reflections. The details depend sensitively on the arrangement and internal order of the shells, and spots can be turned on or off dynamically by modulating the area and/or wavelength of illumination. By combining the very different expertise of a soft matter physics/materials science group and an information and communication technology group specializing in security and trust issues, this strongly interdisciplinary project aims to solve a critical societal and commercial/industrial problem by using a novel and promising approach to liquid crystal technology, involving microfluidic emulsification, polymerization, advanced optics, machine-based pattern analysis, computer simulations and novel security protocol development.

B.18 UL Funding Projects

CAESAREA

Acronym:	CAESAREA
PI:	Alexei BIRYUKOV
Funding:	UL Funding
Duration:	April 15, 2015 – April 14, 2017
Members:	• Alexei BIRYUKOV (Principal Investigator) • Vesselin VELICHKOV (Researcher)
Area:	Information Security

Description

Evaluation and Analysis of Authenticated Encryption Schemes

Collaborative Compound Document Authoring and Annotation

Acronym:	CoCoDA^2
PI:	Steffen ROTHKUGEL
Funding:	UL Funding
Budget:	169,825.00 €
Duration:	Feb. 1, 2014 – Jan. 31, 2017
Members:	• Steffen ROTHKUGEL (Principal Investigator) • Jean BOTEV (Collaborator) • Johannes KLEIN (Doctoral Candidate)
Areas:	• Communicative Systems • Intelligent and Adaptive Systems • Software and Systems

Description

The CoCoDA^2 project focuses on collaboration in compound document systems based on a flexible and more fine-grained document handling than the one provided by existing file abstractions. Taking an interdisciplinary perspective, the efficient collaborative authoring as well as the intra- and inter-item annotation of compound documents particularly for geographically remote users will be investigated. This involves areas of research ranging from network science over concurrency control with operational transformation to the social sciences. The CoCoDA^2 project thus aims at contributing to the general understanding of how the structure of compound documents and collaborative aspects – such as the simultaneous multi-user authoring process itself or the concomitant sharing of semantic data – interact and integrate.

Results

In 2016, a collaborative compound document authoring environment based on the version control system Git has been developed as a reference and for further analysis of central collaboration mechanisms. Subsequently, a second protoytpe harnessing key features of the Swift programming language has been implemented, with the findings from both prototypes forming the basis for two publications. These focus on the concurrency-based command application model and user-centric collaboration approach, as well as on multimedia asset authoring in the distributed collaboration environment.

High Performance Computing @ UL

http://hpc.uni.lu/

Acronym:	UL HPC
PI:	Pascal BOUVRY, Sébastien VARRETTE
Funding:	UL Funding
Duration:	July 1, 2007 – Dec. 31, 2020
Members:	• Pascal BOUVRY (Principal Investigator) • Sébastien VARRETTE (Principal Investigator) • Valentin PLUGARU (Researcher) • Hyacinthe Cartiaux (Collaborator)

Description

The intensive growth of processing power, data storage and transmission capabilities has revolutionized many aspects of science. These resources are essential to achieve high- quality results in many application areas.

In this context, the University of Luxembourg (UL) operates since 2007 an High Performance Computing HPC facility and the related storage. The aspect of bridging computing and storage is a requirement of UL service – the reasons are both legal (certain data may not move) and performance related.

Nowadays, people from the three faculties and/or the two Interdisciplinary centers within the UL, are users of this facility. Obviously, many CSC members are relying on the platform to perform their research, as highlighted on the corresponding list of publications. More specifically, key research priorities such as Systems Bio-medicine (by LCSB) and Security, Reliability & Trust (by SnT) require access to such HPC facilities in order to function in an adequate environment.

At the end of 2016, the UL HPC facility consists of 4 clusters, featuring a total of 494 nodes (i.e. 5404 computing cores: 90 TFlops + 76 TFlops on GPU accelerators) and 4 PB of shared raw storage which are all configured, monitored and operated by 4 HPC specialists. In addition, a total of 188 servers are operated to pilot the HPC platform and the other deployed services for research such as Gforge and GitLab used by hundreds of researchers.

In these exciting times, the role of university-based HPC is more critical than ever in providing the foundation for a healthy HPC "ecosystem" for Luxembourg, where computational scientists and HPC-service providers work together in a highly collaborative community. Through their locality to today's research base, and the students who will become our next generation of computational scientists, universities such as the UL are uniquely positioned to deliver excellent return on investment in HPC as a platform for future economic growth.

Reconciling the Uneasy Relationship between the Economics of Personal Data and Privacy

Acronym:	REQUISITE
PI:	Peter Y. A. RYAN
Funding:	UL Funding
Duration:	June 1, 2015 – May 31, 2018
Members:	• Peter Y. A. RYAN (Principal Investigator) • Qiang TANG (Researcher)
Areas:	• Information Security • Intelligent and Adaptive Systems

Description

Personal data is nowadays a common commodity in the web space, yet our understanding of cost–benefit trade-offs that individuals undertake when getting involved in digital transactions and disclosing personal data is far from complete. On the one hand, users benefit from personalisation of products and contributing to the societal good, but, on the other hand, might be locked into services and suffer from severe privacy risks, e.g. that data may be compromised once disclosed to a service provider. We focus on healthcare-related personal data and mainly consider two scenarios. One is *public medical research*, where personal data will be used by third-party organizations (e.g. by various medical labs) to conduct research, such as studying the trend of a disease. The other is *medical recommender systems*, where patients interact with each other and third-party professionals (e.g. doctors, and people from pharmaceutical and insurance companies) for a variety of purposes. These two scenarios only represent a small segment of the whole ecosystem, but they vividly illustrate the dilemma of utility and privacy of sensitive personal data.

In this project, we carry out interdisciplinary research to bridge the theory-practice gap in tackling the privacy issues associated with personal data. We (economists and information security researchers) will investigate the economic incentives behind users' participation in the systems, and subsequently establish models for gains and costs in the two application scenarios. Then, we will apply the concept of *mechanism design* to our scenarios, and propose mechanisms for safeguarding users' utility and privacy against rational attackers (e.g. legitimate participants in the systems). Finally, to complement the developed mechanisms, we will propose new cryptographic protocols to safeguard privacy against potential malicious and irrational attackers (e.g. outside attackers). The task of this project is essentially twofold: economic understanding and modelling, and realization of (rational) cryptographic protocols.

B.19 Undefined Funding Projects

Bridging the Gap between Formal and Informal Mathematical Reasoning

Acronym:	BriGFIM
PI:	Marcos CRAMER
Funding:	Undefined Funding
Duration:	Nov. 1, 2016 – Oct. 31, 2018
Member:	Marcos CRAMER (Principal Investigator)
Areas:	• Computational Sciences • Mathematics

Description

Mathematics has the reputation of being the most certain of all sciences, because its propositions are established through mathematical proofs. However, there are two very different notions of mathematical proof: On the one hand, there is the very precise notion of a formal proof, written in a formal language and complying with rigorously defined inference rules. On the other hand, there are the informal proofs actually produced by mathematicians, written in natural language and invoking mathematical intuitions. On many occasions in the history of mathematics, previously accepted informal proofs had to be rejected based on new findings.

This project will bridge the gap between these two notions of mathematical proof by developing a formal model of informal mathematical reasoning, which will model the actual modes of inference employed by mathematicians more faithfully than formal proofs do. This will be accomplished by combining methods from mathematical and informal logic, philosophy of mathematics, formal linguistics and argumentation theory.

The model will improve our understanding of mathematical reasoning, historical mathematical progress and progress in the individual mathematician. It will contribute to the goal of teaching machines to do mathematics like humans.

B.20 Unfunded Projects

Active Learning on Streaming Time Series for Cyber-Physical Security Appliances

PI:	Radu STATE

Funding: Unfunded

Budget: 600,000.00 €

Duration: Jan. 1, 2015 – Jan. 1, 2018

Members:
- Radu STATE (Principal Investigator)
- Stefanie OESTLUND (Project Coordinator)
- Eric FALK (Doctoral Candidate)

Area: Communicative Systems

Partner: neXus

Anomaly Detection and Machine Learning with Big Data Systems

PI: Radu STATE

Funding: Unfunded

Budget: 600,000.00 €

Duration: Oct. 1, 2015 – Oct. 1, 2017

Members:
- Radu STATE (Principal Investigator)
- Lautaro DOLBERG (Researcher)
- Stefanie OESTLUND (Project Coordinator)

Area: Communicative Systems

Partner: Choice

Collaborative Context-Aware Mobile Training and Exploration

Acronym: CollaTrEx

PI: Jean BOTEV

Funding: Unfunded

Duration: Feb. 2, 2015 – Feb. 2, 2018

Members:
- Jean BOTEV (Principal Investigator)
- Steffen ROTHKUGEL (Collaborator)

Areas:
- Communicative Systems
- Educational Sciences

Description

The CollaTrEx project aims at providing an integrated framework for collaborative context-aware mobile exploration and training with a focus on the in-situ collaboration within groups of learners engaging in varied educational activities. The advantages and opportunities of context-aware mobile learning are widely recognized but modern mobile devices offer an enormous potential beyond establishing precise spatio-temporal context. The multitude of sensors, as well as advanced recording and networking capabilities, call for increased interactivity and collaboration. However, instead of harnessing these capabilities to full effect for a genuinely collaborative and interactive mobile learning experience, they are often left unexploited.

Results

The main outcome in 2016 is the completion of the initial prototype system and basic CollaTrEx framework for collaborative context-aware mobile training and exploration. It was presented at both ICEduTech and DLI conferences, winning the best paper award of the latter. CollaTrEx at this stage comprises an easily extendable web-based back end for the management and creation of the various activities, as well as a simple-to-use iOS-based client application for tablets. To determine the available activities and provide a tailored experience to users, absolute and relative spatio-temporal context is employed. Several buffering levels are offered for seamlessness and an increased flexibility with regard to connection losses, which is particularly relevant to the operation in remote areas. Further, experimental activity types have also been evaluated and added to the existing front-end implementation.

Doctoral Thesis: Adaptive Literacy-Aware Integration of Learning Material (working title)

PI:	Steffen ROTHKUGEL
Funding:	Unfunded
Duration:	Jan. 15, 2016 – Jan. 15, 2019
Members:	• Steffen ROTHKUGEL (Principal Investigator) • Christian GREVISSE (Doctoral Candidate)

Description

The growing amount of available learning material nowadays requires a significant filtering effort by students for problem solving tasks. In addition, the choice of the appropriate type of learning material differs depending on the individual learner's preferences. In this work, we suggest to move from a material-centered to a student- and task-centered approach by integrating and suggesting

learning material based on the user's literacy and the context of the task to be completed. Data from social networking platforms may both enrich the available learning material and give insights on the user's preferences, to adequately match material and learner in the given context. Finally, computer-based assessment may give insights on the learner's progress and the proposed study material.

Doctoral Thesis: Integrating Compositional and Annotative Approaches for Feature Implementation (working title)

PI:	Steffen ROTHKUGEL
Funding:	Unfunded
Duration:	Jan. 1, 2013 – Dec. 31, 2017
Member:	Steffen ROTHKUGEL (Principal Investigator)
Partner:	Benjamin Behringer (Hochschule für Technik und Wirtschaft des Saarlandes)

Description

Compositional and annotative approaches are two competing yet complementary candidates for implementing feature-oriented software product lines. While the former provides real modularity, the latter excels concerning expressiveness. To combine the respective advantages of compositional and annotative approaches, we aim at unifying their underlying representations by leveraging the snippet system instead of directories and files. In addition, to exploit this unification, we propose different editable views.

This is a collaboration between the University of Luxembourg and the Hochschule für Technik und Wirtschaft des Saarlandes (HTW) with Benjamin Behringer as external PhD student on the project.

Doctoral Thesis: Towards an Integration of Collaborative and Crowd Computing (working title)

PI:	Steffen ROTHKUGEL
Funding:	Unfunded
Duration:	Jan. 1, 2015 – Dec. 31, 2019
Members:	• Steffen ROTHKUGEL (Principal Investigator) • Christian MULLER (Doctoral Candidate)

Description

The need to collaborate is omnipresent, both in the physical world as well as in terms of online software. Domains such as learning and work are still treated mostly separately, although their tight integration is effectively required. While each individual person is the main target of that integration, it is beneficial to harness the power of communities of people to perform tasks which are hard to impossible to do by a single person. The main objective of this dissertation is to elaborate on concepts, strategies, and techniques to incorporate both learning as well as work in collaborative software systems in a seamless fashion, and to integrate them with crowd computing.

Self-learning predictive algorithms: from design to scalable implementation

PI:	Radu STATE
Funding:	Unfunded
Budget:	150,000.00 €
Duration:	Nov. 1, 2015 – Nov. 1, 2018
Members:	• Radu STATE (Principal Investigator) • Stefanie OESTLUND (Project Coordinator) • Manxing DU (Doctoral Candidate)
Area:	Communicative Systems
Partner:	Olamobile

Description

The PhD project focuses on designing prediction algorithms for real-time bidding system. With the support from OLAmobile, our industrial partnering company, we will investigate how to accurately predict user's purchase intention and adjust bidding strategies adaptively in real time for the mobile advertising market, in which less research has been done. We will not only tackle with online analysis of the developed algorithms but also conduct field trails in online mode for evaluation and optimization on the real-time bidding (RTB) platform provided by OLAmobile. The developed algorithms can be further applied to other large-scale real-time applications.

Software Defined Network Service Chaining through Network Analytics

PI:	Radu STATE

Funding:	Unfunded
Budget:	90,000.00 €
Duration:	Oct. 1, 2015 – Oct. 1, 2018
Members:	• Radu STATE (Principal Investigator) • Stefanie OESTLUND (Project Coordinator) • Beltran Fiz Pontiveros (Doctoral Candidate)
Area:	Communicative Systems
Partner:	Telindus

Tool for Specification, Management and Assessment of Teaching Programs

Acronym:	TESMA
PI:	Nicolas GUELFI
Funding:	Unfunded
Duration:	Feb. 15, 2016 – Dec. 31, 2020
Members:	• Nicolas GUELFI (Principal Investigator) • Benoit RIES (Project Coordinator) • Benjamin JAHIC (Collaborator) • Sandro REIS (Collaborator)
Areas:	• Educational Sciences • Software and Systems

Description

Defining and managing teaching programs at university or other institutions is a complex task for which there is not much support in terms of methods and tools. This task becomes even more critical when the time comes to obtain certifications w.r.t. official standards. The objective of the TESMA project is to provide a method and an open-source tool dedicated to the specification and management (including certification) of teaching programs. This tool is to be engineered using a development method called Messir for its requirements elicitations and introduces a domain-specific language dedicated to the teaching domain.

Appendix C

Representational Activities

C.1 Conference Committee Memberships

10th IEEE ICOSST-2016 International Conference on Open Source Systems & Technologies

http://icosst.kics.edu.pk/2016/

Location: Lahore, Pakistan, Dec. 15, 2016 – Dec. 17, 2016.

Participating Members:

- Nicolas GUELFI (PC Member)

10th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO 2016)

Location: Augsburg, Germany, Sept. 12, 2016 – Sept. 16, 2016.

Participating Members:

- Jean BOTEV (Track / Working Group Chair)

10th International Conference on Network and System Security (NSS 2016)

http://nsclab.org/nss2016/

Location: Taipei, Taiwan, Sept. 28, 2016 – Sept. 30, 2016.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

10th International Symposium on Empirical Software Engineering and Measurement (ESEM 2016)

http://alarcos.esi.uclm.es/eseiw2016/esem

Location: Ciudad Real, Spain, Sept. 8, 2016 – Sept. 9, 2016.

Participating Members:

- Mehrdad SABETZADEH (Program Committee Member)

10th International Symposium on Theoretical Aspects of Software Engineering (TASE'16)

Location: Shanghai, China, July 17, 2016 – July 19, 2016.

Participating Members:

- Jun PANG (Program Committee Member)

10th International workshop on Normative Multiagent Systems (NORMAS 2016)

http://icr.uni.lu/normas/normas2016/normas2016.html

Location: The Hague, Netherlands, Aug. 29, 2016 – Aug. 30, 2016.

Description: Norms are crucial for studying both human social behaviour and for developing distributed software applications. The term *norms* is deliberately ambiguous. We study and apply norms in the sense of being normal (conventions, practice), and in the sense of rules and regulations (obligations, permisions).

Normative systems are complex systems in which norms play a crucial role or which need normative concepts in order to describe or specify their behaviour. A normative multi-agent system combines models for normative systems (dealing for example with conventions, or obligations) with models for multi-agent systems (dealing with coordination between individual agents).

Norms have been proposed in multi-agent systems and computer science to deal with issues of coordination, security, electronic commerce, electronic in-

stitutions and agent organization. They have been fruitfully applied to develop simulation models for the social sciences. However, due to the lack of a unified theory, many researchers are presently developing their own ad hoc concepts and applications.

The aim of this workshop is to stimulate interdisciplinary research on normative concepts and their application.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

10th WISTP International Conference on Information Security Theory and Practice (WISTP'16),

Location: Heraklion, Greece, Sept. 27, 2016 – Sept. 26, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)

11th International Conference on Parallel Processing and Applied Mathematics (PPAM)

http://ppam.pl/

Location: Krakow, Poland, Sept. 6, 2016 – Sept. 9, 2016.

Participating Members:

- Pascal BOUVRY (Program Committee Member)

11th International Workshop on Security and High Performance Computing Systems (SHPCS 2016)

http://hpcs2016.cisedu.info/2-conference/workshops---hpcs2016/workshop09-shpcs

Location: Innsbruck, Austria, July 18, 2016 – July 22, 2016.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

12th IEEE International Workshop on Factory Communication Systems (WFCS'2016)

Location: Aveiro, Portugal, May 3, 2016 – May 6, 2016.

Participating Members:

- Nicolas NAVET (Program Committee Member)

12th International Conference on Information Security Practice and Experience (ISPEC'16)

Location: Zhangjiajie, China, Nov. 16, 2016 – Nov. 18, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)

12th International Conference on Wireless Communications, Networking and Mobile Computing (WICOM)

http://www.wincom-conf.org/

Location: Fez, Morocco, Oct. 26, 2016 – Oct. 29, 2016.

Description: The conference will provide a forum for exchanging ideas, discussing solutions, and sharing experiences among researchers and professionals from both academia and industry interested in wireless networks and mobile communications. WINCOM has been organized for the last four years, and that is in the form of two workshops.

Participating Members:

- Latif LADID (Keynote speaker)

12th InternationalWorkshop on Security and Trust Management (STM'16)

Location: Heraklion, Greece, Sept. 26, 2016 – Sept. 27, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)
- Rolando TRUJILLO RASUA (Program Committee Member)

13ème Conférence en Recherche d'information et applications

Location: Toulouse, France, March 8, 2016 – March 11, 2016.

Participating Members:

- Christoph SCHOMMER (PC Member)

13th IEEE International Conference on Advanced and Trusted Computing (ATC'16)

Location: Toulouse, France, July 18, 2016.

Participating Members:

- Rolando TRUJILLO RASUA (Program Committee Member)
- Gabriele LENZINI (PC Member)

13th International Conference on Deontic Logic and Normative Systems (DEON 2016)

http://www.deon2016.org

Location: Bayreuth, Germany, July 18, 2016 – July 21, 2016.

Description: The biennial DEON conferences are designed to promote interdisciplinary cooperation amongst scholars interested in linking the formal-logical study of normative concepts and normative systems with computer science, artificial intelligence, philosophy, organization theory and law.

In addition to these general themes, DEON 2016 will encourage a special focus on the topic "Reasons, Argumentation and Justification".

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

13th International Symposium on Neural Networks (ISNN 2016)

https://conference.cs.cityu.edu.hk/isnn/ISNN2016/index.html

Location: Saint Petersburg, Russia, July 6, 2016 – July 8, 2016.

Participating Members:

- Pascal BOUVRY (Program Committee Member)

13th Working IEEE/IFIP Conference on Software Architecture (WICSA 2016)

http://www.softwarearchitecture.org/

Location: Venice, Italy, April 5, 2016 – April 8, 2016.

Participating Members:

- Domenico BIANCULLI (Program Committee Member)

14th German Conference on Multiagent System Technologies (MATES 2016)

http://www.dfki.de/mates2016/index.html

Location: Klagenfurt, Austria, Sept. 27, 2016 – Sept. 30, 2016.

Description: The MATES conference aims at the promotion of and the cross-fertilization between theory and application of intelligent agents and multiagent systems. It provides an interdisciplinary forum for researchers and members of business and industry to present and discuss latest advances in agent-based computing with prototyped or fielded systems in various application domains. MATES 2016 will offer a competitive set of special topical sessions, invited keynotes by distinguished experts, and issues a Best Paper Award. The MATES conference series is ERA/CORE top-ranked in the field of agent technologies, and its proceedings are published by Springer in its Lecture Notes in Artificial Intelligence (LNAI) series

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

14th International Conference on Applied Cryptography and Network Security (ACNS 2016)

http://acns2016.sccs.surrey.ac.uk/

Location: London, United Kingdom, June 19, 2016 – June 22, 2016.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

15th European Conference on Computational Biology (ECCB'16)

Location: Hague, Netherlands, Sept. 3, 2016 – Sept. 7, 2016.

Participating Members:

- Andrzej MIZERA (Program Committee Member)

15th International Conference on Autonomous Agents and Multiagent Systems (AAMAS2016)

https://sis.smu.edu.sg/aamas2016

Location: Singapore, Singapore, May 9, 2016 – May 13, 2016.

Description: AAMAS is the largest and most influential conference in the area of agents and multiagent systems. The aim of the conference is to bring together researchers and practitioners in all areas of agent technology and to provide a single, high-profile, internationally renowned forum for research in the theory and practice of autonomous agents and multiagent systems.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

15th International Conference on Cryptology and Network Security (CANS 2016)

http://cans2016.di.unimi.it/

Location: Milan, Italy, Nov. 14, 2016 – Nov. 16, 2016.

Participating Members:

- Vincenzo IOVINO (PC Member)
- Qiang TANG (PC Member)

16th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID 2016)

Location: Cartagena, Colombia, May 16, 2016 – May 19, 2016.

Participating Members:

- Grégoire DANOY (Program Committee Member)
- Pascal BOUVRY (Doctoral Symposium Chair)

16th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP 2016)

https://www.arcos.inf.uc3m.es/wp/ica3pp2016/

Location: Granada, Spain, Oct. 14, 2016 – Oct. 16, 2016.

Description: ICA3PP 2016 is the 16th in this series of conferences started in 1995 that are devoted to algorithms and architectures for parallel processing. ICA3PP is now recognized as the main regular event of the world that is covering the many dimensions of parallel algorithms and architectures, encompassing fundamental theoretical approaches, practical experimental projects, and commercial components and systems. As applications of computing systems have permeated in every aspects of daily life, the power of computing system has become increasingly critical. This conference provides a forum for academics and practitioners from countries around the world to exchange ideas for improving the efficiency, performance, reliability, security and interoperability of computing systems and applications.

Participating Members:

- Pascal BOUVRY (Track / Working Group Chair)
- Grégoire DANOY (Program Committee Member)

16th International Conference on Web Engineering (ICWE2016)

http://icwe2016.inf.usi.ch/

Location: Lugano, Switzerland, June 6, 2016 – June 9, 2016.

Participating Members:

- Domenico BIANCULLI (Publicity Chair)
- Domenico BIANCULLI (Program Committee Member)

18th International Conference on Formal Engineering Methods (ICFEM'16)

Location: Tokyo, Japan, Nov. 18, 2016 – Nov. 14, 2016.

Participating Members:

- Jun PANG (Program Committee Member)

18th International Conference on Information and Communications Security (ICICS2016)

http://www.icics2016.org/

Location: Singapore, Singapore, Nov. 29, 2016 – Dec. 2, 2016.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

18th International Conference on Information and Communications Security (ICISC'16)

Location: Singapore, Singapore, Nov. 29, 2016 – Dec. 2, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)

18th Mediterranean Electrotechnical Conference (MELECON'16)

Location: Limassol, Cyprus, April 18, 2016 – April 20, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)

19th Information Security Conference 2016 (ISC 2016)

http://manoa.hawaii.edu/isc2016/

Location: Honolulu, United States of America, Sept. 7, 2016 – Sept. 9, 2016.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

19th International Conference on Fundamental Approaches to Software Engineering (FASE 2016)

http://www.etaps.org/index.php/2016/fase

Location: Eindhoven, Netherlands, April 2, 2016 – April 8, 2016.

1st European Workshop on Usable Security (EuroUSEC) 2016

https://eurousec.secuso.org/2016/

Location: Darmstadt, Germany, July 18, 2016.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

1st IEEE European Symposium on Security and Privacy (EuroS&P 2016)

http://www.ieee-security.org/TC/EuroSP2016/

Location: Saarbrücken, Germany, March 21, 2016 – March 24, 2016.

Participating Members:

- Lionel BRIAND (Program Committee Member)

1st Workshop on Advances in Secure Electronic Voting (VOTING 2016)

http://fc16.ifca.ai/voting/cfp.html

Location: Barbados, Barbados, Feb. 16, 2016.

Participating Members:

- Peter Y. A. RYAN (Co-Chair)

2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)

http://www.ieee.org/conferences_events/conferences/conferencedetails/index.html?Conf_ID=36453

Location: Muscat, Oman, March 15, 2016 – March 16, 2016.

Description: The scope of the conference on Big Data and Smart City is to bring together researchers, designers, developers and practitioners interested in the advances and applications in the field of smart cities, green information and communication technologies, sustainability, energy aware systems and technologies to realize smart communities of the future.

Participating Members:

- Latif LADID (Keynote speaker)

2016 IEEE International Smart Cities Conference (ISC2)

http://smartcities.ieee.org/conferences-events.html

Location: Trento, Italy, Sept. 12, 2016 – Sept. 15, 2016.

Description: The Conference deals with heterogeneous subjects in different areas related to smart cities, with a special emphasis on the quality of life of citizens. Possible broad topics include (but are not limited to) the topics listed in the keywords. The Conference target audience comprises Citizens, Policy makers, Administrators, Infrastructure operators, Engineering professionals (both from Academia and from industry), Economists, Sociologists, and University students.

Participating Members:

- Latif LADID (Chair)

2016 IEEE International Symposium on Innovations in Intelligent Systems and Applications (INISTA 2016)

Location: Sinaia, Romania, Aug. 2, 2016 – Aug. 5, 2016.

Participating Members:

- Ravi JHAWAR (Program Committee Member)

2016 IEEE-SA Ethernet & IP @ Automotive Technology Day

Location: Paris, France, Sept. 20, 2016 – Sept. 21, 2016.

Description: The IEEE-SA Ethernet & IP @ Automotive Technology Day (E&IP@ATD) is the premier venue for OEMs, suppliers, semiconductor vendors and tool providers to discuss and learn about the evolution of Ethernet standards, technologies and applications in the automotive environment.

The IEEE-SA Ethernet & IP @ Automotive Technology Day is open to anyone interested in next generation automotive communication technologies, as well

as those currently involved in related standardization and interoperability activities.

Participating Members:

- Nicolas NAVET (Program Committee Member)

21st European Symposium on Research in Computer Security (ESORICS 2016)

http://www.ics.forth.gr/esorics2016/

Location: Heraklion, Crete, Greece, Sept. 26, 2016 – Sept. 30, 2016.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

23rd ACM Conference on Computer and Communications Security (ACM CCS 2016)

https://www.sigsac.org/ccs/CCS2016/

Location: Vienna, Austria, Oct. 24, 2016 – Oct. 28, 2016.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)
- Dmitry KHOVRATOVICH (Program Committee Member)

23rd Conference on Selected Areas in Cryptography (SAC 2016)

http://www.engr.mun.ca/~sac2016/

Location: St. John's, Canada, Aug. 10, 2016 – Aug. 12, 2016.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

23rd IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER 2016)

http://saner.inf.usi.ch/

Location: Osaka, Japan, March 14, 2016 – March 18, 2016.

Participating Members:

- Domenico BIANCULLI (Program Committee Member)

23rd International SPIN symposium on Model Checking of Software (SPIN'16)

Location: Eindhoven, Netherlands, April 7, 2016 – April 8, 2016.

Participating Members:

- Jun PANG (Program Committee Member)

24th IEEE International Conference on Program Comprehension (ICPC 2016)

http://www.program-comprehension.org/icpc16/

Location: Austin, Texas, United States of America, May 16, 2016 – May 17, 2016.

Participating Members:

- Lucia LUCIA (Program Committee Member)

24th IEEE International Requirements Engineering Conference (RE 2016)

http://re16.org/

Location: Beijing, China, Sept. 12, 2016 – Sept. 16, 2016.

Participating Members:

- Shiva NEJATI (Program Committee Member)
- Mehrdad SABETZADEH (Program Committee Member)

27th IEEE International Symposium on Rapid System Prototyping (RSP'2016)

Location: Pittsburgh, United States of America, Oct. 6, 2016 – Oct. 7, 2016.

Participating Members:

- Nicolas NAVET (Program Committee Member)

27th International Conference on Concurrency Theory (CONCUR'16)

Location: Quebec, Canada, Aug. 24, 2016 – Aug. 27, 2016.

Participating Members:

- Jun PANG (Program Committee Member)

29th IEEE International Symposium on Computer-Based Medical Systems (CBMS)

Location: Dublin, Ireland, June 20, 2016 – June 24, 2016.

Participating Members:

- Christoph SCHOMMER (PC Member)

2nd 6TiSCH (IPv6 over the Timeslotted Channel Hopping mode of IEEE 802.15.4e) Plugtests

http://www.etsi.org/news-events/events/1022-6tisch-2-plugtests

Location: Paris, France, Feb. 2, 2016 – Feb. 4, 2016.

Description: This Plugtests^{TM} event focused on assessing the interoperability of 6TiSCH implementations based on the draft-ietf-6tisch-minimal specification as well as the 6TiSCH Operation Sublayer (6top) Protocol.

The 2nd 6TiSCH Plugtests^{TM} event conducted testing campaign based on the test cases developed by ETSI and the IETF 6TiSCH WG and focused on the conformance and interoperability of the IEEE 802.15.4e technologies.

It was a unique opportunity for 6TiSCH vendors to test their product against different implementations.

Participating Members:

- Maria Rita PALATTELLA (Organizing Chair)

2nd Annual IoT Global Innovation Forum

http://iotevents.org/iot-global-innovation-forum-2016/

Location: Barcelona, Spain, June 15, 2016.

Description: The 2nd Annual IoT Global Innovation Forum, June 15-16, 2016 in Barcelona, Spain, will bring together leading technology innovators, business strategists and senior executives from around the world for two days of focused networking and information sharing at the IoT cutting edge. Expert speakers will discuss the latest applications for traditional commercial processes as well as new business models and opportunities within the emerging Internet of Things ecosphere.

Participating Members:

- Latif LADID (Keynote speaker)

2nd EAI International Conference on Interoperability in IoT (InterIoT) 2016

http://interoperabilityiot.org/2016/show/home

Location: Paris, France, Oct. 26, 2016 – Oct. 27, 2016.

Description: IoT is an emerging concept that involves a larger and larger number of heterogeneous smart everyday-life objects. They enable a large scope of new applications that require all these objects to communicate, to interact, to share data and processes. All these objects have popped up from there to there, using their own communication means, OS or language. A key open issue to realize the full capacity of such concept is thus interoperability. How to make them fully compliant? This conference presents some current research and open issues in interoperability in IoT, ranging from virtualization to standardization.

Participating Members:

- Maria Rita PALATTELLA (Technical Program Committee Member)

2nd International Conference on Applications in Information Technology (ICAIT-2016)

http://kspt.icc.spbstu.ru/conf/icait-2016/

Location: Aizu-Wakamatsu, Japan, Oct. 6, 2016 – Oct. 8, 2016.

Description: The main objective of the 2nd Conference on Applications in Information Technology is to foster rich creativity in students' research works and to encourage students and young scientists to participate actively in open discussions with their colleagues. This conference is a place for the scientific presentations of young researchers representing not only the universities organizing this event but also many partner universities from all over the world. This conference accumulates good traditions established in the past conferences including The Conference on Humans and Computers in 1998-2010, its successor, The 2012 Joint International Conference on Human-Centered Computer Environments and The 2015 International Workshop on Applications in Information Technology.

Participating Members:

- Alfredo CAPOZUCCA (PC Member)
- Nicolas GUELFI (PC Member)
- Benoit RIES (PC Member)

2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)

http://www.icissp.org/?y=2016

Location: Rome, Italy, Feb. 19, 2016 – Feb. 21, 2016.

Participating Members:

- Gabriele LENZINI (Program Committee Member)

2nd Symposium on Dependable Software Engineering (SETTA'16)

Location: Beijing, China, Nov. 9, 2016 – Nov. 11, 2016.

Participating Members:

- Jun PANG (Program Committee Member)

2nd Workshop on Information Security, Assurance, and Reliability in the Cloud (WISARC 2016)

http://www.di.ubi.pt/~inacio/wisarc/

Location: Shanghai, China, Dec. 6, 2016 – Dec. 9, 2016.

Description: Cloud computing is a major research area. Much of the discussion is due to the security issues it poses as a new technology and to the IT paradigm shift, as well as the fact that increasing cybersecurity concerns have a direct impact on the cloud. Issues span from fundamental confidentiality assurance of data in rest and motion, due to data outsourcing, to regulation and jurisdiction problems of legal data ownership and takeover. The virtualization technology that supports the building blocks for multi-tenant infrastructures also poses novel security risks and vulnerabilities that need to be properly addressed. Ironically, the interplay of these new technologies paves the way for the development of novel defenses against the very threats that arise in the current attack landscape. For example, virtual machine escape vulnerabilities are specific to virtualization technology, the same one that simplifies dynamic malware analysis.

Cloud computing research is a multidisciplinary effort involving cryptography, networking, software development, system architecture, among others. This workshop aims to attract innovative research works and foster discussions addressing technical, policy and legal issues of information security, assurance and reliability in cloud computing environments, elaborating on distinguished and emerging topics that are of interest to both the academia and the industry.

Participating Members:

- Vesselin VELICHKOV (Program Committee Member)

2nd Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems (CyberICPS'16)

Location: Heraklion, Greece, Sept. 26, 2016 – Sept. 30, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)

2th IEEE International Workshop on Factory Communication Systems (WFCS'2016)

Location: Aveiro, Portugal, May 3, 2016 – May 6, 2016.

Participating Members:

- Nicolas NAVET (Program Committee Member)

30th annual conference of the Belgian Operational Research Society

http://www.orbel.be/orbel30/

Location: Louvain-La-Neuve, Belgium, Jan. 28, 2016 – Feb. 29, 2016.

Description: ORBEL is the national conference of the SOGESCI-BVWB, the Belgian Operational Research (OR) Society, Member of EURO, the association of European OR Societies, and Belgian representative of IFORS (International Federation of OR Societies).

The conference is intended as a meeting place for researchers, users and potential users of Operational Research, Statistics, Computer Science and related fields. It will provide managers, practitioners and researchers with a unique opportunity to exchange information on quantitative techniques for decision making.

This year's meeting (ORBEL30) will take place in the city of Louvain-la-Neuve at UCL.

Participating Members:

- Raymond Joseph BISDORFF (Program Committee Member)

30th Annual IFIPWG 11.3 Conference on Data and Applications Security and Privacy (DBSec'16)

Location: Trento, Italy, July 18, 2016 – July 20, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)

30th IEEE International Conference on Advanced Information Networking and Applications (AINA) 2016

http://voyager.ce.fit.ac.jp/conf/aina/2016/

Location: Crans-Montana, Switzerland, March 23, 2016 – March 25, 2016.

Description: The conference covers theory, design and application of computer networks and distributed computing and information systems. Aside from the regular presentations, the conference will include keynote addresses with speakers from both industry and academia.

Participating Members:

- Maria Rita PALATTELLA (Technical Program Committee Member)

30th International Conference on Information Networking (ICOIN) 2016

http://2016.icoin.org/main/

Location: Kota Kinabalu, Malaysia, Jan. 13, 2016 – Jan. 15, 2016.

Participating Members:

- Pascal BOUVRY (Program Committee Member)

31st IEEE/ACM International Conference on Automated Software Engineering (ASE 2016)

http://www.ase2016.org/

Location: Singapore, Singapore, Sept. 3, 2016 – Sept. 7, 2016.

Participating Members:

- Lucia LUCIA (Publicity Chair)
- Shiva NEJATI (Program Committee Member)

31st International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2016)

http://ifipsec.org/2016/

Location: Ghent, Belgium, May 30, 2016 – June 1, 2016.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

35th International Conference on Conceptual Modeling (ER 2016)

http://er2016.cs.titech.ac.jp/

Location: Gifu, Japan, Nov. 14, 2016 – Nov. 17, 2016.

Participating Members:

- Mehrdad SABETZADEH (Program Committee Member)

36th International Cryptology Conference (CRYPTO 2016)

https://www.iacr.org/conferences/crypto2016/

Location: Santa Barbara, United States of America, Aug. 14, 2016 – Aug. 18, 2016.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

38th CogSci - Annual Meeting of the Cognitive Science Society.

Location: Philadelphia, United States of America, Aug. 10, 2016 – Aug. 13, 2016.

Participating Members:

- Christoph SCHOMMER (PC Member)

38th International Conference on Software Engineering (ICSE 2016)

http://2016.icse.cs.txstate.edu/

Location: Austin, TX, United States of America, May 14, 2016 – May 22, 2016.

Participating Members:

- Lionel BRIAND (Steering Committee Member)
- Lionel BRIAND (Program Committee Member)
- Shiva NEJATI (Program Committee Member)

3rd International Workshop on CrowdSourcing in Software Engineering (CSI-SE 2016)

https://sites.google.com/site/2016csise/

Location: Austin, Texas, United States of America, May 16, 2016.

3rd International Workshop on Requirements Engineering and Testing (RET 2016)

http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=49036&copyownerid=73024

Location: Gothenburg, Sweden, March 14, 2016.

Participating Members:

- Duy Cu NGUYEN (Program Committee Member)

3rd International Workshop on Self-Improving System Integration (SISSY 2016)

Location: Würzburg, Germany, July 19, 2016 – July 22, 2016.

Participating Members:

- Jean BOTEV (Program Committee Member)

3rd Workshop on Bitcoin and Blockchain Research 2016 (BITCOIN 2016)

http://fc16.ifca.ai/bitcoin/cfp.html

Location: Barbados, Barbados, Feb. 26, 2016.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

40th IEEE Computer Society International Conference on Computers, Software & Applications (COMPSAC'16)

Location: Atlanta, United States of America, June 10, 2016 – June 14, 2016.

Participating Members:

- Jun PANG (Program Committee Member)

4th International Conference on Future Internet of Things and Cloud (2016)

Location: Vienna, Austria, Aug. 22, 2016 – Aug. 24, 2016.

Participating Members:

- Sylvain KUBLER (Track / Working Group Chair)

4th International Conference on Human Aspects of Information Security, Privacy and Trust

http://2016.hci.international/has

Location: Toronto, Canada, July 17, 2016 – July 22, 2016.

Participating Members:

- Gabriele LENZINI (Program Committee Member)

4th International Workshop on Security in Cloud Computing (SCC 2016)

https://conference.cs.cityu.edu.hk/asiaccsscc/16/

Location: Xi'an, China, May 30, 2016.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

4th International Workshop on Self-Adaptive and Self-Organising Socio-Technical Systems (SASO^ST 2016)

Location: Augsburg, Germany, Sept. 16, 2016.

Participating Members:

- Steffen ROTHKUGEL (Program Committee Member)
- Jean BOTEV (Workshop Organiser / Co-Organiser)

4th International Workshop on Self-Optimisation in Organic and Autonomic Computing Systems (SAOS 2016)

Location: Nuremberg, Germany, April 4, 2016.

Participating Members:

- Jean BOTEV (Program Committee Member)

4th Workshop on Hot Issues in Security Principles and Trust (HotSpot 2016)

https://members.loria.fr/VCortier/files/HotSpot2016/

Location: Eindhoven, Netherlands, April 3, 2016.

Participating Members:

- Peter Y. A. RYAN (Program Committee Member)

5G Forum USA

https://tmt.knect365.com/5g-north-america/

Location: Palo Alto, United States of America, April 12, 2016 – April 13, 2016.

Description: The annual 5G Forum USA brings together decision makers from key carriers, solution providers, associations & enterprises discussing use cases and exploring technical challenges to enable you to capitalise on opportunities offered by 5G.

Participating Members:

- Latif LADID (Chair)

5th International Workshop on Hybrid Systems Biology (HSB'16)

Location: Grenoble, France, Oct. 20, 2016 – Oct. 21, 2016.

Participating Members:

- Andrzej MIZERA (Program Committee Member)

6th International Conference on the Internet of Things (IoT 2016)

http://www.iot-conference.org/iot2016/

Location: Stuttgart, Germany, Nov. 7, 2016 – Nov. 9, 2016.

Description: The 6th International Conference on the Internet of Things (IoT 2016), building on the success of its predecessors since 2008, is the premier forum for such efforts, to share, discuss and witness cutting edge research in all areas of development for the Internet of Things.

Participating Members:

- Latif LADID (Keynote speaker)

6th International Workshop on Socio-Technical Aspects in Security and Trust (STAST 2016)

http://stast.uni.lu/

Location: Los Angeles, California, United States of America, Dec. 5, 2016.

Participating Members:

- Gabriele LENZINI (Chair)
- Peter Y. A. RYAN (Program Committee Member)

6TiSCH/6lo Plugtests

http://www.etsi.org/news-events/events/1077-6tisch-6lo-plugtests

Location: Berlin, Germany, July 15, 2016 – July 17, 2016.

Description: This joint Plugtests^{TM} event focused on assessing the interoperability of 6TiSCH and 6lo implementations.

6TiSCH

The focus of the 6TiSCH tests will be on:
- draft-ietf-6tisch-minimal
- draft-ietf-6tisch-6top-protocol
- secure joining
- backbone router operation.

6lo

The focus of the 6lo tests will be on specifications RFC4944, RFC6282 and RFC6775 adapted to:
- Constrained wired networks* (draft-ietf-6lo-6lobac-04)
- DECT Ultra Low Energy air interface* (draft-ietf-6lo-dect-ule-04)
- Bluetooth low energy air interface* (RFC 7668)
- Near Field Communication* (NFC) radio interface* (draft-ietf-6lo-nfc-03)
- IEEE 802.15.4 Networks (RFC 4944), both 2.4 GHz and 900 MHz*

(* if number of implementations permits)

Participating Members:

- Maria Rita PALATTELLA (Organizing Chair)

7th IEEE International Symposium on High Assurance Systems Engineering (HASE 2016)

http://hase2016.org/

Location: Orlando, Florida, United States of America, Jan. 7, 2016 – Jan. 9, 2016.

Participating Members:

- Lionel BRIAND (Program Committee Member)

7th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2016)

Location: Gratz, Austria, April 14, 2016 – April 15, 2016.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

8th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2016)

http://2016.cloudcom.org

Location: Luxembourg, Luxembourg, Dec. 12, 2016 – Dec. 15, 2016.

Description: The 8th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2016) will be held from December 12th to December 15th, 2016, in Luxembourg.

CloudCom 2016, part of IEEE's Cloud Computing Initiative, will feature world-class keynotes, technical papers, tutorials and business panels addressing the key theme of *Cloud Computing*. 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 (supported also by IEEE Technical Committee on Scalable Computing (TCSC and its participants. Since 2009, the conference is committed to fostering the latest technological breakthroughs and business policies. IEEE CloudCom 2016 is expected to attract more than 300 of industry professionals, scientists, and academics from all over the world.

CloudCom is an official portfolio conference of IEEE, the world largest professional association, with over 400,000 members from 160 countries, dedicated to advancing technological innovation and excellence. The full-fledged support of IEEE, IEEE Communication Society, IEEE Cloud Computing Initiative and IEEE Technical Committee on Scalable Computing guarantee high international recognition, quality and visibility.

Participating Members:

- Pascal BOUVRY (Co-Chair)
- Sébastien VARRETTE (Co-Chair)
- Grégoire DANOY (Programme Chair)
- Abdallah Ali Zainelabden Abdallah IBRAHIM (Organising Committee)
- Valentin PLUGARU (Workshops and Tutorials Chair)

8th International Conference on Adaptive and Self-Adaptive Systems and Applications (ADAPTIVE 2016)

Location: Rome, Italy, March 20, 2016 – March 24, 2016.

Participating Members:

- Jean BOTEV (Program Committee Member)

8th International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT 2016)

http://www.icumt.info/2016/

Location: Lisbon, Portugal, Oct. 18, 2016 – Oct. 20, 2016.

Description: ICUMT is an IEEE (R8 + Portugal Section) technically co-sponsored (approved) premier an annual international congress providing an open forum for researchers, engineers, network planners and service providers targeted on newly emerging algorithms, systems, standards, services, and applications, bringing together leading international players in telecommunications, control systems, automation and robotics. The event is positioned as a major international annual congress for the presentation of original and fundamental research and engineering results.

Participating Members:

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

8th International Workshop on Massively Multiuser Virtual Environments (MMVE 2016)

Location: Klagenfurt, Austria, May 12, 2016.

Participating Members:

- Jean BOTEV (Chair)
- Steffen ROTHKUGEL (Program Committee Member)

8th NCTA - International Conference on Neural Computation Theory and Applications

Location: Porto, Portugal, Nov. 9, 2016 – Nov. 11, 2016.

Participating Members:

- Christoph SCHOMMER (PC Member)

9th International Conference on Security of Information and Networks (SIN 2016)

http://www.sinconf.org/sin2016/index.php

Location: Newark, United States of America, July 20, 2016 – July 22, 2016.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

ACM Genetic and Evolutionary Computation Conference (GECCO 2016)

http://gecco-2016.sigevo.org/index.html/HomePage#&panel1-4

Location: Denver, United States of America, July 20, 2016 – July 24, 2016.

Description: The Genetic and Evolutionary Computation Conference (GECCO 2016) will present the latest high-quality results in genetic and evolutionary computation. Topics include: genetic algorithms, genetic programming, evolution strategies, evolutionary programming, memetic algorithms, hyper heuristics, real-world applications, evolutionary machine learning, evolvable hardware, artificial life, adaptive behavior, ant colony optimization, swarm intelligence, biological applications, evolutionary robotics, coevolution, artificial immune systems, and more.

Participating Members:

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

ACM/IEEE 19th International Conference on Model Driven Engineering Languages and Systems (MODELS 2016)

http://models2016.irisa.fr/

Location: Saint Malo, Brittany, France, Oct. 2, 2016 – Oct. 7, 2016.

Participating Members:

- Lionel BRIAND (Steering Committee Member)
- Shiva NEJATI (Program Committee Member)
- Mehrdad SABETZADEH (Organising Committee)

ADaCoR (Advanced Data Collection and Risks) Industry Workshop

https://www.itrust.lu/event/adacor/

Location: Luxembourg, Luxembourg, April 19, 2016 – April 21, 2016.

Description: Sasan Jafarnejad gave a talk on ”Lessons learned from Car Hacking”.

Participating Members:

- Sasan JAFARNEJAD (Invited Speaker)

Aetos International Workshop on ”Research Challenges for Future RPAS/UAV Systems (AETOS 2016)

http://www.labri.fr/perso/chaumett/aetos-iw-2016/

Location: Bordeaux, France, Oct. 12, 2016 – Oct. 13, 2016.

Description: This conference is the fourth in the series on Unmanned Aerial Systems with applications to real-world scenarios. It focuses on UAS, supportive technologies, software environments and the associated key research issues. The aim is to bring together the community and to provide an opportunity to share experiences and views of current trends and activities in the domain.

Participating Members:

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

AFI 360 Conference Track on Future Internet and Internet of Things Applications

http://futureiotapps.org/2016/show/home

Location: Puebla, Mexico, May 25, 2016 – May 27, 2016.

Description: The rapid advancement of ubiquitous computation and mobile networks together are enabling technology advancements in the area of sensing, predicting and controlling of our physical spaces. Such technology advancements are nowadays deployed in a web based information creation and sharing platform to give form to what is now known as the Internet of Things. This conference is targeting academics from fields like AI, operations research, networks, multiagent systems and related. Theoretical and applied work is welcome.

Participating Members:

- Latif LADID (Keynote speaker)

AITP16 - Artificial Intelligence and Theorem Proving

Location: Obergurgl, Austria, April 3, 2016 – April 7, 2016.

Participating Members:

- Marcos CRAMER (Program Committee Member)

BIDMA - International Symposium on Big Data Management and Analytics

Location: Calgary, Canada, April 25, 2016 – April 26, 2016.

Participating Members:

- Christoph SCHOMMER (PC Member)

COIN @ AAMAS 2016

https://nms.kcl.ac.uk/ais/coin2016/

Location: Singapore, Singapore, May 10, 2016.

Description: The pervasiveness of open systems raises a range of challenges and opportunities for research and technological development in the area of autonomous agents and multi-agent systems. Open systems comprise loosely coupled entities interacting within a social space. These entities join the social space in order to achieve some goals that are unattainable by agents in isolation. However, when those entities are autonomous, they might misbehave and, furthermore, in open systems one may not know what entities will be active beforehand, when they may become active or when these entities may leave the system. The challenge in the design and construction of open systems is to devise mechanisms that foster interactions that are conducive to achieving individual or collective goals.

Coordination, organizations, institutions and norms are four key governance elements, and the COIN workshops constitute a space for debate and exploration of these four elements for the design and use of open systems. We seek to attract high-quality papers and an active audience to debate mathematical, logical, computational, methodological, implementational, philosophical and pragmatic issues related to the four aspects of COIN. Of particular interest for the workshop are those papers that articulate a challenging or innovative view.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

COIN++@ECAI2016 – Workshop on Coordination, Organisation, Institutions, and Norms in Multi-Agent Systems

http://www.cs.bath.ac.uk/coin@ecai2016/index.shtml

Location: The Hague, Netherlands, Aug. 30, 2016.

Description: Coordination, organizations, institutions and norms are four key elements in governance, and the COIN workshop series constitutes a space for debate and exploration of these four elements for the design and use of open systems. We seek to attract high-quality papers and an active audience to debate mathematical, logical, computational, methodological, implementation, philosophical and pragmatic issues related to the four aspects of COIN. At ECAI, COIN is joined by NorMAS to become COIN++. NorMAS focuses on one of the COIN aspects, namely normative multi-agent systems; systems in the behavior of which norms play a role and which need normative concepts in order to be described or specified. A normative multi-agent system combines models for normative systems (dealing for example with obligations, permissions and prohibitions) with models for multi-agent systems.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

COLLA 2016 - The Sixth International Conference on Advanced Collaborative Networks, Systems and Applications -

Location: Barcelona, Spain, Nov. 13, 2016 – Nov. 17, 2016.

Participating Members:

- Remus-Alexandru DOBRICAN (Technical Program Committee Member)

COMMA 2016 - International Conference on Computational Models of Argument

Location: Potsdam, Germany, Sept. 13, 2016 – Sept. 16, 2016.

Participating Members:

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

CompArch 2016

http://www.softwarearchitecture.org/

Location: Venice, Italy, April 5, 2016 – April 8, 2016.

Participating Members:

- Domenico BIANCULLI (Program Committee Member)

ECAI - European Conference on Artificial Intelligence.

Location: The Hague, Netherlands, Aug. 29, 2016 – Sept. 2, 2016.

Participating Members:

- Giovanni CASINI (Program Committee Member)
- Marcos CRAMER (Program Committee Member)
- Emil WEYDERT (Program Committee Member)
- Christoph SCHOMMER (PC Member)
- Leon VAN DER TORRE (Tutorial Chair)
- Livio ROBALDO (Tutorial Organizer)
- Leon VAN DER TORRE (SPC member)

ECML/PKDD

Location: Riva des Garda, Italy, Sept. 19, 2016 – Sept. 23, 2016.

Participating Members:

- Christoph SCHOMMER (PC Member)

EOM 2016 - Workshop on ”Exploring Old Maps”

Location: Luxembourg, Luxembourg, June 8, 2016.

Participating Members:

- Christoph SCHOMMER (Chair)

ETSI IP6 Industry Specification Group

https://portal.etsi.org/tb.aspx?tbid=827&SubTB=827

Location: Nice, France, Feb. 1, 2016.

Description: ISG IP6 is addressing the transition from IPv4 to IPv6, which will support the sustainability and growth of the Internet and enable it to cater for the new technologies based on it.

The group's task is to:

- outline best practices
- gather support
- create awareness of the impact of IPv6 for critical stakeholders such as enterprises, Internet service providers, governments, safety and emergency services and the education sector

We have also begun work on the impact of IPv6 on emerging technologies such as the Internet of Things, smart grids, OpenStack-based Cloud computing, Software-Defined Networking-Network Functions Virtualization and the 5G mobile wireless Internet.

Participating Members:

- Latif LADID (Chair)

Eurocrypt 2016

http://ist.ac.at/eurocrypt2016/

Location: Vienna, Austria, May 8, 2016 – May 12, 2016.

Participating Members:

- Dmitry KHOVRATOVICH (Program Committee Member)

European Language Ressource Allocation Workshop

Location: Luxembourg, Luxembourg, June 14, 2016.

Participating Members:

- Christoph SCHOMMER (Chair)

Europe Middle East and North Africa Conference on Technology and Security to Support Learning 2016 (EURO-MENA TSSL 2016)

http://www.emena.org/

Location: Saïdia, Morocco, Oct. 3, 2016 – Oct. 5, 2016.

Description: EMENA-TSSL'16 conference has two aims, first it provides the ideal opportunity to bring together professors, researchers and high education students of different disciplines, discuss new issues, and discover the most recent developments, researches and trends on Information & Communication Technologies, Security and Emerging Technologies in Learning. Second goal is focusing on to boost a future collaboration and cooperation among the researchers and academicians in these two neighboring regions. EMENA covers more than 60 countries.

Participating Members:

- Latif LADID (Keynote speaker)

Europe, Middle East and North Africa Conference on Technology and Security to Support Learning (EMENA-TSSL'16)

Location: Saïdia, Morocco, Oct. 3, 2016 – Oct. 5, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)

Europe's Security: the responsability of States, of the Union and of Citizens

Location: Luxembourg, Luxembourg, Oct. 1, 2016.

Description: Round Table discussion organised by the Conference of European Justice & Peace Commissions.

Participating Members:

- Gabriele LENZINI (Invited Speaker)

FAB - International Symposium on Foundations and Applications of Big Data Analytics.

Location: Davis, United States of America, Aug. 20, 2016 – Aug. 21, 2016.

Participating Members:

- Christoph SCHOMMER (PC Member)

Fast Software Encryption 2016 (FSE 2016)

http://fse.rub.de/

Location: Bochum, Germany, March 20, 2016 – March 23, 2016.

Description: The workshop concentrates on fast and secure primitives for symmetric cryptography, including the design and analysis of block ciphers, stream ciphers, hash functions, encryption schemes, analysis and evaluation tools and message authentication codes.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)
- Dmitry KHOVRATOVICH (Program Committee Member)

Fifth International Symposium on Energy Challenges and Mechanics

http://nscj.co.uk/ecm5/

Location: Inverness, United Kingdom, July 10, 2016 – July 14, 2016.

Description: Since James Watt, a Scottish inventor, improved the efficiency of steam engine, human civilization relies more and more on a steady energy supply. Today, the world is poised on the brink of two historic energy transformations: replacing oil with electricity in transportation, and replacing high carbon, finite-supply coal and natural gas with renewable wind, solar, marine and biomass energies for electricity production. This symposium is about current state of the art small scale technologies being applied to solve energy challenges.

Participating Members:

- Latif LADID (Keynote speaker)

Fourteenth Annual Conference on Privacy, Security and Trust (PST'16)

Location: Auckland, New Zealand, Dec. 12, 2016 – Dec. 14, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)

Fourth International Symposium on Security in Computing and Communications (SSCC'16)

Location: Jaipur, India, Sept. 21, 2016 – Sept. 24, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)

Grande Region Security and Reliability Day 2016 (GRSRD'16)

Location: Nancy, France, March 16, 2016.

Participating Members:

- Jun PANG (Co-Chair)
- Peter Y. A. RYAN (PC Member)

High Performance Computing & Energy Efficiency (HPCEE 2016)

https://www.irit.fr/~Georges.Da-Costa/pages/hpcee.html

Location: Porto, Portugal, July 1, 2016.

Description: Current large scale IT systems are becoming pervasive. Data centers are used from web searches to protein analysis. Energy consumption of these systems is part of the fastest growing of the worldwide energy consumers. As an example, the top supercomputer in the Top500 ranking (Tianhe-2) consumes 18MW, enough to power a city of 30,000 citizens. Two observations can be made on HPC large scale systems: their energy consumption is too important and these systems are getting more and complex to manage. Moreover consuming such quantities of energy produces a lot of heat. Thermal-aware management aims to improve power consumption efficiency by coordinating resource management and thermal based decisions.

How to optimize the resources usage to obtain a "green" infrastructure and to improve energy efficiency?

This workshop is focused on scheduling policies and tools to address energy efficiency for large scale Data Centers and HPC applications.

Participating Members:

- Pascal BOUVRY (Program Committee Member)

HPC School 2016

Location: Luxembourg, Luxembourg, Nov. 25, 2016.

Description: The UL HPC management team will offer instructions and practical sessions with the aim to cover the basic usage of the platform for newcomers, on the following topics:

- Accessing and interacting with the UL HPC infrastructure
- HPC challenges, especially as regards data and storage management
- HPC workflow management
- Software environment deployment

New members of the UL or HPC beginners should not miss this opportunity to learn about the efficient usage of the HPC platform.

This fourth edition of the UL HPC School will take place on:
November 25th, 2016, in the Belval campus - MSA auditorium 3.330

Participating Members:

- Sébastien VARRETTE (Keynote speaker)
- Valentin PLUGARU (Organising Committee)
- Sébastien VARRETTE (Organising Committee)

ICAART - 8th International Conference on Agents and Artificial Intelligence

Location: Rome, Italy, Feb. 24, 2016 – Feb. 26, 2016.

Participating Members:

- Dragan DODER (Program Committee Member)
- Christoph SCHOMMER (PC Member)

IEEE 4th International Conference on Future Internet of Things and Cloud

http://www.ficloud.org/2016/

Location: Vienna, Austria, Aug. 22, 2016 – Aug. 24, 2016.

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:

- Latif LADID (Keynote speaker)

IEEE 5G Berlin Summit - Conference on Standards for Communications & Networking (CSCN 16)

http://www.5gsummit.org/berlin/

Location: Berlin, Germany, Nov. 2, 2016.

Description: CSCN'16 will deliver a rich technical program discussing the future of mobile communications systems, offering four distinguished keynotes, two panels and a dozen of technical sessions. The sessions consist of technical papers reviewed and selected by an international technical program committee representing both academia and industry, with a strong standardization background.

Participating Members:

- Latif LADID (Chair)

IEEE ASONAM - International Conference on Advances in Social Networks Analysis and Mining

Location: Davis, United States of America, Aug. 18, 2016 – Aug. 21, 2016.

Participating Members:

- Christoph SCHOMMER (PC Member)

IEEE Congress on Evolutionary Computation (IEEE CEC 2016)

http://www.wcci2016.org/index.php

Location: Vancouver, Canada, July 24, 2016 – July 29, 2016.

Participating Members:

- Grégoire DANOY (Program Committee Member)

IEEE Global Communications Conference

http://globecom2016.ieee-globecom.org/

Location: Washington, United States of America, Dec. 4, 2016 – Dec. 8, 2016.

Description: IEEE GLOBECOM is one of two flagship conferences of the IEEE Communications Society (ComSoc), and is the largest annual gathering of communications engineering professionals bringing together researchers from academia, industry and governments, technical staff and industry management from all over the world.

Participating Members:

- Latif LADID (Chair)

IEEE/IFIP Network Operations and Management Symposium

http://noms2016.ieee-noms.org/

Location: Istanbul, Turkey, April 25, 2016 – April 29, 2016.

Description: Held in even-numbered years since 1988, NOMS 2016 will follow the 28 years tradition of NOMS as the primary IEEE Communications Society's forum for technical exchange on management of information and communication technology focusing on research, development, integration, standards, services, and user communities. NOMS 2016 focuses on the theme "Managing Everything toward a Secure, Smart, and Hyperconnected World," presenting recent, emerging approaches, and technical solutions for dealing with future network and ICT infrastructures, as well as with novel services provided in smart and hyper-connected environments (e.g., smart cities, Internet of Things).

Participating Members:

- Latif LADID (Panelist)

IEEE International Conference on Communications (ICC) 2016

http://icc2016.ieee-icc.org/

Location: Kuala Lumpur, Malaysia, May 23, 2016 – May 27, 2016.

Participating Members:

- Maria Rita PALATTELLA (Technical Program Committee Member)

IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies

http://www.emergitech2016.org/

Location: Balaclava, Mauritius, Aug. 3, 2016 – Aug. 6, 2016.

Description: The 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (IEEE EmergiTech 2016) is the new flagship Conference of the IEEE Mauritius Subsection following the flamboyant achievement of 2013 IEEE AFRICON conference. The first edition of IEEE EmergiTech 2016 is organised jointly with the University of Technology, Mauritius (UTM) and aims to provide an interdisciplinary forum where industry, Government, and academia will meet to discuss the most recent innovations, trends, and concerns regarding the evolution of technology and its impact on societies and businesses.

Participating Members:

- Latif LADID (Keynote speaker)

IEEE International Conference on Software Analysis, Evolution, and Reengineering

Location: Osaka, Japan, March 14, 2016 – March 18, 2016.

Participating Members:

- Dongsun KIM (Program Committee Member)

IEEE International Conference on Software Testing, Verification and Validation (ICST 2016)

https://www.cs.uic.edu/~icst2016/

Location: Chicago, IL, United States of America, April 10, 2016 – April 15, 2016.

Participating Members:

- Lionel BRIAND (Programme Chair)
- Shiva NEJATI (Program Committee Member)

IEEE Wireless Communications and Networking Conference (WCNC) 2016

http://wcnc2016.ieee-wcnc.org/

Location: Doha, Qatar, April 3, 2016 – April 6, 2016.

Description: IEEE WCNC is the world premier wireless event that brings together industry professionals, academics, and individuals from government agencies and other institutions to exchange information and ideas on the advancement of wireless communications and networking technology.

Participating Members:

- Maria Rita PALATTELLA (Technical Program Committee Member)

IEEE World Forum on Internet of Things

http://wfiot2016.ieee-wf-iot.org/

Location: Reston, United States of America, Dec. 12, 2016 – Dec. 14, 2016.

Description: The 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) – IoT: Smart Innovation for Vibrant Ecosystems is a unique event for industry leaders, academics and decision making government officials.

This event is designed to examine key critical innovations across technologies which will alter the research and application space of the future. The Internet of Things envisions a highly networked future, where every object is integrated to interact with each other, allowing for communications between objects, as well as between humans and objects, which enables the control of intelligent systems in our daily lives.

Participating Members:

- Latif LADID (Co-Chair)
- Maria Rita PALATTELLA (Technical Program Committee Member)

IETF 96 Meeting

Location: Berlin, Germany, July 17, 2016 – July 22, 2016.

Participating Members:

- Maria Rita PALATTELLA (Invited Speaker)

IJCAI16

Location: New York, United States of America, July 9, 2016 – Sept. 15, 2016.

Participating Members:

- Giovanni CASINI (Program Committee Member)
- Marcos CRAMER (Program Committee Member)

Inaugural Singapore Cyber Security R&D Conference (SG-CRC 2016)

http://itrust.sutd.edu.sg/sg-crc-2016/

Location: Singapore, Singapore, Jan. 14, 2016 – Jan. 15, 2016.

Participating Members:

- Lionel BRIAND (Program Committee Member)

International Conference “Digital Transformation & Global Society”

http://dtgs.ifmo.ru/

Location: St. Petersburg, Russia, June 22, 2016 – June 24, 2016.

Description: The conference will be held in June, 24-25, as a part of the Joint Conference “Internet and Modern Society” (IMS-2016), which takes place in St. Petersburg annually since 1998 and brings together leading researchers and professionals in the field of Information Society issues.

Participating Members:

- Latif LADID (Keynote speaker)

International Conference on Innovations in Mobile Privacy and Security (IMPS 2016)

http://groups.inf.ed.ac.uk/security/IMPS/

Location: London, United Kingdom, April 6, 2016.

Participating Members:

- Gabriele LENZINI (Program Committee Member)

International Conference on Integrated and Sustainable Transportation (INTGAST)

Location: Malacca, Malaysia, Dec. 15, 2016 – Dec. 17, 2016.

Participating Members:

- Grégoire DANOY (Program Committee Member)

International Conference on Mobile, Secure and Programmable Networking (MSPN'16)

Location: Paris, France, June 1, 2016 – June 3, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)

International Conference on Renewable Energies and Power Quality

http://www.icrepq.com/

Location: Madrid, Spain, May 4, 2016 – May 6, 2016.

Description: The intention of the organisers of the International Conference on Renewable Energies and Power Quality (ICREPQ) is to give an opportunity to academics, scientists, engineers, manufacturers and users from all over the world to come together in a pleasant location to discuss recent development in the areas of Renewable Energies and Power Quality.

Participating Members:

- Surena NESHVAD (Invited Speaker)

International Conference on Signal Processing and Communication Systems (SPCS'16)

Location: Lisbon, Portugal, April 7, 2016 – April 8, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)

International Conference on Telecommunications and Multimedia

http://www.temu.gr/index.html

Location: Heraklion, Greece, July 25, 2016 – July 27, 2016.

Description: The International Conference on Telecommunications and Multimedia (TEMU) provides a forum for discussion on recent advances in wired and wireless communication systems, audiovisual applications and content creation/delivery technologies, Internet services and interactive applications, as well as on tools and techniques for their performance evaluation and QoS/QoE validation under simulated and real conditions environments. It was launched in 2006 as a bi-annual international conference, motivated by the ever increasing interest in the above R&D fields, their strategic importance in humans' everyday life and their impact on users' personal and social activities. TEMU 2016 will celebrate its ten-year anniversary under the Technical Co-Sponsorship of IEEE/ComSoc.

Participating Members:

- Latif LADID (Chair)

International Symposium on Search-Based Software Engineering (SSBSE 2016)

Location: Raleigh, NC, United States of America, Oct. 8, 2016 – Oct. 10, 2016.

Participating Members:

- Dongsun KIM (Program Committee Member)

International Workshop on Emerging Trends in Software Metrics (WoETSM)

Location: Austin, TX, United States of America, May 14, 2016 – May 22, 2016.

Participating Members:

- Dongsun KIM (Program Committee Member)

International Workshop on Parallel Optimization using/for Multi and Many-core High Performance Computing (POMCO 2016)

http://hpcs2016.cisedu.info/2-conference/workshops---hpcs2016/workshop20-pomm

Location: Innsbruck, Austria, July 18, 2016 – July 22, 2016.

Description: This workshop seeks to provide an opportunity for the researchers to present their original contributions on the joint use of advanced (discrete or continuous, single or multi-objective, static or dynamic, deterministic or stochastic, hybrid) optimization methods and distributed and/or parallel multi/many-core computing, and any related issues.

Participating Members:

- Pascal BOUVRY (Program Committee Member)

INTERNATIONAL WORKSHOP ON SECURE INTERNET OF THINGS (SIOT 2016)

http://siot-workshop.org/

Location: Crete, Greece, Sept. 27, 2016.

Participating Members:

- Alfredo RIAL DURAN (PC Member)

IoV-VoI 2016 : Workshop on Internet of Vehicles and Vehicles of Internet

http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=51967&copyownerid=85368

Location: Paderborn, Germany, July 5, 2016.

Description: First International Workshop on Internet of Vehicles and Vehicles of Internet,
co-located with ACM MobiHoc 2016

Participating Members:

- Raphaël FRANK (Chair)
- German CASTIGNANI (Technical Program Committee Member)

IPv6 World Congress 2016

http://www.uppersideconferences.com/mpls-sdn-nfv/2016/

Location: Paris, France, March 8, 2016 – March 11, 2016.

Description: The Congress focus on IPv6 centric, Segment Routing, country

deployment status, and measurement. The agenda will also place particular emphasis on open source issues. Other sessions will cover in details SDN, NFV and IoT challenges.

Participating Members:

- Latif LADID (Chair)

ISAS 2016 - International Symposium on Aggregation and Structures

Location: Luxembourg, Luxembourg, July 5, 2016 – July 8, 2016.

Participating Members:

- Emil WEYDERT (Program Committee Member)

ISSRE 2016 - 27th IEEE International Symposium on Software Reliability Engineering

http://2016.issre.net/

Location: Ottawa, Canada, Oct. 23, 2016 – Oct. 27, 2016.

Participating Members:

- Nicolas GUELFI (PC Member)

JELIA16

http://www.cyprusconferences.org/jelia2016/

Location: Larnaca, Cyprus, Nov. 9, 2016 – Nov. 11, 2016.

Participating Members:

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

Joint ITU/UNECE Workshop on Laying the foundation for Sustainable Development Goals: Role of Smart Sustainable Cities

https://www.itu.int/en/ITU-T/Workshops-and-Seminars/Pages/201605/forum-20160502.aspx

Location: Geneva, Switzerland, May 2, 2016 – May 13, 2016.

Description: International Telecommunication Union (ITU) together with United Nations Economic Commission for Europe (UNECE) organized this event to meet the growing demand for guidance on establishing smarter and more sustainable cities which will in turn assist in the attainment of the Sustainable Development Goals (SDGs) and also help contribute effectively to the Habitat III Process.

Participating Members:

- Latif LADID (Workshop Organiser / Co-Organiser)

JURIX2016

http://jurix2016.unice.fr/

Location: Sophia Antipolis, France, Dec. 15, 2016 – Dec. 16, 2016.

Description: For almost 30 years, the JURIX conference has provided an international forum for research on the intersection of Law, Artificial Intelligence and Information Systems, under the auspices of the JURIX The Foundation for Legal Knowledge Systems.

The 2016 JURIX conference will take place on the beautiful French Riviera on **14, 15 and 16 December 2016.** We invite submissions of papers (long and short), technology demonstrations and proposals for workshops & tutorials.

Participating Members:

- Livio ROBALDO (Workshop Organiser / Co-Organiser)

KR-16

http://kr2016.cs.uct.ac.za/

Location: Cape Town, South Africa, April 25, 2016 – April 29, 2016.

Participating Members:

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

Latin American IPv6 Forum

http://www.lacnic.net/web/eventos/lacnic25

Location: Havana, Cuba, Feb. 4, 2016 – May 4, 2016.

Description: LACNIC is an international organization based in Montevideo, Uruguay, responsible for administrating IP address space, Reverse Resolution, Autonomous System Numbers and other resources for the region of Latin America and the Caribbean on behalf of the Internet community.

Participating Members:

- Latif LADID (Keynote speaker)

MIning and REasoning with Legal texts (MIREL 2016)

http://jurix2016.unice.fr/?page_id=127

Location: Sophia Antipolis, France, Dec. 14, 2016.

Description: The aim of MIREL-2016 workshop is to bridge the gap between the community working on legal ontologies and NLP parsers and the community working on reasoning methods and formal logic, in line with the objectives of the MIREL (MIning and REasoning with Legal texts) project. The workshop aims at fostering the scientific discussion between approaches based on language technologies applied to the legal domain (representing legal knowledge) and those based on legal reasoning (using the legal knowledge to build specialized services and applications).

Participating Members:

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

MOD - Second International Workshop on Machine Learning, Optimization and Big Data.

Location: Pisa, Italy, July 21, 2016 – July 23, 2016.

Participating Members:

- Christoph SCHOMMER (PC Member)

NESUS - Third Action Workshop (NESUS 2016)

http://www.nesus.eu/third-nesus-action-workshop

Location: Sofia, Bulgaria, Oct. 6, 2016 – Oct. 7, 2016.

Description: NESUS 2016 workshop focuses on the software side, aiming at bringing together researchers from academia and industry interested in the design, implementation, and evaluation of services and system software mechanisms to improve sustainability in ultrascale computing systems with a holistic approach.

Participating Members:

- Pascal BOUVRY (Program Committee Member)

Net Futures 2016

http://netfutures2016.eu/

Location: Brussels, Belgium, April 20, 2016 – April 21, 2016.

Description: NET FUTURES wishes to maximize competitiveness of the European technology industry. The conference will gather over 1.000 attendees, to form an interconnected community involving companies, organizations and people in

- Research & Innovation
- Market Validation & Living Lab Research
- Business Development, Entrepreneurship & Enterprise Strategy
- Policy Making

It is our firm belief that by bridging the gaps between these communities, innovations will more easily and effectively find their way to the market.

Participating Members:

- Latif LADID (Chair)

Ninth Edition of the Requirements Engineering Track (RE-Track 2016)

http://www.cin.ufpe.br/~sac16-re/

Location: Pisa, Italy, April 4, 2016 – April 8, 2016.

Participating Members:

- Mehrdad SABETZADEH (Program Committee Member)

PNSE'16 - International Workshop on Petri Nets and Software Engineering

http://www.informatik.uni-hamburg.de/TGI/events/pnse16/

Location: Torun, Poland, June 20, 2016 – June 21, 2016.

Participating Members:

- Nicolas GUELFI (PC Member)

PRIMA 2016

http://prima2016.di.unito.it/

Location: Phuket, Thailand, Aug. 22, 2016 – Aug. 26, 2016.

Description: Software systems are becoming more intelligent in the kind of functionality they offer users. At the same time, systems are becoming more decentralized, with components that represent autonomous entities who must communicate among themselves to achieve their goals. Examples of such systems range from healthcare and emergency relief and disaster management to e-business and smarts grids. A *multiagent* worldview is crucial to properly conceptualizing, building, and governing such systems. It offers abstractions such as *intelligent agent, protocol, norm, organization, trust, incentive*, and so on, and is rooted in solid computational and software engineering foundations. As a large but still growing research field of Computer Science, multiagent systems today remains a unique enabler of interdisciplinary research.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

Privacy Aware Machine Learning for Health Data Science (PAML'16)

Location: Salzburg, Austria, Sept. 1, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)

RADIANCE@DSN 2016 - International Workshop on Recent Advances in the DependabIlity AssessmeNt of Complex systEmshttp://radiance2016.devasses.eu/

http://radiance2016.devasses.eu/

Location: Toulouse, France, June 28, 2016.

Participating Members:

- Nicolas GUELFI (PC Member)

Second International Conference on Advances and Trends in Software Engineering (SOFTENG 2016)

http://www.iaria.org/conferences2016/SOFTENG16.html

Location: Lisbon, Portugal, Feb. 21, 2016 – Feb. 25, 2016.

Participating Members:

- Duy Cu NGUYEN (Program Committee Member)

SERENE 2016 - 8th International Workshop on Software Engineering for Resilient Systems

http://serene.disim.univaq.it/2016/committees/

Location: Gothenburg, Sweden, Sept. 5, 2016 – Sept. 6, 2016.

Participating Members:

- Nicolas GUELFI (PC Member)

Singapore Cyber Security R&D Conference (SG-CRC'16)

Location: Singapore, Singapore, Jan. 14, 2016 – Jan. 15, 2016.

Participating Members:

- Sjouke MAUW (Program Committee Member)

Software Verication and Testing track at ACM Symposium on Applied Computing 2016 (SAC-SVT'16)

Location: Pisa, Italy, April 3, 2016 – April 8, 2016.

Participating Members:

- Jun PANG (Program Committee Member)

Student Contest on Software Engineering (SCORE 2016)

http://score-contest.org/2016/projects.php

Location: Austin, TX, United States of America, May 14, 2016 – May 22, 2016.

Participating Members:

- Domenico BIANCULLI (Program Committee Member)

Summer School on Verication Technology, Systems & Applications (VTSA'16)

Location: Liege, Belgium, Aug. 28, 2016 – Sept. 2, 2016.

Description: The fourth summer school on verication technology, systems & applications takes place at University of Liege, Belgium from August 29th to September 2th, 2016. All three aspects verication technology, systems & applications strongly depend on each other and that progress in the area of formal analysis and verication can only be made if all three aspects are considered as a whole. Five speakers Hubert Comon, Thomas Eiter, Jean Krivine, Tobias Nipkow and Ruzica Piskac stand for this view in that they represent and will present a particular verication technology and its implementation in a system in order to successfully apply the approach to real world verication problems. There were about 20 participants for the summer school.

Participating Members:

- Jun PANG (Organizing Chair)

Tenth IFIP WG 11.11 International Conference on Trust Management (IFIPTM'16)

Location: Darmstadt, Germany, July 18, 2016 – July 22, 2016.

Description: The tenth IFIP TM conference took part in Darmstadt (Germany) as part of the Security and Privacy Week 2016. The conference focused on all aspects of trust, including trust and reputation management systems, trust models, identity management and socio-technical, economic and sociological

aspects of trust. The conference featured key note speeches by Vijay Varadharajan (Macquarie University, Australia) and Simone Fischer-Hübner (Karlstadt University, Sweden). Besides the main conference, there was a very successful graduate student symposium.

Participating Members:

- Sjouke MAUW (Co-Chair)
- Gabriele LENZINI (PC Member)

The 10th Multi-Disciplinary International Workshop on Artificial Intelligence (MIWAI 2016)

https://khamreang.msu.ac.th/miwai16/

Location: Chiang Mai, Thailand, Dec. 7, 2016 – Dec. 9, 2016.

Description: Artificial Intelligence (AI) research has broad applications in real world problems. Examples include control, planning and scheduling, pattern recognition, knowledge mining, software applications, strategy games an others. The ever-evolving needs in society and business both on a local and on a global scale demand better technologies for solving more and more complex problems. Such needs can be found in all industrial sectors and in any part of the world.

This workshop aims to be a meeting place where excellence in AI research meets the needs for solving dynamic and complex problems in the real world. The academic researchers, developers, and industrial practitioners will have extensive opportunities to present their original work, technological advances and practical problems. Participants can learn from each other and exchange their experiences in order to fine tune their activities in order to help each other better. The main purposes of the MIWAI series of workshops are:

- To provide a meeting place for AI researchers and practitioners.
- To inform research students about cutting-edge AI research via the presence of outstanding international invited speakers.
- To raise the standards of practice of AI research by providing researchers and students with feedback from an internationally-renowned program committee.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

The 2016 IEEE International Conference on Software Quality, Reliability & Security (QRS 2016)

http://paris.utdallas.edu/qrs16/

Location: Vienna, Austria, Aug. 1, 2016 – Aug. 3, 2016.

Participating Members:

- Duy Cu NGUYEN (Program Committee Member)

The 20th International Conference on Knowledge Engineering and Knowledge Management (EKAW 2016)

http://ekaw2016.cs.unibo.it/

Location: Bologna, Italy, Nov. 19, 2016 – Nov. 23, 2016.

Description:

The 20th International Conference on Knowledge Engineering and Knowledge Management is concerned with the impact of time and space on the representation of knowledge. Knowledge engineering has mostly been about creating static, universal representations. Yet the world is rarely static: everything changes, including the models, and real world systems need to evolve along with the surrounding world. Also, what makes some representations valid in some contexts may make them invalid elsewhere (e.g., jurisdiction for laws).

The special focus of this year's EKAW is "evolving knowledge", which concerns all aspects of the management and acquisition of knowledge representations of evolving, contextual, and local models. This includes change management, trend detection, model evolution, streaming data and stream reasoning, event processing, time-and space dependent models, contextual and local knowledge representations, etc.

EKAW 2016 will put a special emphasis on the evolvability and localization of knowledge and the correct usage of these limits.

Participating Members:

- Leon VAN DER TORRE (Workshop Organiser / Co-Organiser)

The 28th Benelux Conference on Artificial Intelligence (BNAIC2016)

http://bnaic2016.cs.vu.nl

Location: Amsterdam, Netherlands, Nov. 10, 2016 – Nov. 11, 2016.

Description: BNAIC is the Annual Benelux Conference on Artificial Intelligence. This year, the 28th edition of BNAIC is jointly organized by the University of Amsterdam and the Vrije Universiteit Amsterdam, under the auspices of the Benelux Association for Artificial Intelligence (BNVKI) and the Dutch Research School for Information and Knowledge Systems (SIKS).

Participating Members:

- Grégoire DANOY (Program Committee Member)

the 28th International Conference on Legal Knowledge and Information Systems

http://jurix2015.di.uminho.pt/

Location: Braga, Portugal, Dec. 9, 2016 – Dec. 11, 2016.

Description: For more than 25 years, the JURIX conference has provided an international forum for academics and practitioners for the advancement of cutting edge research in the interface between law and computer technology.

The 2015 JURIX conference will take place at the University of Minho, Law School, Campus of Gualtar, Braga, Portugal, on 9, 10 and 11 December, 2015. As JURIX 2015 approaches, more information will be published on the conference website, or distributed via Twitter by @jurixfoundation using the hashtag #jurix15. The JURIX conferences are held under the auspices of the JURIX The Foundation for Legal Knowledge Systems.

Participating Members:

- Livio ROBALDO (Program Committee Member)

The 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech'16)

http://www.macc.ma/cloudtech16/

Location: Marrakech, Morocco, May 24, 2016 – May 26, 2016.

Description: CloudTech'16 will address topics related to cloud technologies; architecture and applications including distributed computing and data centers, cloud infrastructure and its security, end-user services, Big data and its applications. The conference will provide a high-level, international forum for scientists, researchers, professionals and students who will have the opportunity to present state-of-the-art research results, address new challenges, and

discuss trends in Cloud Technology and Big data.

Participating Members:

- Pascal BOUVRY (Program Committee Member)
- Grégoire DANOY (Program Committee Member)
- Claudio FIANDRINO (Program Committee Member)
- Dzmitry KLIAZOVICH (Program Committee Member)

The 7th International Conference on Trusted Systems(INTRUST 2015)

Location: Beijing, China, Dec. 7, 2015 – Feb. 8, 2016.

Participating Members:

- Qiang TANG (Co-Chair)
- Qiang TANG (Co-Chair)

The First Chinese Conference on Logic and Argumentation (CLAR 2016)

http://www.xixilogic.org/events/clar2016

Location: Hangzhou, China, April 2, 2016 – April 3, 2016.

Description: The interplay of logic and argumentation has a long history, from ancient Aristotle's logic to very recent formal argumentation in AI. This is an interdisciplinary research field, involving researchers from logic, philosophy, artificial intelligence, and law, etc.

The goal of the CLAR 2016 conference is to promote communication between researchers in the field of logic and argumentation within and outside China.

CLAR 2016 takes place at Xixi Campus, Zhejiang University, Hangzhou, P.R. China during April 2-3, 2016.

Participating Members:

- Dragan DODER (Program Committee Member)

The First International Workshop on Resilience and/or Energy-aware techniques for High-Performance Computing (RE-HPC'16)

http://graal.ens-lyon.fr/~abenoit/RE-HPC/

Location: Hangzhou, China, Nov. 7, 2016 – Nov. 9, 2016.

Participating Members:

- Pascal BOUVRY (Program Committee Member)

The International Conference for Electronic Voting E-Vote-ID 2016

https://www.e-vote-id.org/

Location: Bregenz, Austria, Oct. 18, 2016 – Oct. 21, 2016.

Participating Members:

- Peter Y. A. RYAN (Co-Chair)

The International Workshop on AI for Privacy and Security (PrAISe 2016)

http://mas.cmpe.boun.edu.tr/praise2016/

Location: The Hague, Netherlands, Sept. 2, 2016.

Participating Members:

- Pascal BOUVRY (Program Committee Member)
- Peter Y. A. RYAN (PC Member)

The Second International Symposium on Ubiquitous Networking

http://www.unet-conf.org/UNet2016/index.php

Location: Casablanca, Morocco, May 30, 2016 – June 1, 2016.

Description: UNet is an international scientific event that highlights new trends and findings in hot topics related to ubiquitous computing/networking. This second edition will be held on May 30, 2016, in the fascinating city of Casablanca, Morocco. UNet16 is technically sponsored by IEEE Morocco Section and IEEE COMSOC Morocco Chapter.

Participating Members:

- Latif LADID (Keynote speaker)

The Third International Workshop on Graphical Models for Security (GraMSec'16)

Location: Lisbon, Portugal, June 27, 2016.

Description: Graphical security models provide an intuitive but systematic methodology to analyze security weaknesses of systems and to evaluate potential protection measures. Formal methods and computer security researchers, as well as security professionals from industry and government, have proposed various graphical security modeling schemes. Such models are used to capture different security facets (digital, physical, and social) and address a range of challenges including security assessment, risk analysis, automated defensing, secure services composition, policy validation and verification. The objective of GraMSec is to contribute to the development of well-founded graphical security models, efficient algorithms for their analysis, as well as methodologies for their practical usage.

Participating Members:

- Sjouke MAUW (Steering Committee Member)
- Olga GADYATSKAYA (Program Committee Member)
- Ravi JHAWAR (Program Committee Member)

Third Workshop on Legal Knowledge and the Semantic Web (LK&SW-2016)

http://ekaw-lksw2016.cirsfid.unibo.it/

Location: Bologna, Italy, Nov. 19, 2016.

Description: The two research areas of Legal Knowledge and the Semantic Web are very much interconnected. The legal domain is an appropriate field of study an application for Semantic Web researchers, as it uses and contributes to most of the topics that are relevant to the community. Given the complex interactions of legal actors, legal sources and legal processes, as well as the relevance and potential impact of decisions in social and political processes, law is actually providing challenging contexts and scenarios to reach groundbreaking research results. At the same time, Semantic Web formalisms and technologies provide a set of technical instruments which can be fruitfully adopted by legal experts to representing, interlinking, and reasoning upon the legal knowledge and several of its related aspects —such as provenance, security, data protection, privacy, and trust. In particular, Semantic Web technology might provide standard-based legal knowledge representations to enable the management and reuse of legal information across the Web.

Ontologies, knowledge extraction, and reasoning techniques have been studied by the Artificial Intelligence & Law community for years, but only loosely and sparsely connected with Semantic Web developments. Moreover, additional topics related to the semantics of legal interpretation intersect as well.

The aim of LK&SW-2016 is to study the challenges that the legal domain poses to Semantic Web research, and how Semantic Web technologies and formalisms can contribute to address these open issues. This way, we promote the use of legal knowledge for addressing Semantic Web research questions and, vice versa, to use Semantic Web technologies as reasoning tools to be implemented into the legal domain.

Participating Members:

- Leon VAN DER TORRE (Chair)

Ultrascale Computing for Early Researchers (UCER 2016)

http://dps.uibk.ac.at/~juan/ucer/

Location: Granada, Spain, Dec. 14, 2016 – Dec. 16, 2016.

Description: The aim of this workshop is to give the opportunity to early researchers (PhD students or recent PhD graduates) to show their work related to Ultrascale Computing. Although a future technology, currently, many systems are being designed with the goal of being used in ultrascale systems. Many different subtopics are related in the exploration of system software and applications for enabling a sustainable development of future high-scale computing platforms. The tasks involved range from the analysis of the current state-of-the-art on sustainability in large-scale systems to the proposition of new tools that aim to improve computations on these systems. The topics addressed are, among others, HPC, distributed systems, and big data communities in cross cutting aspects like programmability, scalability, resilience, energy efficiency, and data management. To get the goal of ultrascale computation it is needed to explore new programming paradigms, runtimes, and middlewares to increase the productivity, scalability, and reliability of parallel and distributed programming. At the same time, the new magnitude of data and computations brings up as inevitability consequence the probability of failure, so any advance on resilient schedulers that handle errors reactive or proactive, monitoring and assessment of failures, and malleable applications that can adapt their resource usage at runtime are welcome. Other major challenges involved are the restructuring the Input/Output (I/O) stack, the advancing predictive and adaptive data management, and the concern about huge energy consumption as one of the major limitations. This topic also includes identifying applications, high-level algorithms, and services amenable to ultrascale systems and investigating the redesign and reprogramming efforts needed for applications to efficiently exploit ultrascale platforms while providing sustainability.

Participating Members:

- Grégoire DANOY (Program Committee Member)

VII Workshop on Artificial Intelligence and the Complexity of Legal Systems (AICOL 2016)

http://jurix2016.unice.fr/?page_id=138

Location: Sophia Antipolis, France, Dec. 15, 2016 – Dec. 16, 2016.

Description: The aim of AICOL is to develop models of legal knowledge more suitable to the complexity of contemporary legal systems.

The AICOL workshops welcome research in AI, political and legal theory, jurisprudence, philosophy of technology and the law, social intelligence, nMAS,to address the ways in which the current information revolution affects basic pillars of today's legal and political systems, in such fields as e-democracy, e-government, e-justice, transnational governance, Data Protection, and Security.

Participating Members:

- Leon VAN DER TORRE (Program Committee Member)

Workshop on Internet of Vehicles and Vehicles of Internet

http://www.tech.dmu.ac.uk/~iwagne00/iov-voi2016/index.shtml

Location: Paderborn, Germany, June 5, 2016.

Description: IoV-VoI 2016 First International Workshop on Internet of Vehicles and Vehicles of Internet

Participating Members:

- Latif LADID (Keynote speaker)

C.2 Doctoral Thesis Defense Committee Memberships

Hassan Afzal, University of Luxembourg

Date: Sept. 6, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Leon VAN DER TORRE (Chairman)

PhD Defense Jury External Partners:

- David Fofi (Vice-chairman)
- Bruno Mirbach (Member)

Alessio Antonini, University of Luxembourg

Date: Dec. 12, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Leon VAN DER TORRE (Supervisor)
- Christoph SCHOMMER (Member)

Dennis Appelt, University of Luxembourg

Date: June 24, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Jacques KLEIN (Chairman)
- Duy Cu NGUYEN (Vice-chairman)
- Lionel BRIAND (Supervisor)

PhD Defense Jury External Partners:

- Alexander Pretschner (Member)
- Marco Vieira (Member)

Andreas Chouliaras, University of Luxembourg

Date: June 7, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Christoph SCHOMMER (Co-supervisor)

Lara Codeca, University of Luxembourg

Date: Nov. 18, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Thomas ENGEL (Supervisor)

PhD Defense Jury External Partners:

- Mario Gerla (Vice-chairman)
- Jérôme Härri (Member)
- Christoph Sommer (Member)
- Francesco Viti (Chairman)

PhD Advisory Board Members:

- Raphaël FRANK (Expert)

Daniel Di Nardo, University of Luxembourg

Date: April 22, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Yves LE TRAON (Chairman)
- Lionel BRIAND (Supervisor)

PhD Defense Jury External Partners:

- Robert Feldt (Member)
- Fabrizio Pastore (Vice-chairman)
- Hélène Waeselynck (Member)

Remus-Alexandru Dobrican, University of Luxembourg

Date: Dec. 6, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Pascal BOUVRY (Chairman)
- Denis ZAMPUNIERIS (Supervisor)
- Steffen ROTHKUGEL (Member)

PhD Defense Jury External Partners:

- Anthony Cleve (Vice-chairman)
- Michael Schumacher (Member)

Claudio Fiandrino, University of Luxembourg

Date: Oct. 25, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Denis ZAMPUNIERIS (Chairman)
- Pascal BOUVRY (Supervisor)

PhD Defense Jury External Partners:

- Paolo Giaccone (Vice-chairman)
- Dzmitry Kliazovich (Member)
- Franciszek Seredynski (Member)

Feltus Florian, University of Luxembourg

Date: Nov. 21, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Christoph SCHOMMER (Vice-chairman)

Ibrahim Fahad Jasim GHALYAN, University of Luxembourg

Date: Jan. 14, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Leon VAN DER TORRE (Chairman)

PhD Defense Jury External Partners:

- Gabriel Abba (Member)
- Wolfgang Gerke (Member)

Nicolas Gobillot, Institut Supérieur de l'Aéronautique et de l'Espace (ISAE)

Date: April 29, 2016
Location: Toulouse, France

PhD Defense Jury Members:

- Nicolas NAVET (Examiner)

Susann Gottmann, University of Luxembourg

Date: Dec. 2, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Ulrich SORGER (Chairman)
- Thomas ENGEL (Supervisor)

PhD Defense Jury External Partners:

- Claudia Ermel (Member)
- Frank Hermann (Vice-chairman)
- Raimondas Sasnauskas (Member)

Sviatlana Höhn, University of Luxembourg

Date: Feb. 24, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Leon VAN DER TORRE (Chairman)
- Christoph SCHOMMER (Supervisor)

PhD Defense Jury External Partners:

- Stephan Busemann (Member)
- Charles Max (Member)
- Karola Pitsch (Member)

Llio Humphreys, University of Luxembourg

Date: July 25, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Leon VAN DER TORRE (Co-supervisor)
- Christoph SCHOMMER (Member)

PhD Defense Jury External Partners:

- Matteo Baldoni (Vice-chairman)
- Guido Boella (Co-supervisor)
- Monica Palmirani (Member)
- Giovanni Sartor (Member)

Jean-Louis HUYNEN, University of Luxembourg

Date: June 30, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Gabriele LENZINI (Chairman)
- Peter Y. A. RYAN (Supervisor)

Dimitrios Kampas, University of Luxembourg

Date: May 30, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Ulrich SORGER (Chairman)
- Pascal BOUVRY (Vice-chairman)

- Christoph SCHOMMER (Supervisor)

PhD Defense Jury External Partners:

- Jürgen Rolshoven (Member)
- Philip Treleaven (Member)

Martin Kracheel, University of Luxembourg

Date: April 22, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Thomas ENGEL (Vice-chairman)

PhD Defense Jury External Partners:

- Vincent König (Chairman)
- Romain Martin (Supervisor)
- Roderick McCall (Invited member)
- Francesco Viti (Expert)
- Steffen Walz (Invited member)

Nico Nachtigall, University of Luxembourg

Date: Aug. 29, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Ulrich SORGER (Chairman)
- Thomas ENGEL (Supervisor)

PhD Defense Jury External Partners:

- Frank Hermann (Vice-chairman)
- Barbara König (Member)
- Raimondas Sasnauskas (Member)

PhD Advisory Board External Partners:

- Benjamin Braatz (Expert)

Surena Neshvad, University of Luxembourg

Date: June 14, 2016
Location: Luxembourg City, Luxembourg

PhD Defense Jury Members:

- Thomas ENGEL (Chairman)
- Juergen SACHAU (Supervisor)

PhD Defense Jury External Partners:

- Markus Jostock (Examiner)
- Stijn Stevens (Examiner)

Anh Quan Nguyen, University of Luxembourg

Date: Dec. 12, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Steffen ROTHKUGEL (Chairman)
- Grégoire DANOY (Member)

PhD Defense Jury External Partners:

- Frédéric Guinand (Vice-chairman)
- El-Ghazali Talbi (Member)

PhD Advisory Board Members:

- Grégoire DANOY (Member)

Sune Nielsen, University of Luxembourg

Date: Feb. 24, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Pascal BOUVRY (Supervisor)
- Grégoire DANOY (Member)

PhD Defense Jury External Partners:

- Wiktor Jurkowski (Member)
- Roland Krause (Expert)
- Reinhard Schneider (Chairman)
- El-Ghazali Talbi (Vice-chairman)

PhD Advisory Board Members:

- Grégoire DANOY (Advisor)

Martin Sewell, UCL London

Date: Sept. 26, 2016
Location: London, United Kingdom

PhD Defense Jury Members:

- Christoph SCHOMMER (Examiner)

Ana-Maria Simionovici, University of Luxembourg

Date: Oct. 25, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Steffen ROTHKUGEL (Chairman)
- Pascal BOUVRY (Supervisor)

PhD Defense Jury External Partners:

- Henri Luchian (Vice-chairman)
- Franciszek Seredynski (Member)
- Andrei Tchernykh (Member)

Xin Sun, University of Luxembourg

Date: June 30, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Pierre KELSEN (Chairman)
- Xavier PARENT (Vice-chairman)
- Leon VAN DER TORRE (Supervisor)

PhD Defense Jury External Partners:

- Jan Broersen (Member)
- Christian Strasser (Member)

Masoud Tabatabei, University of Luxembourg

Date: Oct. 24, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Leon VAN DER TORRE (Chairman)
- Peter Y. A. RYAN (Supervisor)

Miguel Urquidi, University of Luxembourg

Date: Oct. 10, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Jean-Sébastien CORON (Chairman)
- Peter Y. A. RYAN (Supervisor)
- Jean LANCRENON (Member)

Maryam Vahabi, University of Porto

Date: Jan. 19, 2016
Location: Porto, Portugal

PhD Defense Jury Members:

- Nicolas NAVET (Examiner)

Yang Zhang, University of Luxembourg

Date: Nov. 30, 2016
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Leon VAN DER TORRE (Chairman)
- Jun PANG (Vice-chairman)
- Sjouke MAUW (Supervisor)

PhD Defense Jury External Partners:

- Mathias Humbert (Member)
- Michaël Rusinowitch (Member)

C.3 Awards

Best Paper Award at HotPNS 2016, Nov. 8, 2016

Recipients: Pascal BOUVRY, Dzmitry KLIAZOVICH
Best Paper Award at HotPNS 2016 for the paper by in Wang, Lei Jiao, Dzmitry Kliazovich and Pascal Bouvry titled: "Reconciling Task Assignment and Scheduling in Mobile Edge".

More information at: http://hotpns16.weebly.com/program.html

Best Paper Award at ICAIT-2016, Oct. 8, 2016

Recipients: Nicolas GUELFI, Benjamin JAHIC, Benoit RIES
Best Paper Award for the paper "TESMA: Towards the Development of a Tool for Specification, Management and Assessment of Teaching Programs" presented at the 2nd International Conference on Applications in Information Technology.

Best Paper Award at IEEE Cloudnet 2016, Oct. 5, 2016

Recipients: Pascal BOUVRY, Claudio FIANDRINO, Dzmitry KLIAZOVICH
Best paper award at IEEE Cloudnet 2016 to Andrea Sciarrone, Claudio Fiandrino, Igor Bisio, Fabio Lavagetto, Dzmitry Kliazovich and Pascal Bouvry for the paper titled : *"Smart Probabilistic Fingerprinting for Indoor Localization over Fog Computing Platforms".*

See more here: http://cloudnet2016.ieee-cloudnet.org

Best Paper Award at the International Conference on Design, Learning & Innovation (DLI 2016), May 3, 2016

Recipients: Jean BOTEV, Steffen ROTHKUGEL
Title: "CollaTrEx – Collaborative Context-Aware Mobile Training and Exploration", authors: J. Botev, R. Marschall, S. Rothkugel

Best partner award, Sept. 20, 2016

Recipients: Thomas ENGEL, Stefanie OESTLUND
The SECAN-Lab team received the best partner award for the project FETCH.

Google Internet of Things (IoT) Technology Research Award Pilot, Feb. 10, 2016

Recipients: Thomas ENGEL, Luca LAMORTE, Maria Rita PALATTELLA
The SECAN-Lab team has been recently selected as recipient of the 2016 Google IoT Technology Research Award. The team received a set of Google Internet of Things (IoT) devices such as Intel Edison boards supporting Arduino SW/HW, and Eddystone beacons to be tested in an IoT pilot. The awarded proposal was in line with the work UL is carrying within the H2020 F-Interop project F-Interop aims to develop interoperability, conformance and performance test tools, running on a federation of European testbeds. The SECAN-Lab team will use the Google devices to perform tests, and check their conformance to specific IoT protocols, as well as their interoperability with other IoT devices.

Honorable mention in recognition of the great effort and valuable contribution to the 2nd International Conference on Applications in Information Technology (ICAIT-2016) as member of the conference program committee., Oct. 8, 2016

Recipients: Alfredo CAPOZUCCA

C.4 Media Appearances

Die richtige Adresse - Latif Ladid und der unermüdliche Kampf für ein besseres Internet (LËTZEBUERGER Journal)

Article (Newspaper), Dec. 31, 2016
Members: Thomas ENGEL, Latif LADID

http://www.journal.lu/article/die-richtige-adresse/

Latif Ladid was awarded with the IPv6 Life Time Achievement Award.

IPv6 Lifetime Achievement Award to Latif LADID (BusinessWire)

Article (Internet), Dec. 21, 2016
Members: Thomas ENGEL, Latif LADID

http://www.businesswire.com/news/home/20161221005031/en

Latif Ladid was awarded with the IPv6 Life Time Achievement Award.

Cloud Computing : 200 spécialistes mondiaux du cloud computing se donnent rendez-vous au Luxembourg (Science.lu)

News (Internet), Dec. 13, 2016
Members: Pascal BOUVRY, Sébastien VARRETTE

http://science.lu/fr/content/cloud-computing-200-spécialistes-mondiaux-du-cloud-computing-se-donnent-rendez-vous-au

Puissance de calcul en explosion (PaperJam)

Interview (Internet), Dec. 12, 2016
Members: Pascal BOUVRY

http://paperjam.lu/news/puissance-de-calcul-en-explosion

CloudCom 2016 (PaperJam)

News (Internet), Dec. 8, 2016
Members: Pascal BOUVRY, Sébastien VARRETTE

http://club.paperjam.lu/event/cloudcom-2016

CloudCom 2016 (Innovation.public.lu)

News (Internet), Dec. 8, 2016
Members: Pascal BOUVRY, Sébastien VARRETTE

http://www.innovation.public.lu/fr/agenda/conferences/2016/12/cloudcom/index.html

Dossier Cloud Computing (PaperJam)

Article (Internet), Nov. 1, 2016
Members: Pascal BOUVRY

http://paperjam.lu/dossier/2016/11/technologies/#/page-129137

Beaucoup de matériel, peu de solutions logicielles (LËTZEBUERGER Journal)

Article (Newspaper), Sept. 23, 2016
Members: Thomas ENGEL, Sébastien FAYE

http://www.journal.lu/top-navigation/article/beaucoup-de-materiel-peu-de-solutions-logicielles/

High-fidelity spherical cholesteric liquid crystal Bragg reflectors generating unclonable patterns for secure authentication (Multiple)

Article (Internet), July 8, 2016
Members: Gabriele LENZINI
https://www.youtube.com/watch?v=KOW-Jqtb6NI

http://www.packagedsummit.com/speakers/

https://www.100komma7.lu/program/episode/128400/201607140940-201607140950

http://www.wort.lu/de/wissen/neue-authentifizierungstechnik-luxemburger-forscher-gegenfaelscher-577e259aac730ff4e7f631e8

https://phys.org/news/2016-06-unclonable-patterns-counterfeiting.html

https://idw-online.de/de/news654398

http://www.labo.de/news/produktschutz--faelschungssicher-durch-einzigartigereflexionsmuster.htm

http://www.innovations-report.de/html/berichte/physik-astronomie/faelschungssicher-durcheinzigartige-reflexionsmuster.html

Les coulisses des autoroutes (BFM)

Interview (TV), June 30, 2016
Members: Thomas ENGEL, Sébastien FAYE
Participation in the French TV documentary *RMC Découverte*

De Magazin - Kapital - Wei e Stellewäert fir de Roboter? (RTL Télé Lëtzebuerg)

News (TV), May 27, 2016
Members: Leon VAN DER TORRE, Pouyan ZIAFATI

http://tele.rtl.lu/emissiounen/de-magazin-kapital/3037349.html

News report on robots including Robolab.

“Big Brother“ kennt Dich genau (Luxembourg Wort)

Interview (Newspaper), Feb. 18, 2016
Members: Jun PANG

http://goo.gl/ZD713M

An overview of the research activities of Dr. Jun Pang at the University of Luxembourg.

C.5 Guest Researchers

The following guest researchers were invited to the CSC:

Dr. Benjamin Braatz (Graph-IT GmbH)

Period: Aug. 29, 2016
Hosted by: Thomas ENGEL
Reason: Member of a PhD defense committee.

Prof. Torsten Braun (University of Bern)

Period: May 12, 2016 – May 13, 2016
Hosted by: Thomas ENGEL, Maria Rita PALATTELLA
Reason: Kick off research project meeting

Prof. Dr. Cas Cremers (University of Oxford)

Period: Sept. 16, 2016
Hosted by: Sjouke MAUW

Kristijonas Čyras

Period: Oct. 14, 2016
Hosted by: Leon VAN DER TORRE

Prof. Dr. Falko Dressler (Heinz Nixdorf Institute, University of Paderborn)

Period: Sept. 6, 2016
Hosted by: Thomas ENGEL

Reason: Supervision of Phd student

Joao Duarte (University of Bern)

Period: May 12, 2016 – May 13, 2016
Hosted by: Thomas ENGEL, Maria Rita PALATTELLA
Reason: Kick off research project meeting

Dr. Claudia Ermel (Technical University of Berlin)

Period: Dec. 2, 2016
Hosted by: Thomas ENGEL
Reason: Member of a PhD defense committee.

Dr. Claudia Ermel (Technical University of Berlin)

Period: Aug. 29, 2016
Hosted by: Thomas ENGEL
Reason: Supervision of Phd student

Prof. Dr. Robert Feldt (Blekinge Institute of Technology, Sweden; Chalmers University, Sweden)

Period: April 22, 2016
Hosted by: Lionel BRIAND
Reason: SnT Research Seminar

”Applying Software Testing Research in Industrial Practice – Towards Reporting and Requiring Minimal Information”

Abstract: Based on a set of research projects on helping industrial practitioners improve their testing we propose the hypothesis that it is critical to consider the number of, complexity of and inter-relations between the information sources the improvement one suggest relies on. Very frequently research results from academia do not consider this and are thus less applicable. We propose that future research in software testing should very clearly both consider, limit and describe the information it requires. Additionally the proposed changes must also consider what happens when the actual information available is incomplete, missing and so on. We exemplify from our testing research in industry on system test case aging and test case prioritization and outline experimental procedures for cost/benefit analysis of information sources in empirical software testing research.

Robert Feldt is professor of Software Engineering at Blekinge Institute of Technology in Karlskrona, Sweden and (part-time) also at Chalmers University in Gothenburg, Sweden. His research is focused on empirical software engineering (SE) research in software testing, automated SE, behavioural SE / human aspects, applying information theory in SE, as well as on requirements engineering. Most of his research is conducted in close collaboration with European and Asian software companies. He is a member of the ICST Steering Committee and passionate about taking testing and SE research into practice.

http://www.robertfeldt.net/

http://www.robertfeldt.net/publications/index.html

Prof. Aldo Gangemi (CNR-ISTC Rome)

Period: March 15, 2016 – March 16, 2016
Hosted by: Livio ROBALDO
Reason: Gave seminar titled "Introduction to Pattern-based Ontology Design and Knowledge Extraction from Legal Text", organised by Livio Robaldo.

Prof. Aldo Gangemi (CNR-ISTC Rome)

Period: Jan. 6, 2016 – Jan. 8, 2016
Hosted by: Leon VAN DER TORRE

Prof. Dr. Mario Gerla (University of California)

Period: Nov. 18, 2016
Hosted by: Thomas ENGEL, Raphaël FRANK, Ridha SOUA
Reason: Member of a PhD defense committee and discussion of further research collaboration with SECAN-Lab team.

Dr. Gabriela Gheorghe (PwC Luxembourg)

Period: Dec. 12, 2016 – Dec. 13, 2016
Hosted by: Thomas ENGEL
Reason: SECAN-Lab meeting

Dr. Alessandra Gorla (IMDEA Software Institute, Spain)

Period: April 26, 2016
Hosted by: Lionel BRIAND
Reason: Research Seminar: "Automatic Generation of Oracles for Exceptional Behaviors"

Abstract: Test suites should test exceptional behavior to detect faults in error-handling code. However, manually-written test suites tend to neglect exceptional behavior. Automatically-generated test suites, on the other hand, lack test oracles that verify whether runtime exceptions are the expected behavior of the code under test.

In this talk I will present a technique that automatically creates test oracles for exceptional behaviors from Javadoc comments. The technique uses a combination of natural language processing and program analysis. Our implementation, Toradocu, can be combined with a test input generation tool. Our experimental evaluation shows that Toradocu improves the fault-finding effectiveness of automatically-generated test suites, while at the same time it reduces the number of false positives.

This is a joint work with Alberto Goffi, Michael D. Ernst and Mauro Pezzè and will be presented at ISSTA 2016.

Alessandra Gorla received her Bachelor's and Master's degrees in computer science from the University of Milano-Bicocca in Italy. She completed her Ph.D. in informatics at the Università della Svizzera Italiana in Lugano, Switzerland in 2011. In her Ph.D. thesis she defined and developed the notion of Automatic Workarounds, a self-healing technique to recover Web applications from field

failures, a work for which she received the Fritz Kutter Award for the best industry related Ph.D. thesis in computer science in Switzerland.

Before joining IMDEA Software Institute in December 2014, she has been a postdoctoral researcher in the software engineering group at Saarland University in Germany. During her postdoc, she has also been a visiting researcher at Google in Mountain View.

More information

A-Prof. Dr. Jérôme Härri (EURECOM)

Period: Nov. 18, 2016
Hosted by: Thomas ENGEL, Raphaël FRANK
Reason: Member of a PhD defense committee.

Dr. Frank Hermann (Carmeq GmbH)

Period: Aug. 29, 2016
Hosted by: Thomas ENGEL
Reason: Supervision of Phd student

Dr. Frank Hermann (Carmeq GmbH)

Period: Dec. 2, 2016
Hosted by: Thomas ENGEL
Reason: Member of a PhD defense committee.

Dr. Frank Hermann (Carmeq GmbH)

Period: May 9, 2016
Hosted by: Thomas ENGEL
Reason: Supervision of Phd student

Dr. Frank Hermann (Carmeq GmbH)

Period: Aug. 29, 2016
Hosted by: Thomas ENGEL
Reason: Member of a PhD defense committee.

Jesse Heyninck

Period: July 12, 2016 – July 15, 2016
Hosted by: Leon VAN DER TORRE

Dr. Mathias Humbert (CISPA, Germany)

Period: Nov. 22, 2016 – Nov. 23, 2016
Hosted by: Jun PANG

Eirini Kalogeiton (University of Bern)

Period: May 12, 2016 – May 13, 2016
Hosted by: Thomas ENGEL, Maria Rita PALATTELLA
Reason: Kick off research project meeting

Dr. Christian Köbel (Honda r&d Europe GmbH)

Period: Dec. 15, 2016
Hosted by: Florian ADAMSKY, Thomas ENGEL
Reason: To get in touch with reserahers in SECAN-Lab group and future collaboration between SECAN-Lab group and Honda r&d Europe GmbH.

Prof. Dr. Barbara König (University of Duisburg-Essen)

Period: May 9, 2016
Hosted by: Thomas ENGEL
Reason: Supervision of Phd student

Prof. Dr. Barbara König (University of Duisburg-Essen)

Period: Aug. 29, 2016
Hosted by: Thomas ENGEL
Reason: Member of a PhD defense committee.

Dr. Nikolai Kosmatov (Software Safety Lab of CEA LIST, France)

Period: Feb. 11, 2016
Hosted by: Lionel BRIAND
Reason: SnT Research Seminar "Combinations of Static and Dynamic Analyses in Frama-C: An Overview"

Abstract: Initially considered as orthogonal research fields, static and dynamic analysis techniques have been for a long time used separately to improve the quality of software. However, the development of both approaches has led to the discovery of common issues and to the realization of potential synergies. The present talk gives an overview of some of the

combinations between static and dynamic verification approaches that were realized in the context of Frama-C, a framework for static and dynamic analysis of C programs developed at CEA LIST.

First, we illustrate how static analysis can be used to help test generation. The SANTE tool takes advantage of abstract interpretation and program slicing in order to achieve more precise detection of runtime errors. These ideas have been pushed further in the LTest tool in order to optimize automatic test generation for a large class of coverage criteria, through the detection of infeasible test objectives.

Second, we illustrate how test generation can in turn help static analysis. We explore in the StaDy tool how program proof and test generation can be combined in order to help the validation engineer to understand and to fix proof failures during deductive verification of programs.

Finally, we show how runtime verification can take benefit of static analysis in order to avoid the monitoring of irrelevant variables and statements (E-ACSL tool).

Nikolai Kosmatov works as a researcher at the Software Safety Lab of CEA LIST, one of the biggest research centers in France. Nikolai obtained M.Sc. degree in Mathematics at Saint-Petersburg State University in 1997, and Ph.D. in Mathematics jointly at Saint-Petersburg State University and the University of Be-

sançon in 2001. After receiving M.Sc. degree in Computer Science at the University of Besançon in 2003, Nikolai's research interests have focused on software testing, constraint solving and combinations of various software verification techniques. He is the main author of the online testing service pathcrawler-online.com. He co-organized tutorials on software testing, deductive verification and runtime assertion checking at several international events (TAP 2012, TAROT 2012, ASE 2012, QSIC 2012, TAP 2013, iFM 2013, SAC 2013, RV 2013, TAP 2014), and teaches software verification in several French universities.

Katsiaryna Labunets (University of Trento)

Period: April 5, 2016 – April 6, 2016
Hosted by: Olga GADYATSKAYA

Philippe Lalanda (University Joseph Fourier (Grenoble))

Period: Sept. 22, 2016
Hosted by: Denis ZAMPUNIERIS
Reason: Prof. Lalanda took part in the CET meeting for PhD candidate M. Gilles Neyens

Dr. Aleksandr Lenin (Cybernetica, Estonia)

Period: Sept. 27, 2016 – Sept. 29, 2016
Hosted by: Olga GADYATSKAYA, Rolando TRUJILLO RASUA

Bing Li (Nanjing University, China)

Period: Nov. 24, 2016 – Nov. 4, 2016
Hosted by: Jun PANG

Dr. Cheng-Te Li (Academia Sinica, Taiwan)

Period: May 23, 2016 – July 1, 2016
Hosted by: Andrzej MIZERA, Jun PANG

Dr. Yongjian Li (Chinese Academy of Sciences)

Period: Jan. 18, 2016 – Jan. 13, 2016
Hosted by: Jun PANG

Dr. Roderick McCall (Luxembourg Institute of Science and Technology (LIST))

Period: Dec. 12, 2016 – Dec. 13, 2016
Hosted by: Thomas ENGEL
Reason: SECAN-Lab meeting

Dr. Roderick McCall (Luxembourg Institute of Science and Technology (LIST))

Period: April 22, 2016
Hosted by: Thomas ENGEL
Reason: Member of a PhD defense committee.

Dr. Tim Muller (University of Oxford)

Period: July 19, 2016
Hosted by: Sjouke MAUW

Gillman Payette

Period: May 9, 2016 – May 12, 2016
Hosted by: Leon VAN DER TORRE

Gabriella Pigozzi

Period: March 8, 2016 – March 9, 2016
Hosted by: Leon VAN DER TORRE

Dr. Hongyang Qu (Sheeld University)

Period: March 21, 2016 – March 25, 2016
Hosted by: Jun PANG

Dr. Saša Radomirović (ETH Zurich)

Period: May 23, 2016 – May 25, 2016
Hosted by: Sjouke MAUW

Prof. John Regehr (University of Utah)

Period: Feb. 9, 2016
Hosted by: Lionel BRIAND
Reason: SnT Research Seminar "Blurring the Line Between Testing and Verification"

Abstract: Sound static analysis of C code is difficult. This talk explores using a C verifier as an interpreter, sacrificing soundness but eliminating overapproximation-related bugs. This mode of analysis works best for systems that have very thorough test suites, whether manually constructed or generated by a tool such as afl-fuzz. Using Frama-C as an interpreter we have analyzed widely-used, security-critical libraries such as SQLite, libpng, and libwebp, find a number of issues in each and also paving the way for future sound verification efforts.

Professor Regehr received his PhD in 2001 from the University of Virginia. He is currently a professor of computer science at the University of Utah, where he has been on the faculty since 2003. His research is on compilers, software testing, and software verification.

Dr. Gianluca Rizzo (University of Applied Sciences Western Switzerland (HES-SO))
Period: May 12, 2016 – May 13, 2016
Hosted by: Thomas ENGEL, Maria Rita PALATTELLA
Reason: Kick off research project meeting

Dr. Raimondas Sasnauskas (SES Engineering)
Period: Dec. 2, 2016
Hosted by: Thomas ENGEL
Reason: Member of a PhD defense committee.

Dr. Raimondas Sasnauskas (SES Engineering)
Period: May 9, 2016
Hosted by: Thomas ENGEL
Reason: Supervision of Phd student

Dr. Raimondas Sasnauskas (SES Engineering)
Period: Aug. 29, 2016
Hosted by: Thomas ENGEL
Reason: Member of a PhD defense committee.

Dr. Raimondas Sasnauskas (SES Engineering)
Period: Aug. 29, 2016
Hosted by: Thomas ENGEL
Reason: Supervision of Phd student

Alain Schumacher (SICAP Luxembourg)
Period: Dec. 12, 2016 – Dec. 13, 2016
Hosted by: Thomas ENGEL
Reason: SECAN-Lab meeting

A-Prof. Dr.-Ing. Christoph Sommer (University of Paderborn)
Period: Nov. 18, 2016
Hosted by: Thomas ENGEL, Raphaël FRANK
Reason: Member of a PhD defense committee.

Prof. Dr. Otto Spaniol (RWTH Aachen University)
Period: Dec. 12, 2016 – Dec. 13, 2016
Hosted by: Thomas ENGEL
Reason: Secan-Lab meeting

Thomas Studer
Period: March 21, 2016 – March 23, 2016
Hosted by: Leon VAN DER TORRE

Dr. Alexandru Tantar (Black Swan Luxembourg)
Period: Dec. 12, 2016 – Dec. 13, 2016
Hosted by: Thomas ENGEL
Reason: SECAN-Lab meeting

Dr. Emilia Tantar (Black Swan Luxembourg)
Period: Dec. 12, 2016 – Dec. 13, 2016
Hosted by: Thomas ENGEL
Reason: SECAN-Lab meeting

Dr. Marc van Opijnen
Period: April 11, 2016 – April 12, 2016
Hosted by: Livio ROBALDO
Reason: Gave seminar titled "Publishing court decisions on the internet: legal and technical developments", organized by Livio Robaldo.

Srdjan Vesic
Period: Nov. 23, 2016 – Nov. 25, 2016
Hosted by: Leon VAN DER TORRE

Srdjan Vesic
Period: March 8, 2016 – March 10, 2016
Hosted by: Leon VAN DER TORRE

Dr. Gérard Wagener (Computer Incident Response Center Luxembourg (CIRCL))
Period: Dec. 12, 2016 – Dec. 13, 2016
Hosted by: Thomas ENGEL
Reason: SECAN-Lab meeting

Dr. Steffan Walz (MIT University Melbourne)
Period: April 22, 2016
Hosted by: Thomas ENGEL
Reason: Member of a PhD defense committee.

C.6 Visits

The following visits by CSC members to external organisations took place:

Diego Agustin AMBROSSIO
Institution: KU Leuven
Location: Leuven, Belgium
Period: March 21, 2016 – March 22, 2016.
Reason: SIEP Project Meeting:
Presentation of on- going work and discussion of the proposed Decision Proce-

dure details.

Alfredo CAPOZUCCA

Institution: Peter the Great St.Petersburg Polytechnic University
Location: St.Petersburg, Russia
Period: Sept. 19, 2016 – Sept. 30, 2016.
Reason: Invited Professor - Course responsible at Bachelor and Master levels

Alfredo CAPOZUCCA

Institution: Peter the Great St.Petersburg Polytechnic University
Location: St.Petersburg, Russia
Period: Nov. 28, 2016 – Dec. 9, 2016.
Reason: Invited Professor - Course responsible at Bachelor and Master levels

Giovanni CASINI

Institution: University of Cape Town
Location: Cape Town, South Africa
Period: April 24, 2016 – May 8, 2016.

Giovanni CASINI

Institution: ISTI - CNR
Location: Pisa, Italy
Period: Oct. 4, 2016 – Oct. 11, 2016.

Giovanni CASINI

Institution: ISTI - CNR
Location: Pisa, Italy
Period: Dec. 16, 2016 – Dec. 29, 2016.

Afonso DELERUE ARRIAGA

Institution: FCUL
Location: Lisbon, Portugal
Period: April 14, 2016.
Reason: Invited lecture ”Searchable encryption schemes” - Strategic partnership in Information Security (ParIS - ISP) - http://paris-isp.campus.ciencias.ulisboa.pt/home

Dragan DODER

Institution: IRIT
Location: Toulouse, France
Period: March 29, 2016 – April 1, 2016.

Olga GADYATSKAYA
Institution: NTU and SUTD
Location: Singapore, Singapore
Period: Feb. 28, 2016 – March 5, 2016.

Nicolas GUELFI
Institution: Peter the Great St.Petersburg Polytechnic University
Location: St.Petersburg, Russia
Period: Sept. 5, 2016 – Sept. 16, 2016.
Reason: Invited Professor - Course responsible at Bachelor and Master levels

Nicolas GUELFI
Institution: Peter the Great St.Petersburg Polytechnic University
Location: St.Petersburg, Russia
Period: Dec. 12, 2016 – Dec. 23, 2016.
Reason: Invited Professor - Course responsible at Bachelor and Master levels

Ravi JHAWAR
Institution: NTU and SUTD
Location: Singapore, Singapore
Period: Feb. 28, 2016 – March 5, 2016.

Ravi JHAWAR
Institution: Sintef
Location: Trondheim, Norway
Period: May 2, 2016 – May 6, 2016.

Pierre KELSEN
Institution: University of Lisbon
Location: Lisbon, Portugal
Period: April 14, 2016 – April 15, 2016.
Reason: Pierre Kelsen visited University of Lisbon for a consortium meeting of Erasmus+ project PARIS from April 14 to April 15.

Gabriele LENZINI
Institution: Friedrich-Alexander-Universität Erlangen-Nürnberg
Location: Nürnberg, Germany
Period: July 2, 2016 – July 7, 2016.
Reason: Research visit

Qin MA
Institution: Research Group of Information Systems and Enterprise Modelling, University of Duisburg-Essen
Location: Duisburg, Germany
Period: April 11, 2016 – April 14, 2016.

Sjouke MAUW
Institution: TU Denmark
Location: Lyngby, Denmark
Period: Jan. 13, 2016 – Jan. 15, 2016.

Sjouke MAUW
Institution: TU Darmstadt
Location: Darmstadt, Germany
Period: Feb. 24, 2016.

Sjouke MAUW
Institution: NTU and SUTD
Location: Singapore, Singapore
Period: Feb. 28, 2016 – March 20, 2016.

Sjouke MAUW
Institution: Sintef
Location: Trondheim, Norway
Period: April 2, 2016 – April 5, 2016.

Sjouke MAUW
Institution: University Lisbon
Location: Lisbon, Portugal
Period: April 13, 2016 – April 15, 2016.

Sjouke MAUW
Institution: University of Amsterdam
Location: Amsterdam, Netherlands
Period: Dec. 13, 2016 – Dec. 14, 2016.

Andrzej MIZERA
Institution: Abo Akademi University
Location: Turku, Finland
Period: Feb. 8, 2016 – Feb. 19, 2016.

Andrzej MIZERA
Institution: Biomedical Informatics Graduate Lab, NTU
Location: Singapore, Singapore
Period: March 1, 2016.

Andrzej MIZERA
Institution: NTU
Location: Singapore, Singapore
Period: March 2, 2016 – March 3, 2016.

Andrzej MIZERA
Institution: Saarland University
Location: Saarbrücken, Germany
Period: Nov. 15, 2016.

Surena NESHVAD
Institution: Forschungszenter Jülich
Location: Jülich, Germany
Period: Dec. 1, 2016 – Dec. 3, 2016.
Reason: Energy Economy Seminar

David NORTA
Institution: Forschungszenter Jülich
Location: Jülich, Germany
Period: Dec. 1, 2016 – Dec. 3, 2016.
Reason: Energy Economy Seminar

Andriy PANCHENKO
Institution: RWTH Aachen University
Location: Aachen, Germany
Period: July 18, 2016.
Reason: Dr. Andriy Panchenko visited the chair for communication and distributed systems (COMSYS) as invited speaker in a workshop on censorship in the Internet and participated the follow-up research discussion on this topic.

Jun PANG
Institution: Middlesex University
Location: Hendon, United Kingdom
Period: Feb. 17, 2016 – Feb. 18, 2016.

Jun PANG
Institution: NTU and SUTD
Location: Singapore, Singapore
Period: Feb. 28, 2016 – March 20, 2016.

Jun PANG
Institution: Nanjing University
Location: Nanjing, China
Period: July 26, 2016 – July 28, 2016.

Jun PANG

Institution: Institute of Software, Chinese Academy of Sciences
Location: Beijing, China
Period: Aug. 15, 2016 – Aug. 18, 2016.

Valentin PLUGARU

Institution: ACK Cyfronet AGH, University of Science and Technology
Location: Krakow, Poland
Period: March 10, 2016.
Reason: Visit of Poland's supercomputing facility at Cyfronet, Krakow: Prometheus supercomputer (#38 in the world).

The meetings comprised discussions on advanced computing facility deployment and installation, the introduction of the UL HPC center and discusion of possible collaborations.

Andrei POPLETEEV

Institution: Belarusian State University
Location: Minsk, Belarus
Period: June 20, 2016 – July 1, 2016.
Reason: Dr. Andrei Popleteev visited Belarusian State University (Belarus) to establish research collaboration in the field of indoor positioning and data analytics.

Benoit RIES

Institution: Peter the Great St.Petersburg Polytechnic University
Location: St.Petersburg, Russia
Period: Oct. 3, 2016 – Oct. 14, 2016.
Reason: Invited Professor - Course responsible at Bachelor and Master levels

Benoit RIES

Institution: Peter the Great St.Petersburg Polytechnic University
Location: St.Petersburg, Russia
Period: Nov. 14, 2016 – Nov. 25, 2016.
Reason: Invited Professor - Course responsible at Bachelor and Master levels

Livio ROBALDO

Institution: Stanford University
Location: Stanford, California, United States of America
Period: June 14, 2016 – June 25, 2016.
Reason: Livio Robaldo visited Stanford University to work with Cleo Condoravdi towards the objective of the MIREL project (http://www.mirelproject.eu/), whose activities he is coordinating together with Leon van der Torre, Giovanni Casini, and Xavier Parent.

Peter ROENNE
Institution: IT University of Copenhagen
Location: Copenhagen, Denmark
Period: Aug. 8, 2016.
Reason: Talk and collaboration.

Peter ROENNE
Institution: Horizon 2020 brokerage
Location: Paris, France
Period: Sept. 5, 2016.
Reason: Presentation of university of Luxembourg.

Peter Y. A. RYAN
Institution: University of Surrey
Location: Surrey, United Kingdom
Period: Nov. 30, 2015 – Jan. 17, 2016.

Peter Y. A. RYAN
Institution: University of Oxford
Location: Oxford, United Kingdom
Period: Jan. 31, 2016 – March 19, 2016.

Juergen SACHAU
Institution: Forschungszenter Jülich
Location: Jülich, Germany
Period: Dec. 1, 2016 – Dec. 3, 2016.
Reason: Energy Economy Seminar

Christoph SCHOMMER
Institution: University of Cologne
Location: Cologne, Germany
Period: Jan. 28, 2016.
Reason: Invited Guest Lecture

Christoph SCHOMMER
Institution: Tsinghua University
Location: Beijing, China
Period: June 25, 2016 – July 10, 2016.
Reason: Teaching "Data Science" at Tsinghua University

Mandatory course for somophores (35 students); 36 h course including exercises, homeworks, and 2 examinations.

Rolando TRUJILLO RASUA
Institution: University of Rennes
Location: Rennes, France
Period: May 8, 2016 – May 19, 2016.

Rolando TRUJILLO RASUA
Institution: Universitat Rovira i Virgili
Location: Tarragona, Spain
Period: Sept. 28, 2016 – Sept. 30, 2016.

Marc VAN ZEE
Institution: Google
Location: Pittsburgh, PA, United States of America
Period: May 15, 2016 – Aug. 19, 2016.
Reason: PhD internship

Appendix D

Software Developments

ADTool

http://satoss.uni.lu/software/adtool

License: free use *Members:* Piotr KORDY (Developer), Sjouke MAUW (Analyst)

Description: The attack–defense tree language formalizes and extends the attack tree formalism. It is a methodology to graphically analyze security aspects of scenarios. With the help of attributes on attack–defense trees, also quantitative analysis can be performed. As attack–defense tree models grow, they soon become intractable to be analyzed by hand. Hence computer support is desirable. Software toll, called the ADTool, has been implemented as a part of the ATREES project to support the attack–defense tree methodology for security modeling. The main features of the ADTool are easy creation, efficient editing, and quantitative analysis of attack–defense trees. The tool is available at http://satoss.uni.lu/software/adtool. The tool was realized by Piotr Kordy and its manual was written by Patrick Schweitzer.

Changes: In 2016 we picked up the ADTool development again in order to improve its functionality (e.g., by including the sequential-AND operator, ranking, copy paste) and to integrate it into the TREsPASS project process. Later development development of library of trees is planned. Piotr Kordy has again joined SaToSS to work on the ADTool in December 2015 (until June 2017).

Algorithms for Probabilistic Argumentation

License: Creative Common *Members:* Leon VAN DER TORRE (Architect)

Description: We developed efficient algorithms for computing probabilistic

argumentation. These algorithms were implemented in Java, and tested on a machine with an Intel CPU running at 2.26 GHz and 2.00 GB RAM. Please refer to the following paper in details.

1. Beishui Liao, Kang Xu, Huaxin Huang. Formulating Semantics of Probabilistic Argumentation by Characterizing Subgraphs: Theory and Empirical Results, Jurnal of Logic and Computation, to appear. http://arxiv.org/abs/1608.00302

ASSA-PBN

http://satoss.uni.lu/software/ASSA-PBN/

License: free use *Members:* Jun PANG (Analyst)

Description: ASSA-PBN is a tool specially designed for approximate steady-state analysis of large probabilistic Boolean networks (PBNs). The approximate steady-state analysis is crucial for large PBNs, which naturally arise in the domain of Systems Biology. ASSA-PBN provides different solutions for different size PBNs. In particular, ASSA-PBN provides the two-state Markov chain approach and the Skart approach for large PBNs. The latest version of the package was released in Nov. 2014 and is available from http://satoss.uni.lu/software/ASSA-PBN/.

bagit

http://demos.uni.lux/bagit

License: non-redistributable, for internal use only *Members:* Christian GLODT (Designer, Developer, Tester)

Description: An internal web-based tool that provides assistance to research groups by storing, pooling, tagging and indexing papers and other publications.

Baumüller ProMaster

License: UL *Members:* Surena NESHVAD (Developer), Marco NEY (Developer), David NORTA (Developer)

Description: Baumüller ProMaster is the software to operate the inverter and electrical machines in the lab.

BlueScanner

License: MIT *Members:* Walter BRONZI (Developer)

Description: The scope of the application is to collect Bluetooth beacons whilst in a driving scenario and send them to a server. In this context was performed a 2-month collection campaign within SnT. More than 20 participants where collected for this stage.

CollaTrEx

License: N/A *Members:* Jean BOTEV (Architect)

Description: CollaTrEx is framework for collaborative context-aware mobile exploration and training. It is particularly designed for the in-situ collaboration within groups of learners performing together diverse educational activities to explore their environment in a fun and intuitive way.

Aside from employing both absolute and relative spatio-temporal context for determining the available activities, different buffering levels are an important conceptual feature supporting seamless collaboration in spite of temporary connection losses or when in remote areas.

CollaTrEx comprises a prototypical front-end implementation for tablet devices, as well as a web-based back-end solution for the creation and management of activities which can be easily extended to accommodate both future technologies and novel activity types.

CSC Information System

http://demos.uni.lux/csc

License: Internal use only *Members:* Bertrand DESSART (Analyst, Architect), Christian GLODT (Analyst, Architect, Designer, Developer, Tester)

Description: The CSC Information System is a web-based interface for the management of information related to the CSC, such as research projects, research areas, research groups, and many other elements related to the CSC and its member's activities. The CSC Information System is built using the Django Framework.

Data acquisition platform

License: MIT *Members:* Andrei POPLETEEV (Developer)

Description: The INDOORS project has created an open-source data acquisition platform (DAQ), which is designed to facilitate data collection for indoor localization experiments. The DAQ platform allows recording of raw radio signal samples from multiple bands simultaneously with ground-truth location and environment state (weather and crowd dynamics) metadata. The platform employs an Ettus Research USRP B210 software-defined radio to collect short raw samples of FM, GSM downlink, Wi-Fi and several active DVB-T channels. Ground truth location is specified manually by the operator by selecting one of the predefined reference points on an interactive map; the detailed weather information, in turn, is automatically fetched from an online service. By collecting raw radio-frequency (RF) signal samples from a software-defined radio receiver, this tool separates data acquisition from the extraction of location-dependent signal features, thus offering unprecedented flexibility for the evaluation of classic and novel localization methods (potentially including those yet to be devised).

Changes: The data acquisition platform has been published as open source software (via this publication http://ieeexplore.ieee.org/document/7822838/).

Democles

http://democles.lassy.uni.lu/

License: Freely redistributable, see details at: http://democles.lassy.uni.lu/license.html *Members:* Christian GLODT (Architect, Designer, Developer, Tester)

Description: Democles is a modeling tool that supports the EP language developed by LASSYs MDE group. It is mainly developed by Christian Glodt.

Digraph3

http://leopold-loewenhein.uni.lu/docDigraph3

License: GNU General Public License v.2+ *Members:* Raymond Joseph BISDORFF (Developer)

Description: Digraph3 is a collection of Python3 modules and resources for implementing decision aiding algorithms for selecting, ranking, sorting or rating, and clustering with multiple incommensurable criteria. These computing resources are useful in the field of Algorithmic Decision Theory and more specifically in outranking based multiple criteria decision aiding.

ELRA Language Corpus

License: LC/ELDA/DISTR-S/2014-11/001-UNILU *Members:* Sviatlana HÖHN (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

License: Eclipse Public License 1.0 *Members:* Alfredo CAPOZUCCA (Developer), Nicolas GUELFI (Developer), Benoit RIES (Developer)

Description: Excalibur is a tool supporting the Messir methodology, a Scientific Method for the Software Engineering Master, used in Software Engineering Lectures at bachelor and master levels.

Excalibur tool covers the phase of Requirements Analysis and its main features are requirements analysis specification (its own DSL), requirements report generation (latex/pdf) and requirements simulation (prolog). It relies on Eclipse technologies as XText for textual specification and Sirius for graphical views of the textual specifications.

It is available here: http://messir.uni.lu

Changes:

- Excalibur v1.5 for BINFO semester 4 students.
  - http://messir.uni.lu:8085/jira/browse/EX/fixforversion/11902
- Excalibur v1.6 for BINFO semester 3 students, lifelong learning students and for Peter the Great Polytechnic University bachelor and master students

– http://messir.uni.lu:8085/jira/browse/EX/fixforversion/11600

GreenCloud Simulator

https://greencloud.gforge.uni.lu/

License: Open source *Members:* Claudio FIANDRINO (Developer), Mateusz GUZEK (Architect), Dzmitry KLIAZOVICH (Architect)

Description: Greencloud is a sophisticated packet-level simulator for energy-aware cloud computing data centers with a focus on cloud communications. It offers a detailed fine-grained modeling of the energy consumed by the data center IT equipment, such as computing servers, network switches, and communication links.

IDP

http://icr.uni.lu/mcramer/index.php?id=3

License: Public *Members:* Diego Agustin AMBROSSIO (Tester), Marcos CRAMER (Tester)

Description: implementation of revocation schemes according to the classification proposed by Hagström et al. (2001)

Changes: IDP specification of Hagström et al.'s (2001) delegation revocation framework, together with various inferences on it that solve different tasks. URL: http://icr.uni.lu/mcramer/downloads/hagstrom-RDS.zip

Lightning

http://lightning.gforge.uni.lu/

License: binary only, freely redistributable without modification *Members:* Loïc GAMMAITONI (Analyst, Architect, Designer, Developer, Tester), Christian GLODT (Architect, Designer, Developer, Tester)

Description: Lightning is a lightweight language workbench based on Alloy and Eclipse.

Lightning allows the definition of Languages via the specification of Alloy models, thus allowing the lightweight analysis of its components.

The focus of Lightning is to provide support to language engineers to efficiently design their DSLs.

LuST-LTE

License: MIT *Members:* Thierry DERRMANN (Developer)

Description: A Simulation Package for Pervasive Vehicular Connectivity.

LuST-LTE is a package of open-source simulation tools that allows the simulation of vehicular traffic along with pervasive LTE connectivity. Most importantly, LuST-LTE provides handover functionality and adds LTE infrastructure of a mobile network operator to the LuST road traffic simulation scenario of Luxembourg City.

Luxembourg SUMO Traffic (LuST) Scenario

https://github.com/lcodeca/LuSTScenario

License: MIT *Members:* Lara CODECA (Developer)

Description: The community needs a scenario with the following requirements:

- It has to be able to support different kinds of traffic demand such as congested or free-flow patterns.
- It should support different scenario dimensions.
- It has to include different road categories (e.g. residential, arterial and highway).
- It should allow multi-modal evaluations.
- Is should describe a realistic traffic scenario over one day (i.e. avoid gridlocks and teleportations).

LuST is used for:

- Evaluation of different multi-modal strategies for commuters
- Testing protocols and applications on different scales
- On-board routing system to provide scenarios with different levels of congestion to test different re-routing algorithms.
- Test optimisation algorithms for
  - main arterial road (e.g. green waves)
  - emergency protocols (e.g. allow emergency vehicles to be prioritised)

Changes: The Luxembourg SUMO Traffic (LuST) Scenario 2.0 has been released at the end of October. The new version provides multiple mobility traces, different traffic light systems, and various improvement in the network topology. LuST Scenario 2.0 is freely available under the MIT license to the whole community and in now featured in the Official SUMO Wiki. A complete evaluation and

validation of the mobility scenario has been accepted for publication in IEEE Intelligent Transposition System Magazine and it will be published in 2017.

MaRCo Model Editor

http://marco.gforge.uni.lu/tools.html

License: binary only, freely redistributable without modification *Members:* Christian GLODT (Architect, Designer, Developer, Tester)

Description: The MaRCo Model Editor is an Eclipse plugin that provides functionality for creating and editing XBPNM and Policy models, as well as transformation capabilities allowing to generate an Alloy representation of an XBPNM model.

MDPRevision

https://github.com/marcvanzee/mdp-plan-revision

License: Creative Commons *Members:* Marc VAN ZEE (Developer)

Description: Read a more detailed description of the conceptual underpinnings and experimental results in the following paper:

Intention Reconsideration as Metareasoning (Marc van Zee, Thomas Icard), In Bounded Optimality and Rational Metareasoning NIPS 2015 Workshop, 2015.

Summary: This project implements an agent that is situated on a Markov Decision Process (MDP). The agent is able to compute the optimal policy through Value Iteration. The MDP is changing over time, and the agent can respond to this change by either acting (i.e. executing the optimal action according to its current policy) or thinking (i.e. computing a new policy). The task is to learn the best meta-reasoning strategy, i.e. deciding when to think or act, based on the characteristics of the environment.

This general setup is quite complex, so we have simplified the environment (i.e. the MDP) to the TIleworld environment. This consists of an agent that is situated on a grid. It can move up, down, left, or right and has to fill holes, which means it has to reach specific states in the grid. It cannot move through obstacles.

We then develop several metareasoning strategies that the agent can use.

MiCS Management System

http://demos.uni.lux/mics

License: non-redistributable, for internal use only *Members:* Christian GLODT (Designer, Developer, Tester)

Description: An internal web-based tool developed for the management of modules, courses and profiles of the Master in Information and Computer Sciences. Developed by Christian Glodt.

MinUS

http://satoss.uni.lu/software/MinUS

License: free use *Members:* Jun PANG (Analyst)

Description: This tool, MinUS, integrates the technologies of trajectory pattern mining with the state-of-the art research on discovering user similarity with trajectory patterns. Specifically, with MinUS, we provide a platform to manage movement datasets, and construct and compare users trajectory patterns. Tool users can compare results given by a series of user similarity metrics, which allows them to learn the importance and limitations of different similarity metrics and promotes studies in related areas, e.g., location privacy. Additionally, MinUS can also be used by researchers as a tool for preliminary process of movement data and parameter tuning in trajectory pattern mining. The tool is available at http://satoss.uni.lu/software/MinUS.

Mobility Profiler

License: MIT *Members:* Sébastien FAYE (Developer)

Description: This profiler is able to estimate a user's mobility profile based on anonymized and lightweight smartphone data. In particular, this system is composed of (1) a web analytics platform, able to analyze multimodal sensing traces and improve our understanding of complex mobility patterns, and (2) a smartphone application, able to show a user's profile generated locally in the form of a spider graph. In particular, this system uses anonymized and privacy-friendly data and methods, obtained thanks to the combination of Wi-Fi traces, activity detection and graph theory, made available independent of any personal information.

Model Decomposer

http://democles.lassy.uni.lu/documentation/TR_LASSY_10_06.pdf

License: free to use, binary redistribution permitted *Members:* Christian GLODT (Architect, Developer), Qin MA (Analyst)

Description: An Eclipse plugin that implements a generic model decomposition technique which is applicable to Ecore instances and EP models, and is described in a paper published in the proceedings of the FASE 2011 conference.

PREXT

https://github.com/karim-emara/PREXT

License: GNU GPL *Members:* Karim Ahmed Awad El-Sayed EMARA (Developer)

Description: PREXT is a unified and extensible framework that simulate pseudonym change schemes (i.e. privacy schemes) in VANET. It supports seven privacy schemes of different approaches including silent period, context-based and mix-zone and can be easily extended to include more schemes. It includes adversary modules that can eavesdrop vehicle messages and track their movements. This adversary is used in measuring the gained privacy in terms of several popular metrics such as entropy, traceability and pseudonym usage statistics.

RationalGRL

https://github.com/RationalArchitecture/RationalGRL

License: Creative Common *Members:* Marc VAN ZEE (Developer)

Description: Goal modeling languages, such as i* and the Goal-oriented Requirements Language (GRL), capture and analyze high-level goals and their relationships with lower level goals and tasks. However, in such models, the rationalization behind these goals and tasks and the selection of alternatives are usually left implicit.Rationalization consists of arguments for and against certain goals and solutions, which allow checking whether a particular goal model is a correct rendering of the relevant stakeholders' opinions and discussions. To better integrate goal models and their rationalization, we develop the RationalGRL framework, in which argument diagrams can be mapped to goal models. Moreover, we integrate the result of the evaluation of arguments and

their counterarguments with GRL initial satisfaction values. We develop an interface between the argument web tools OVA and TOAST and the Eclipse-based tool for GRL called jUCMNav.

ROS face_recognition package

http://www.ros.org/wiki/face_recognition

License: Attribution-NonCommercial 3.0 *Members:* Pouyan ZIAFATI (Developer)

Description: Provides a ROS simple actionlib server interface for performing different face recognition functionalities in video stream.

SWIPE: Monitoring Human Dynamics using Smart Devices

https://github.com/sfaye/SWIPE/

License: MIT *Members:* Sébastien FAYE (Developer)

Description: SWIPE is a platform for sensing, recording and processing human dynamics using smart devices. The idea behind this type of system, which exists for the most part on smartphones, is to consider new metrics from wearables — in our case smartwatches. These new devices, used in parallel with traditional smartphones, provide clear indicators of the activities and movements performed by the users who wear them. They can also sense environmental data and interactions. The SWIPE architecture is structured around two main elements, namely (1) an Android application deployed directly on the devices, allowing them to synchronize and collect data; and (2) a server for storing and processing the data.

TESMA

License: Eclipse Public License 1.0 *Members:* Nicolas GUELFI (Analyst), Benjamin JAHIC (Developer), Sandro REIS (Developer), Benoit RIES (Analyst)

Description: Tool for the Specification, Management and Assessment of Teaching Programs.

Nicolas Guelfi, Benjamin Jahic and Benoît Ries, TESMA: Towards the Development of a Tool for Specification, Management and Assessment of Teaching Programs, published in the Proceedings of the 2nd International Conference on Applications in Information Technology (ICAIT-2016)

http://orbilu.uni.lu/handle/10993/28607

Changes: Initial version of the software comprising

- a textual domain-specific language allowing to specify teaching programs and their related compliance with educational standards for the purpose of accreditation.
- a generator of moodle pages from the textual specifications

ULHPC-credits

https://gitlab.uni.lu/vplugaru/ulhpc-tools

License: GPLv3 *Members:* Valentin PLUGARU (Designer)

ULHPC-platform-usage

License: GPLv3 *Members:* Valentin PLUGARU (Designer)

Description: Tool used on the UL HPC platform (Gaia/Chaos clusters: 'ulhpc_platform_usage') to monitor per-user resource utilization, with configurable email alerting.

Combined with the ULHPC-credits tool, it allows for a more comprehensive understanding of platform utilization.

Visual Contract Builder

http://vcl.gforge.uni.lu/

License: free to use, binary redistribution permitted *Members:* Christian GLODT (Architect, Designer, Developer)

Description: A suite of Eclipse plugins that provide support for graphically editing and typechecking VCL (Visual Contract Language) diagrams.

Web-based itinerary planner for Luxembourg

http://sfaye.com/vehicularlab/OTP.zip

License: MIT *Members:* Sébastien FAYE (Developer)

Description: The first prototype allows users to plan trips using several intermediate location points. In particular, users can choose between different modes of transport or a combination of several modes, including those with time-dependent availability (i.e. bike-sharing). The system automatically computes interesting trips and suggested the best ones to the user. Current modes of transportation include car, bicycle, Veloh, public transport and walking.

WFP toolbox

License: TBA *Members:* Karim Ahmed Awad El-Sayed EMARA (Developer), Daniel FORSTER (Developer), Fabian LANZE (Developer), Asya MITSEVA (Developer), Andriy PANCHENKO (Developer)

Description: The website fingerprinting toolbox consists of multiple scripts and binaries that allow a user to carry out research related to the website fingerprinting attack. The toolbox enables a user to automate the visit of websites, record the traffic traces, clean the traffic traces from wrong instances, extract features from the traffic traces and finally train a machine learning classifier.

Changes: During the research in scope of the Privacy Flag project, the website fingerprinting toolbox was improved to perform a live demonstration of website fingerprinting on Tor traffic. Thus, we showed the serious threat to online privacy of Tor users and the need for further research in this direction. Furthermore, we started extending the tool to collect traffic information not only for regular web browsing via the Tor network, but also for accessing resources in the dark web (hidden services).

XDEM (eXtended Discrete Element Method)

http://luxdem.uni.lu/

License: Internal use only *Members:* Bernhard PETERS (Developer), Alban ROUSSET (Developer), Sébastien VARRETTE (Developer)

Description: The eXtended Discrete Element Method (XDEM), formerly Discrete Particle Method (DPM), is an advanced numerical simulation tool which deals with both motion and chemical conversion of particulate material such as coal or biomass in furnaces. However, predictions of solely motion or con-

version in a de-coupled mode are also applicable. The Discrete Particle Method uses object oriented techniques that support objects representing three-dimensional particles of various shapes such as cylinders, discs or tetrahedrons for example, size and material properties. This makes it a highly versatile tool dealing with a large variety of different industrial applications of granular matter. A user interface allows easily extending the software further by adding user-defined models or material properties to an already available selection of materials, properties and reaction systems describing conversion. Thus, the user is relieved of underlying mathematics or software design, and therefore, is able to direct his focus entirely on the application. The Discrete Particle Method is organised in a hierarchical structure of C++ classes and works both in Linux and XP environments also on multi-processor machines. This software is developed by the XDEM research team, led by Prof. Bernhard Peters from the Research Unit in Engineering Science (RUES) in collaboration with the Computer Science and Communications (CSC) research unit.

Changes: The parallel implementation with MPI is working and is now being used by the all LuXDEM to speedup their simulation on the cluster. New approaches to improvement the performance of parallel executions are being investigated as part of the LSDEM project:

- OpenMP parallelization, in order to target hybrid execution OpenMP/MPI
- Better load-balancing using external libraries: Zoltan (RIB, RCB, PhG), parMETIS and SCOTCH
- Support for parallel execution for coupled simulation XDEM-OpenFOAM
- Automated scripts for performance profiling of XDEM

Additionally, XDEM has being used as a realistic benchmarking application for Cloud Computing performance and cost evaluation in [142].

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	61.8
Research Associate (Post-doc)	43.37
Professor	14.97
Research Scientist	13.01
Research Associate	8.56
Administrative Aid	7.09
Associate Professor	5.98
Technical Support Staff Member	3.99
Senior Lecturer	3
Technician on Project	1.53
Scientific Support Staff Member	1
Vice-President	1
Student with Limited Contract	0.38
Intern	0.29
Total	*165.96*

Table E.1: Number of Staff by Category

E.2 Distribution of Staff by Category

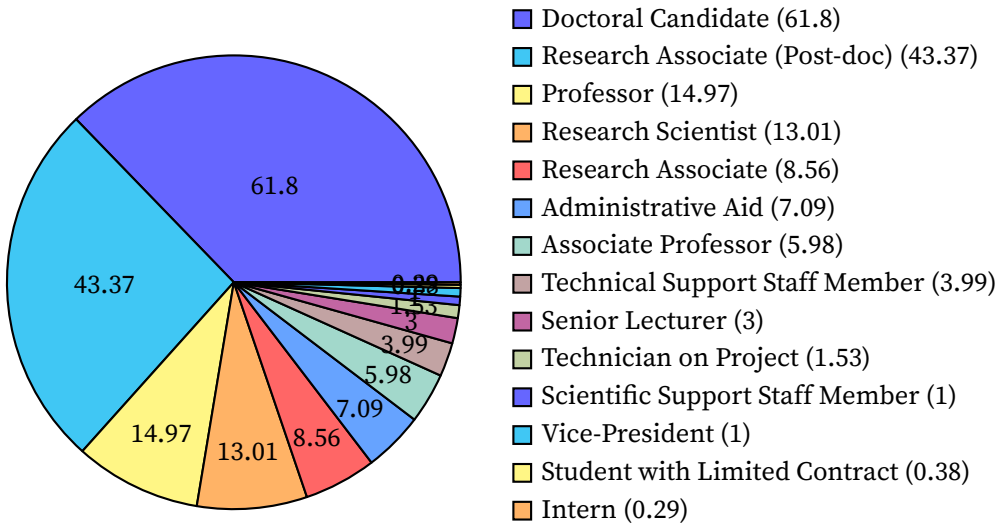


Figure E.1: Staff Distribution

E.3 List of Members by Category

Note: In the following list, staff members without an explicitly shown FTE number implicitly have an FTE number of 1.0.

Position	Last Name	First Name
Professor	BIRYUKOV	Alexei
	BISDORFF	Raymond Joseph
	BOUVRY	Pascal
	BRIAND	Lionel
	ENGEL	Thomas
	ESTEVES VERISSIMO	Paulo
	GUELFI	Nicolas
	KELSEN	Pierre
	LE TRAON	Yves
	MAUW	Sjouke
	RYAN	Peter Y. A.
	SACHAU	Juergen
	SORGER	Ulrich
	VAN DER TORRE	Leon
	ZAMPUNIERIS	Denis
Associate Professor	CORON	Jean-Sébastien
	MÜLLER	Volker

Position	Last Name	First Name
	NAVET	Nicolas
	ROTHKUGEL	Steffen
	SCHOMMER	Christoph
	STEENIS	Bernard
Vice-President	LEPREVOST	Franck
Research Associate (Post-doc)	ADAMSKY	Florian (0.33 FTE)
	ALTMEYER	Sebastian (0.16 FTE)
	APPELT	Dennis (0.83 FTE)
	ARORA	Chetan (0.16 FTE)
	BIANCULLI	Domenico (0.58 FTE)
	BISSYANDE	Tegawendé François d Assise (0.67 FTE)
	BRUST	Matthias (0.21 FTE)
	CASINI	Giovanni
	CASTIGNANI	German
	COGLIATI	Benoît-Michel (0.25 FTE)
	CRAMER	Marcos
	DI NARDO	Daniel (0.5 FTE)
	DODER	Dragan (0.41 FTE)
	DOU	Wei
	EMARA	Karim Ahmed Awad El-Sayed (0.25 FTE)
	EMERAS	Joseph (0.16 FTE)
	FAYE	Sébastien
	GADYATSKAYA	Olga
	GHEORGHE	Gabriela (0.41 FTE)
	GUZEK	Mateusz (0.58 FTE)
	GÖKNIL	Arda
	HARTMANN	Thomas (0.13 FTE)
	HENARD	Christopher (0.41 FTE)
	HU	Tingting (0.04 FTE)
	HUYNEN	Jean-Louis (0.99 FTE)
	HÖHN	Sviatlana (0.04 FTE)
	IOVINO	Vincenzo
	JHAWAR	Ravi
	KANTOR	Miroslaw (0.45 FTE)
	KHOVRATOVICH	Dmitry
	KIM	Dongsun (0.99 FTE)
	KLIAZOVICH	Dzmitry (0.41 FTE)
	KUBLER	Sylvain
	LAMORTE	Luca (0.84 FTE)
	LANCRENON	Jean (0.83 FTE)
	LANZE	Fabian (0.16 FTE)
	LEE	Moon Sung
	LOUVETON	Nicolas (0.92 FTE)

Position	Last Name	First Name
	LUCIA	Lucia (0.75 FTE)
	MA	Qin (0.21 FTE)
	MATINNEJAD	Reza
	MIZERA	Andrzej
	NAVEH	David
	NESHVAD	Surena (0.42 FTE)
	NGUYEN	Duy Cu (0.58 FTE)
	OSTREV	Dimiter (0.25 FTE)
	OUCHANI	Samir
	PALATTELLA	Maria Rita (0.77 FTE)
	PARENT	Xavier
	POPLETEEV	Andrei
	RIAL DURAN	Alfredo (0.84 FTE)
	ROBALDO	Livio
	ROBERT	Jérémy
	RODRIGUEZ LERA	Francisco Javier (0.25 FTE)
	ROENNE	Peter (0.75 FTE)
	SANNIER	Nicolas
	SASNAUSKAS	Raimondas (0.25 FTE)
	SHAR	Lwin Khin
	SOUA	Ridha (0.71 FTE)
	TABATABAEI	Masoud
	TANG	Qiang (0.92 FTE)
	TRUJILLO RASUA	Rolando
	VELICHKOV	Vesselin
Research Associate	ALLIX	Kevin (0.79 FTE)
	BOTEV	Jean
	FORSTER	Daniel (0.63 FTE)
	FOUQUET	François
	GLODT	Christian
	GROSZSCHÄDL	Johann
	LUCAS FILHO	Edson Ramiro (0.08 FTE)
	MACHALEK	Aurel
	MOAWAD	Assaad (0.96 FTE)
	MUSZYNSKI	Jakub (0.04 FTE)
	PLUGARU	Valentin (0.58 FTE)
	SIRRES	Raphaël (0.12 FTE)
	ZIAFATI	Pouyan (0.37 FTE)
Research Scientist	BERNARD	Nicolas
	BIANCULLI	Domenico (0.42 FTE)
	BISSYANDE	Tegawendé François d Assise (0.33 FTE)
	CAPOZUCCA	Alfredo
	DANOY	Grégoire
	FRANCK	Christian

Position	Last Name	First Name
	FRANK	Raphaël
	MA	Qin (0.29 FTE)
	NEJATI	Shiva
	PANCHENKO	Andriy
	PANG	Jun
	PAPADAKIS	Mike
	RIES	Benoit
	VARRETTE	Sébastien
	WEYDERT	Emil
Administrative Aid	DESSART	Bertrand
	EDWARDSDOTTIR	Helga
	FLAMMANG	Danièle (0.75 FTE)
	OCHSENBEIN	Anne
	OESTLUND	Stefanie (0.7 FTE)
	SCHMITZ	Fabienne
	SCHROEDER	Isabelle (0.5 FTE)
	THÜR	Claudia
	WOLTERS	Nicola (0.15 FTE)
Technical Support Staff Member	DUNLOP	Dominic
	LE CORRE	Yann
	REIS	Sandro
	STEMPER	André
Technician on Project	JAHIC	Benjamin (0.29 FTE)
	KORDY	Piotr (0.83 FTE)
	PLUGARU	Valentin (0.41 FTE)
Scientific Support Staff Member	LADID	Latif
Doctoral Candidate	AMBROSSIO	Diego Agustin
	ARORA	Chetan (0.83 FTE)
	ATASHPENDAR	Arash
	BEN ABDESSALEM (HELALI)	Raja
	BEN FADHEL	Ameni (0.99 FTE)
	BRAU	Guillaume (0.99 FTE)
	BRONZI	Walter
	BRÜHL	Manuel (0.99 FTE)
	CAPPONI	Andrea (0.33 FTE)
	CHANGAIVAL	Boonyarit (0.96 FTE)
	CHENAL	Massimo
	CODECA	Lara
	DAUPHIN	Jérémie (0.08 FTE)
	DELERUE ARRIAGA	Afonso
	DERRMANN	Thierry
	DI MAIO	Antonio (0.71 FTE)
	DI NARDO	Daniel (0.33 FTE)

Position	Last Name	First Name
	DINU	Dumitru-Daniel
	DOBRICAN	Remus-Alexandru
	FARJAMI	Ali (0.08 FTE)
	FIANDRINO	Claudio (0.87 FTE)
	GAMMAITONI	Loïc (0.99 FTE)
	GOTTMANN	Susann (0.93 FTE)
	GREVISSE	Christian (0.96 FTE)
	GUO	Siwen (0.96 FTE)
	HAJRI	Ines
	HARTMANN	Thomas (0.87 FTE)
	HUMPHREYS	Llio (0.54 FTE)
	HURIER	Médéric
	HÖHN	Sviatlana (0.16 FTE)
	HÖHN	Winfried
	IBRAHIM	Abdallah Ali Zainelabden Abdallah
	JAFARNEJAD	Sasan
	JAN	Sadeeq
	JIMENEZ	Matthieu
	KAMPAS	Dimitrios (0.45 FTE)
	KLEIN	Johannes
	KRACHEEL	Martin (0.33 FTE)
	LE	Ha Thanh
	LI	Daoyuan
	LI	Li
	LIU	Bing
	LOPEZ BECERRA	José Miguel
	LOUNIS	Karim
	MADDOURI	Sami (0.1 FTE)
	MARGOSSIAN	Harag (0.04 FTE)
	MARTINEZ	Jabier (0.83 FTE)
	MITSEVA	Asya (0.75 FTE)
	MOAWAD	Assaad (0.04 FTE)
	MOULINE	Ludovic
	MULLER	Christian (0.49 FTE)
	NACHTIGALL	Nico (0.53 FTE)
	NESHVAD	Surena (0.58 FTE)
	NEYENS	Gilles
	NIELSEN	Sune Steinbjorn (0.2 FTE)
	NORTA	David
	PEJO	Balazs
	PEREZ URQUIDI	Jose Miguel (0.75 FTE)
	PERRIN	Léo Paul
	PIERINA BRUSTOLIN SPAGNUELO	Dayana
	SANCHEZ GUINEA	Alejandro
	SIMIONOVICI	Ana-Maria (0.83 FTE)

Position	Last Name	First Name
	SKROBOT	Marjan (0.99 FTE)
	SMITH	Zachary Daniel (0.55 FTE)
	SOLTANA	Ghanem
	SUN	Xin (0.49 FTE)
	SUNDHARAM	Sakthivel Manikandan
	THOME	Julian
	TIKHOMIROV	Sergei (0.25 FTE)
	TORO POZO	Jorge Luis
	UDOVENKO	Aleksei
	VAN ZEE	Marc
	VAZQUEZ SANDOVAL	Itzel (0.16 FTE)
	WANG	Chunhui
	WANG	Jun
	YUAN	Qixia
	ZHANG	Yang (0.91 FTE)
Senior Lecturer	KLEIN	Jacques
	LENZINI	Gabriele
	SABETZADEH	Mehrdad
Student with Limited Contract	SOROUSH	Najmeh (0.38 FTE)
Intern	FORSTER	Daniel (0.29 FTE)

Appendix F

List of Acronyms

ComSys: Communicative Systems Laboratory
CSC: Computer Science & Communications
HPC: High Performance Computing
ILIAS: Interdisciplinary Laboratory for Intelligent and Adaptive Systems
LACS: Laboratory of Algorithmics, Cryptology and Security
LASSY: Laboratory for Advanced Software Systems
SnT: Interdisciplinary Centre for Security Reliability and Trust
UL: University of Luxembourg
FNR: Fonds National de la Recherche Luxembourg

http://csc.uni.lu

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

Administrative Contact:

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