Department of Computer Science

Activity Report 2022

Department of Computer Science

Activity Report 2022

Keywords:
Activity Report, University of Luxembourg, Department of Computer Science, UL, DCS

Department of Computer Science
Activity Report 2022

Address:

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

Administrative Contact:

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

Preface

Dear reader,

This annual report synthesizes the progress and activities of the Department of Computer Science in 2022, including our research projects, teaching programs, organized events, awarded papers, visiting researchers and publications. We hope that you will find this report stimulating and inspiring. On behalf of the Department of Computer Science, we invite you to contact any one of us if you have any questions regarding the research we conduct in the DCS.

Best regards,

Sjouke Mauw
Pascal Bouvry

Contents

Mission

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

DCS 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.

DCS mission: To perform groundbreaking fundamental and applied research in computer science, 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. DCS 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 conse- quently we have set up a structure that can deal with a dynamic environment. The multiple research areas and interests of DCS 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 di- versity and agility continue to provide a very solid base for visible and relevant research in a changing world.

Executive Summary

The Department of Computer Science, or DCS for short (https://dcs.uni.lu), includes a staff of roughly 165 full-time equivalent members involved in teaching, research and outreach activities.

Strategic development remained a priority of the department in 2022, leading to the definition of a number of positions to strengthen the department's research and teaching activities. The recruitment process for a new Machine Learning position has been successfully completed.

Our research activities have led to 240 publications in 2022, many of them in top journals and conferences, and have also led to significant outreach activities in the academic and social context. Our productivity has benefited strongly from the large number of externally funded projects executed in our department.

The results of the university-wide teaching evaluation became available in 2021. The final report clearly shows that the Computer Science teaching cluster provides high quality teaching. We are happy with this result, but quality management is of course a dynamic process. Therefore, the outcome of the evaluation will serve as a solid basis to further improve the teaching quality and optimise resource allocation through synergies between programmes.

In addition to the positive overall teaching evaluation, three of our educational programmes have been officially accredited by the German Accreditation, Certification and Quality Assurance Institute (ACQUIN). The three concerned programmes are: the Bachelor in Applied Information Technology (BINFO), the Bachelor in Applied Information Technology - Continuing Education Programme (BINFO-CEP), and the Master in Information and Computer Science (MICS). In 2023, we plan to start the accreditation procedure for our newer Bachelor in Computer Science (BICS).

A consortium of European partners led by the University of Luxembourg has been selected by the EuroHPC Joint Undertaking to design and implement the first pan-European High Performance Computing (HPC) pilot Master's programme. Our department was heavily involved in this initiative, which shows that our decade long investments in HPC facilities and research, led by Pascal Bouvry, has made us a major player in this field. The new HPC Master has started in September 2022.

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

DCS is divided into 4 themes:

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

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

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

Head

- Sjouke Mauw, professor, Head of DCS until 31/03/2022
- Pascal Bouvry, professor, Head of DCS from 01/04/2022

Vice head

- Nicolas Navet, professor, Vice Head of DCS and Departmental Head of Teaching

Academic Staff

- Alex Biryukov, professor
- Pascal Bouvry, professor
- Jean-Sébastien Coron, professor
- Thomas Engel, professor, head of COMSYS
- Dov Gabbay, guest professor
- Nicolas Guelfi, professor
- Pierre Kelsen, professor, head of LASSY
- Franck Leprévost, professor, head of LACS
- Luis Leiva, assistant professor
- Sjouke Mauw, professor, head of DCS
- Yves Le Traon, professor
- Volker Müller, associate professor
- David Naccache, honorary professor
- Nicolas Navet, professor, vice head of DCS
- Henderik Proper, affiliated professo
- 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
- Martin Theobald, professor
- Leon van der Torre, professor
- Denis Zampunieris, professor

Since DCS counts among its contributions the continued support of the SnT, please look at the SnT 2022 annual report to get a complementary overview of DCS activities in the area of Security, Reliability and Trust.

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 Department (CSC) including the Communicative Systems Lab (COMSYS), the Interdisciplinary Lab for Intelligent and Adaptive Systems (ILIAS), and the Lab of Advanced Software Systems (LASSY). In 2006, LACS and the Decision Support chair also joined CSC.

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

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

Until 2020, the three faculties of the University of Luxembourg were formally subdivided into Research Units, one of which was CSC. From January 1st, 2020, a new substructuring of the faculties came into force, which formally led to the transformation of CSC into the Department of Computer Science (DCS). This provided a more independent role of the department in relation to teaching, which led to the creation of the position of Departmental Head of Teaching.

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 DCS, 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, the third interdisciplinary center on digital humanities called C^{2}DH, and the faculty priority on computational sciences. Moreover, we will continue investing in research areas of interest to such domains, such as machine learning and high-performance computing.

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

Detailed Research Program

Communicative Systems

The Communicative Systems Laboratory (Com.Sys) performs state-of-the-art research in digital communications. The rapidly growing demand for information sharing requires technologies such as pervasive and ubiquitous computing, IoT, and other related paradigms and technologies to meet the information society's needs and devise new adaptive approaches to address the continued data and interaction issues. Embracing the end-to-end arguments in system design, Com.Sys follows an integrated research approach in the areas of Information Transfer and Communicating Systems. Information Transfer is concerned with information transmission over potentially complex channels and networks. Communicating Systems, in turn, are the composition of multiple distributed entities employing communication networks to achieve a common goal collaboratively. However, Com.Sys focuses not only on the communication between but also on communication with and within such systems. Com.Sys has strong technical and personal facilities to improve existing and develop new solutions in the following research topics:

- Adaptive Networking
- Information Transmission and Diffusion
- Machine Learning for Communication Systems
- Mediated Reality and Human-Computer Interaction
- Network and Systems Security
- Peer-to-Peer Computing and Networking
- Secure Communication Protocols

- Socio-Technical Systems Design
- Trust Models, Anonymity, and Privacy in Distributed Systems
- Wireless (Mobile/Vehicular) Communication Systems

Com.Sys comprises the following collaborating groups and labs conducting research in complementary areas: the Collaborative and Socio-Technical Systems (COaST) group with its Virtual Reality and Augmented Reality lab (VR/AR Lab), and the Security and Networking lab (SECAN-Lab).

COaST focuses on distributed collaborative systems, complex networks and self-organization, socio-technical modeling, educational technologies, and mediated reality. The group operates the VR/AR Lab at the Department of Computer Science, which develops and explores immersive experiences, novel context-aware applications, and distributed virtual environments.

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

Intelligent and Adaptive Systems

The *Intelligent and Adaptive Systems Research Group* (ILIAS; see ilias.uni.lu) is home to 5 research groups and the associated scientific staff.

ILIAS investigates the theoretical foundations and algorithmic realisations of Intelligent Systems for complex problem solving and decision making in uncertain and dynamic environments. Our activities include interdisciplinary research that fits to the rapidly growing role of Artificial Intelligence and Data Science.

Collaboration with the interdisciplinary centres **C^{2}DH, LCSB** and **SnT** and the **Faculty of Law, Economics and Finance**, as well as with the **Faculty of Humanities, Education and Social Sciences**, participation in the **High Performance Computing** (HPC) facility and collaboration with the **Computational Sciences Initiative** reflect the importance of ILIAS to Luxembourg's strategic priorities and future. In recent years, ILIAS has contributed to **Esch2022** with the AI&Art Pavilion and created a centre for knowledge exchange with the **Computational Creativity Hub**.

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

- **Big Data** (Prof. Theobald): we investigate scalable architectures for the distributed indexing, querying and analysis of large volumes of data. Specific focus areas include information extraction, probabilistic and temporal database models as well as distributed graph and streaming engines.
- **Computational Interaction** (Prof. Leiva): The Computational Interaction group conducts research at the intersection of Human-Computer Interaction and Machine Learning, grounded on both foundational and practical principles via computational methods and data-driven models that can enable, support, explain, and improve any kind of user interaction.
- **Knowledge Discovery and Mining** (Prof. Schommer): the research areas include fundaments and applications of Machine Learning including Deep Learning, Sentiment Analysis, the use of Natural Language Processing for a ChatBot design, and Data/Text Mining.
- **Knowledge Representation and Reasoning** (Prof. van der Torre): we concern ourselves with normative reasoning in Multi-Agent Systems, particularly, Logics for Security and

Compliance as well as Machine Ethics, Legal Knowledge Representation, Inference under Uncertainty and Inconsistency, Logic-based models for intelligent Agents and Robots, and Computational Choice.

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

Our outreach activities are manifold, diverse, and interdisciplinary, and span collaborations with other departments. We regularly do presentations at schools and student fairs and cooperate with industry, if our expertise for the society is requested. We motivate young students to work with robots, for example within the AIRoboLab, and prepare them for new upcoming disciplines in Artificial Intelligence, Machine Learning, and beyond.

Algorithmics, Cryptology and Security

The Laboratory of Algorithmics, Cryptology and Security (LACS) adopts a state of the art, dynamic, multifaceted and algorithmic approach to cryptology and cybersecurity-related research topics. We cover the following topics:

- Complexity theory and algorithmics
- Theoretical computer science
- Mathematics of security
- Symmetric and public key cryptography
- Efficient software and hardware implementation of cryptography
- Side-channel attacks and countermeasures
- Security protocols
- Privacy and anonymity
- Formal methods for security and privacy
- Verifiable voting systems, E-democracy
- Network, mobile and embedded systems security
- Cloud computing, reputation based systems
- Cryptocurrencies, blockchain & distributed ledger technologies
- Socio-technical aspects of security and trust
- Quantum and post-quantum information assurance
- Security and privacy of AI, machine learning

LACS contributes to teaching programs, including:

- Bachelor: BICS, BINFO
- Master: MICS, MISSM, MADS
- Doctoral Program in Computer Science and Computer Engineering: DP-CSCE

LACS also contributes to the development and implementation of new teaching programs: Master in HPC, Master in Cybersecurity and Cyberdefense, etc.

LACS outreach activities have had a significant impact on computer and cybersecurity in society: presentations to schools, participation to Science Festivals, Scienceteens, hackathons, membership of governing bodies of public and private entities in security, contribution to standards in cryptography, etc.

The following professors and their teams contribute to this research and teaching area: Alex

BIRYUKOV, Jean-Sébastien CORON, Franck LEPRÉVOST, Sjouke MAUW, Volker MÜLLER, Jun PANG, Peter Y. A. RYAN.

Detailed areas of expertise:

- Alex BIRYUKOV
  – Symmetric Cryptography
  – Cryptanalysis and Design of Cryptographic Algorithms
  – Privacy and Anonymity
  – Blockchain and Distributed Ledgers
  – Side-channel Attacks and Countermeasures
  – Network, Mobile and Embedded Systems Security

- Jean-Sébastien CORON
  – Computational Number Theory
  – Public-Key Cryptography
  – Side-Channel Attacks

- Franck LEPRÉVOST
  – Computational Number Theory
  – Security of Convolutional Neural Networks
  – Evolutionary Algorithms
  – Geopolitics of Security Issues

- Sjouke MAUW
  – Security Protocols
  – Privacy, Anonymity and Unlinkability
  – Formal Methods and logics for security and privacy
  – Privacy in social networks
  – Electronic voting protocols
  – Distance-bounding protocols
  – Secure and private electronic payments
  – Secure memory attestation and erasure
  – Attack Trees

- Volker MÜLLER
  – Computational Number Theory
  – Security Primitives in Business Applications

- Jun PANG
  – Complex networks
  – Formal models and methods for security
  – Formal verification
  – Graph machine learning
  – Privacy and anonymity
  – Security and privacy in machine learning

- Peter Y. A. RYAN
  – Analysis of Information Flow
  – Design and analysis of cryptographic Protocols
  – Verifable Voting Schemes
  – Efficient, side-channel resistant implementation of crypto algorithms
  – Modelling and Analysis of security-critical systems and security policies
  – Quantum and post-quantum cryptography
  – Socio-technical Aspects of Security

– Application of game theory to security

Advanced Software and Systems

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

- Modelling: we investigate the foundations of model-driven engineering (MDE) as well as applications of MDE in fields as diverse as mobile computing, the 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. Building trustable AI systems is a major challenge today, in particular concerning their correctness, security and ethics. This research aims at providing means to assess that the machine learning system works reliably and as expected, without deviating over time from its initial performances and being robust to adversarial attacks.
- Application domains: examples are automotive and aerospace embedded systems, enterprise architectures, cyberphysical systems, e-learning and pervasive healthcare systems.

Research Groups

4.1 Applied Crypto Group (ACG)
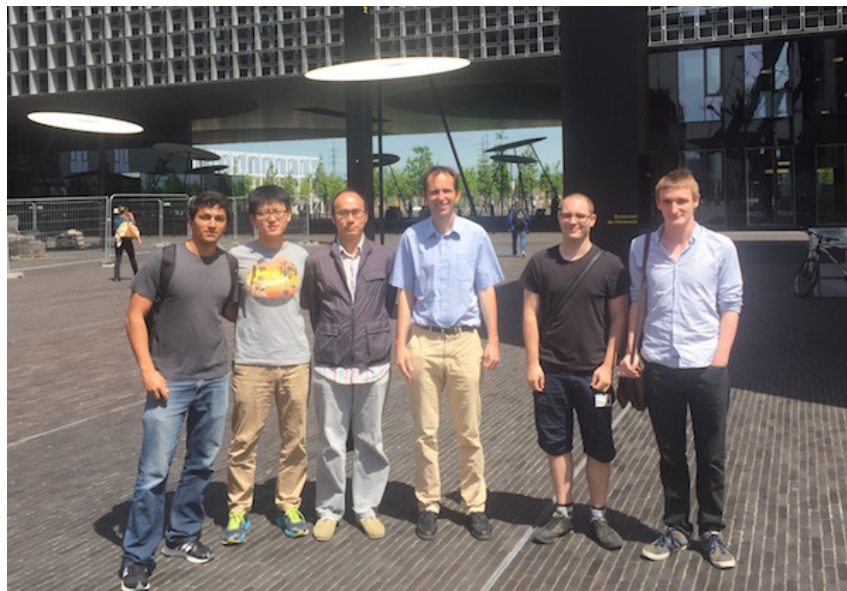
Head of research group: Jean-Sebastien Coron

The Applied Crypto Group (ACG) is doing research in cryptography, within the Department of Computer Science (DCS) of the University of Luxembourg.

ERC Advanced Grant CLOUDMAP (2018-2025).

Summary of the group's achievements in 2022

• 4 publications at top-tier conferences in cryptography (Eurocrypt, Asiacrypt and TCHES x2)

Three most interesting publications (or other achievements) in 2022.

• Jean-Sébastien Coron, François Gérard, Simon Montoya, Rina Zeitoun. High-order Table-based Conversion Algorithms and Masking Lattice-based Encryption. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2022(2): 1-40 (2022)

We describe an efficient countermeasure against side-channel attacks, and describe an

application to the Kyber post-quantum encryption scheme.
- Orel Cosseron, Clément Hoffmann, Pierrick Méaux, François-Xavier Standaert. Towards Case-Optimized Hybrid Homomorphic Encryption - Featuring the Elisabeth Stream Cipher. ASIACRYPT (3) 2022: 32-67

We describe an efficient homomorphic encryption friendly stream cipher.
- Thomas Espitau, Pierre-Alain Fouque, François Gérard, Mélissa Rossi, Akira Takahashi, Mehdi Tibouchi, Alexandre Wallet, Yang Yu. Mitaka: A Simpler, Parallelizable, Maskable Variant of Falcon. EUROCRYPT (3) 2022: 222-253

We describe an efficient post-quantum signature scheme.

4.2 Applied Security and Information Assurance (APSIA)

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

The APSIA group is part of the SnT and has strong connections to DCS and the LACS laboratory. The group specialises in the design and analysis of security and privacy primitives and protocols. Of particular interest: secure, verifiable voting protocols, authenticated key establishment protocols, both classical and quantum, including password-based and out of band-based. APSIA also has expertise in the socio-technical aspects of security and trust. The group recently established the APSIA Quantum Lab that specialises in the design and analysis of both quantum crypto and "post-quantum" (aka quantum resistant) and hybrid crypto. The Strategy Lab was also established soon after the Quantum Lab and this addresses applications of game theory and strategy theory to security critical.

Summary of the group's achievements in 2022

Research projects

The group was again successful in the CORE call and was awarded the SpaceVote that continues the group's collaboration with Polish Academy of Sciences on formal verification of secure voting procedures and is the group's first step into space applications.

The Quantum continued to go from strength to strength with several new projects on secure quantum communications infrastructure under way, including the INT-UQKD project which has its kickoff meeting in September 2022. The group also landed a joint project with LuxTrust on developing optimal migration strategies to a quantum resistant security infrastructure.

The Strategy Lab High productivity of the Strategy Lab, with very interesting results on computational strategic ability in security games, as well as the epistemic vs. information-theoretic variants of coercion resistance.

Software

1. INT-UQKD Crypto Box: A software based quantum resistant cryptographic solution for end to end communication.

2. Web applications for the Selene and the Hyperion voting schemes with transparent verification.

3. SZK Compiler: A compiler for stateful zero knowledge proofs.

4. A verifiable mixnet for electronic voting: undergoing optimization/testing.

Teaching

Courses taught in the MISC: Information Security Basics, Security Modelling and Principles of Security Engineering, "Advanced Computing" and "Software Foundations". The group contributes to the BICS Security 2 course. The group continues to run the internal "breakfast" talks as well as organizing the bulk of the SRMs, the joint SATOSS/APSIA seminars.

Four most interesting publications in 2022

1. Mónica P. Arenas, Muhammed Ali Bingol, Hüseyin Demirci, Georgios Fotiadis, Gabriele Lenzini: A Secure Authentication Protocol for Cholesteric Spherical Reflectors Using Homomorphic Encryption. In L. Batina, J. Daemen (eds.), *13th International Conference on Cryptology in Africa – AFRICACRYPT'2022*, vol. 13503 of *Lecture Notes in Computer Science - LNCS*, pp. 425–447, Springer, Cham., 2022. https://doi.org/10.1007/978-3-031-17433-9_18.

2. David Mestel, Johannes Müller, Pascal Reisert: How Efficient are Replay Attacks against Vote Privacy? A Formal Quantitative Analysis. IEEE CSF 2022

3. Hao Cheng, Georgios Fotiadis, Johann Großschädl, Peter Y. A. Ryan: Highly Vectorized SIKE for AVX-512. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022(2): 41-68.

4. Ehsan Ebrahimi. Post-quantum security of Plain OAEP Transform. International Conference on Theory and Practice of Public Key Cryptography 2022 (PKC 2022). DOI: https://doi.org/10.1007/978-3-030-97121-2_2

4.3 BigData, Data Science & Databases (BigData)

Head of research group: Prof. Dr. Martin Theobald

The "Big Data" group at the University of Luxembourg has meanwhile been active for six years. The group is headed by Prof. Dr. Martin Theobald, who previously held positions at the Max-Planck-Institute in Saarbrücken, at the University of Antwerp, and at Ulm University. In 2022, the group consisted of three PhD students, Alessandro Temperoni, Mauro Dalle Lucca Tosi and Jingjing Xu, as well as one post-doctoral researcher, Dr. Maria Birykuv. One further PhD student, Aiste Gerybaite, has jointly been supervised in the context of the "Joint International Doctoral (Ph.D.) Degree in Law, Science and Technology" in collaboration with the Universities of Bologna and Turin. Three of our PhD candidates are expected to graduate in 2023. Martin Theobald returned from a parental leave in January 2022 and since then took over his new academic duty as Study Director of the Bachelor in Computer Science (BiCS) program.

(1) Relation Extraction & Knowledge-Base Construction

Relation extraction (RE) is a sub-discipline of information extraction (IE) which focuses on the prediction of a relational predicate from a natural-language input unit (such as a sentence, a clause, or even a short paragraph consisting of multiple sentences and/or clauses).

Together with named-entity recognition (NER) and disambiguation (NED), RE forms the basis for many advanced IE tasks such as knowledge-base (KB) population and verification. In our recent works, we explored how recent approaches for open information extraction (OpenIE) may help to improve the task of RE by encoding structured information about the sentences' principal units, such as subjects, objects, verbal phrases, and adverbials, into various forms of vectorized (and hence unstructured) representations of the sentences. Our main conjecture is that the decomposition of long and possibly convoluted sentences into multiple smaller clauses via OpenIE even helps to fine-tune context-sensitive language models such as BERT (and its plethora of variants) for RE. Our experiments over two annotated corpora, KnowledgeNet and FewRel, demonstrate the improved accuracy of our enriched models compared to existing RE approaches. Our best results reach 92% and 71% of F1 score for KnowledgeNet and FewRel, respectively, proving the effectiveness of our approach on competitive benchmarks.

(2) Question-Answering over Hybrid Knowledge Graphs

Answering complex questions over textual resources remains a challenging problem—especially when interpreting the fine-grained relationships among multiple entities that occur within a natural-language question or clue. Curated knowledge bases (KBs), such as YAGO, DBpedia, Freebase and Wikidata, have been widely used in this context and gained great acceptance for question-answering (QA) applications in the past decade. With our BigText-QA project, we aim to develop an integrated QA system which is able to answer questions based on a more redundant form of a knowledge graph (KG) that organizes both structured and unstructured (i.e., "hybrid") knowledge in a unified graphical representation. BigText-QA thereby is able to combine the best of both worlds—a canonical set of named entities, mapped to a structured background KB (such as YAGO or Wikidata), as well as an open set of textual clauses providing highly diversified relational paraphrases with rich context information.

(3) TensAIR – Online Learning from Data Streams via Asynchronous Iterative Routing

Online learning (OL) from data streams is an emerging area of research that encompasses numerous challenges from stream processing, machine learning, and networking. Recent extensions of stream-processing platforms, such as Apache Kafka and Flink, already provide basic extensions for the training of neural networks in a stream-processing pipeline. However, these extensions are not scalable and flexible enough for many real-world use-cases, since they do not integrate the neural-network libraries as a first-class citizen into their architectures. With our TensAIR project, we provide an end-to-end dataflow engine for OL from data streams via a protocol to which we refer as asynchronous iterative routing. TensAIR supports the common dataflow operators, such as Map, Reduce, Join, and has been augmented by the data-parallel OL functions Train and Predict. Our decentralized architecture allows TensAIR to efficiently shard incoming data batches across the distributed model replicas, which in turn trigger the model updates via asynchronous stochastic gradient descent (ASGD). We empirically demonstrate that TensAIR achieves a nearly linear scale-out in terms of (1) the number of worker nodes deployed in the network, and (2) the throughput at which the data batches arrive at the dataflow operators. We exemplify the versatility of TensAIR by investigating both sparse (Word2Vec) and dense (CIFAR-10) use-cases, for which we are able to demonstrate very significant performance improvements in comparison to Kafka, Flink, and Horovod (developed by Uber).

Furthermore, our teaching activities focus on Databases, Data Science and Big Data Analytics:

We intensively employed current Big Data platforms, such as the Apache Hadoop/Pig/HIVE/HBase

software stack, Spark, Giraph, GraphX, as well as MongoDB, for teaching and application development. In particular Spark offers a wealth of constantly updated Machine Learning libraries (MLlib), which we applied to a variety of data collections in the context of different student projects. The group also actively contributes to the curricula for three study programs at the Departments of Computer Science (Bachelor & Master in Computer Science) as well as the Department of Mathematics (Master in Data Science) with four lectures per year. Two lectures in the areas of "Cloud Computing & NoSQL Databases" and "Big Data Analytics" are shared among the two Master programs.

Summary of the group's achievements in 2022

1. Vinu Ellampallil Venugopal, Martin Theobald, Damien Tassetti, Samira Chaychi, Amal Tawakuli: Targeting a light-weight and multi-channel approach for distributed stream processing. J. Parallel Distributed Comput. 167: 77-96 (2022)

2. Maciej Skorski, Alessandro Temperoni, Martin Theobald: Robust and Provable Guarantees for Sparse Random Embeddings. PAKDD (2) 2022: 211-223

3. Mauro Dalle Lucca Tosi, Vinu Ellampallil Venugopal, Martin Theobald: Convergence time analysis of Asynchronous Distributed Artificial Neural Networks. COMAD/CODS 2022: 314-315

4.4   Collaborative and Socio-Technical Systems (COaST)

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

Deputy Head of research group: Dr. Jean Botev

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

Summary of the group's achievements in 2022

In 2022, the COaST group counted 6 members (1 professor, 1 senior researcher, 4 PhD candidates) and 5 publications. The group's research, particularly in the context of the ongoing projects ChronoPilot and DELICIOS, appeared in renowned academic publications and was presented at various international conferences and scientific events. The Minett Stories Rallye, developed by the VR/AR Lab in collaboration with the Luxembourg Centre for Contemporary and Digital History (C^{2}DH) to promote the Esch2022 exhibition "Remixing Industrial Pasts – Constructing the Identity of the Minett" (February 27, 2022 - May 15, 2022) at the Massenoire in Esch Belval, went live at the end of February and remained available during the year. The digital treasure hunt allows visitors of the European Capital of Culture to discover on-site various places related to the history of the area's industrial past. The VR/AR Lab and its EU-funded H2020 FET Open project ChronoPilot were also featured at the nearly sold-out Science Slam at Neumünster Abbey in Luxembourg. Members of the group were involved in the organisation of various

international scientific events and conferences, such as IEEE ACSOS, LIFELIKE, and ACM MMSys/MMVE. The COaST group's teaching activities comprised numerous lectures and seminars in the different bachelor and master programs (BINFO, BICS, MICS, BINFO-FC) offered by the University of Luxembourg.

Three most important publications in 2022

1. **Ningyuan Sun, Jean Botev, Yara Khaluf, Pieter Simoens.** Theory of Mind and Delegation to Robotic Virtual Agents. In Proc. 31st IEEE International Conference on Robot & Human Interactive Communication (RO-MAN 2022), pp.454-460, 2022.

   This study explores whether a robotic virtual agent's ability to use theory of mind (ToM) affects users' delegation behaviour, but the results invalidate the hypothesis that the level of theory of mind is a reliable indicator of delegation choices. Instead, the participants' performance strongly correlates with their delegatory intentions, suggesting that designers should focus on balancing user performance perception to induce the desired delegation behaviours rather than using ToM-resemblance features.

2. **Aryobarzan Atashpendar, Christian Grévisse, Jean Botev, Steffen Rothkugel.** Semantic and Interactive Search in an Advanced Note-taking App for Learning Material. In Proc. 24th International Conference on Human-Computer Interaction (HCI International 2022) / 9th International Conference on Learning and Collaboration Technologies (LCT 2022), pp.13-29, 2022.

   This paper proposes improvements to digital note-taking apps by introducing semantic search and automatic question-answering for more efficient information retrieval. It also suggests visual methods for finding specific notes, including integrating a semantic similarity metric and dynamically generated filters, and explores a graph-based visualisation for search results.

3. **Stéven Picard, Jean Botev.** Rhythmic Stimuli Effects on Subjective Time Perception in Immersive Virtual Environments. In Proc. 14th International Workshop on Immersive Mixed and Virtual Environment Systems (MMVE 2022) / 13th ACM Multimedia Systems Conference (MMSys 2022), pp.5-11, 2022.

   In this paper, time perception and performance in a virtual environment during a cognitive task while exposed to rhythmic stimuli are investigated, finding that single stimuli can lead to more pronounced time perception variations, while synchronised stimuli can lead to compression or dilation. The study also shows that the tempo of the stimuli affects the judgment of time being fast or slow and that the presence of visual stimuli can negatively impact task performance. The findings suggest that tailored rhythmic stimuli modulation can improve the design of immersive virtual environments.

4.5   Computational Interaction (COIN)

Head of research group: Prof. Dr. Luis Leiva

Members: Dr. Mateusz Dubiel (September 2021), Mr. Kayhan Latifzadeh (January 2022) and Dr. Bereket Yilma (February 2022)

The COIN group was established in February 2021 and is part of the Interdisciplinary Lab for Intelligent and Adaptive Systems (ILIAS) of the Department of Computer Science. We use computational methods and data-driven models in user interaction research. In particular, our work addresses both fundamental and applied research activities in the following areas:

- Human-Computer Interaction, with a strong focus on computational user interface design and interactive input techniques.
- Machine Learning, in particular research with Deep Learning models.
- Information Retrieval, especially related to human factors and interfaces.
- Natural Language Processing, including text generation, phrase sampling, and text entry.

In addition, teaching and supervision of both Master of Science and Doctorate students rank high in the group's activities. We pursue a strong educational policy and actively combine state-of-the-art research with the training of next generation of high-class researchers. The group also engages in strong cooperative research activities by direct and peer-to-peer interactions with relevant industrial actors resulting in jointly funded PhD students and significant technology transfer.

Summary of achievements

In 2022 the group published 5 conference papers and 5 journal articles in top scientific venues in their respective fields. The group taught two new courses: "Designing Interactive Systems" in the Master's in Computer Science (MiCS) and "Prototyping with Deep Learning " in the Master's in Data Science (MADS). The group also taught in the 6th Summer School on Computational Interaction. The group has been very successful in attracting international funding from the European Innovation Council of the European Union (Pathfinder program) as well as national funding from the Fonds National de la Recherche (AFR program). The group has collaborated with the Centre for Contemporary and Digital History (C2DH), NVIDIA AI Luxembourg, and LuxProvide/MeluXina. The group has participated in the organization of 8 international scientific conferences. Prof. Leiva participated as a panel evaluator for the Danish Data Science Academy (DDSA) and was appointed as DCS representative in the Faculty Council in July and DCS communications representative in September. Dr. Dubiel got the Best Dissertation Award Runner Up from the prestigious iSchools institute.

Three most interesting publications in 2022

1. Luis A. Leiva, Asutosh Hota, Antti Oulasvirta. Describing UI Screenshots in Natural Language. ACM Transactions on Intelligent Systems and Technology, Vol. 14(1), 2022.

   We propose a novel user interface captioning method, combining Deep Learning models for topic classification and element saliency prediction, and a template-based natural language generation engine.

2. Klen Čopič Pucihar, Nuwan T. Attygalle, Matjaž Kljun, Christian Sandor, Luis A. Leiva. Solids on Soli: Millimetre-Wave Radar Sensing through Materials. Proceedings of the ACM on Human-Computer Interaction (PACM HCI, EICS), 2022.

   We investigate how the internal structure of materials impacts recognition performance for radar sensing technology. We got the best paper honorable mention award.

3. Mateusz Dubiel, Bereket A. Yilma, Kayhan Latifzadeh, Luis A. Leiva. A Contextual Framework for Adaptive User Interfaces: Modelling the Interaction Environment. CHI'22 Computational UI Workshop, 2022.

   We formalize a contextual framework based on Reinforcement Learning for adaptive user interfaces and illustrate a practical application using learning management systems as a case study.

4.6   Critical Real-Time Embedded Systems (CRTES)

Head of research group: Prof. Nicolas Navet

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

Summary of the group's results in 2022

In 2022 the CRTES group comprised 4 members (1 professor, 1 research scientist, 2 PhD students) and had 6 peer-reviewed publications published or accepted. Prof. Navet was on a scientific leave at the Institute of Electronics, Information Engineering and Telecommunications (National Research Council) in Turin from September to December 2022. Prof. Navet serves since July 2020 as deputy head of the department in charge of teaching. The group's members have taught 2 courses, both at the Bachelor and Master levels, and supervised 4 Bachelor semester projects (BSP). Group members were in the defense board of 4 PhD thesis, 2 Master thesis and TPC member of 7 conferences.

Most of our work in 2022 was in the field of E/E architecture design and real-time communication networks. Our work aims to further automate the design activities based on constraints and goals. We have been investigating for several years an approach rooted in computational thinking where system designers break down the general multi-dimensional design problem into smaller problems that algorithmic tools can solve in a near optimal way. In 2022, research works have also been done in the field of timing analysis of real-time networks with results on the use of simulation to validate real-time constraints and worst-case schedulability analysis considering the overhead of message authentication protocols.

Selected publications

1. **R. Gonzalez de Oliveira, N. Navet, A. Henkel, "Multi-objective optimization for safety-related available E/E architectures scoping highly automated driving vehicles", ACM Trans. on Design Automation of Electronic Systems (TODAES), Volume 28, Issue 3, Article No.: 41, pp 1-37, 2023.** This work proposes a design-space exploration framework for the development of Safety-Related Availability (SaRA) system according to ISO 26262 in the context in automated driving. The Model-Based Systems Engineering (MBSE) framework supports the synthesis and the multi-objective evaluation of automotive E/E architectures for the design of next-generation automotive E/E architectures.

2. **P. Keller, N. Navet, "Approximating WCRT through the aggregation of short simulations with different initial conditions: application to TSN", Proc. 30th International Conference on Real-Time Networks and Systems (RTNS '2022), Paris, June 7-8, 2022.** Simulation is the most popular and sometimes only suitable verification technique in the field of embedded systems, but it has the important limitation that, in most cases, worst-case scenarios are not observed during a simulation. This work investigates how to set simulation parameters to increase the likelihood to observe scenarios leading to large response times in communication networks. The approach taken is to aggregate simulation results over many short simulations instead of running a single long one, and, in our experiments on three realistic case-studies, it yields an average improvement of 10.5% of the maximum frame latencies observed.

3. **O. Ikumapayi, H. Olufowobi, J. Daily, T. Hu, I. C. Bertolotti and G. Bloom, "CANASTA: Controller Area Network Authentication Schedulability Timing Analysis", accepted for publication in IEEE Transactions on Vehicular Technology, 2022.** Controller Area Network (CAN) is one of main networking technologies in automotive systems and other industrial domains. Authenticity of a CAN frame was not considered in the protocol design but can be ensured by sending a Message Authentication Code (MAC) as a separate message. This will however create additional delays for safety-critical messages. This study provides the first comprehensive analysis of real-time schedulability analysis applied to authentication schemes for CAN networks and assess the overhead of MACs over a wide range of message sets.

4.7   Critical and Extreme Security and Dependability (CritiX)

Head of research group: Prof. Dr. Marcus Völp

The CritiX lab (https://wwwen.uni.lu/snt/research/critix) investigates and develops paradigms and techniques for defeating extreme adversary power and for sustaining perpetual and unattended operation. CritiX focusses on three scientific priorities:

• Resilience of cyber-physical system infrastructures and control;
• Internet and cloud infrastructures resilience; and
• Security and dependability of embedded components.

Our mid term development plan relies on investigating and publishing state-of-the-art advances along the following strategic objectives, which we deploy as research lines:

• Ultra-resilient minimal roots-of-trust and enclaves;
• Hybridisation aware distributed algorithms, models, and architectures;
• High-confidence vertical verification of mid-sized software;

Summary of the group's achievements in 2022

In 2022, CritiX contributed to the teaching in the Master of Information and Computer Science (MICS) through the course Fault and Intrusion Tolerant Systems as well as through the course Microkernel-based Systems. CritiX has successfully kicked off the FNR Core project ReSAC, which focuses on resilient activation in flexible real-time systems. Our goal is to leverage results from time-triggered systems while protecting against time-domain attacks. First results on Tolerating Resource Exhaustion Attacks in the Time-Triggered Architecture have already been published in collaboration with our German project partners Mouhammad Ibrahim Alkoudsi and Prof. Gerhard Fohler.

In our industry partnership with Huawei, we have developed mechanisms and protocols for securing intra-vehicular systems against targeted attacks (e.g., by replicating the controller which is responsible for following safe trajectories that have been identified by the perception and planning subsystems).

In the ADMORPH project, we have developed techniques for resilient consensual control as well as for nearby vehicles to take over control of other vehicles whose autonomous driving stack have failed. We achieve this by projecting the ego view of the helping vehicle to the location of the vehicle in jeopardy to safely steer the latter to a safe parking location.

In the context of the HERA project, we were able to demonstrate Methods for increasing the dependability of High-performance, Many-core Systems on a Chip as we

In 2022, two PhD students graduated on Secure, privacy-preserving and practical collaborative Genome-Wise Association Studies, on Architectural support for hypervisor-level intrusion tolerance in MPSoCs.

Prof. Völp had the pleasure to server in the executive board of the 34th Euromicro Conference on Real-Time Systems. He was elected member of the IFIP WG10.4 Dependability Working Group.

4.8 CryptoLux

Head of research group: Professor Dr. Alex Biryukov

The CryptoLux group is part of LACS/DCS/FSTM as well as SnT and works on all aspects of symmetric cryptography, ranging from the design and analysis of primitives over efficient and secure implementation to the deployment in real-world systems and networks. CryptoLux is also pursuing research on blockchain cryptography, distributed ledgers, smart contracts, and other emerging areas in information security, privacy, and anonymity. In 2022, the CryptoLux group consisted of seven members:\ a full professor, a research and development specialist (shared), four postdoctoral researchers, and one Ph.D. student. Further information about the group is available at https://www.cryptolux.org.

2022 was an outstanding year for the CryptoLux group in terms of both research performance and acquisition of third-party funding. The group successfully applied for an FNR CORE grant for the project CryptoFin and also obtained AFR funding for a Ph.D. project in the area of lightweight cryptography. CryptoFin is the successor of a previous CORE project with acronym FinCrypt (2018-2021) and will focus on advanced cryptographic algorithms and protocols for blockchains and smart contracts. The INTER project APLICA entered its second year in 2022 and brought many new insights into the theoretical and practical security of lightweight symmetric cryptosystems, especially authenticated encryption

algorithms. APLICA is a joint research project with the Workgroup for Symmetric Cryptography (Prof. Gregor Leander) of Ruhr-University Bochum. Members of the CryptoLux group published a total of 9 peer-reviewed papers in 2022 and served on the technical program committee of 8 major international journals and conferences in the area of cryptology and information security. The Ph.D. students Giuseppe Vitto and Luan Cardoso dos Santos successfully defended their thesis in January and June 2022, respectively. Dr. Vitto's thesis on "Security, scalability and privacy in applied cryptography" was selected as one of 13 outstanding theses of the Doctoral School of Science and Engineering (DSSE). The CryptoLux group taught various courses in the bachelor and master programs and supervised student projects.

Most interesting achievements in 2022

Members of the CryptoLux group extended and improved a key-recovery framework for differential cryptanalysis, called Meet-in-the-Filter (MiF), which was initially developed in the course of the APLICA project. MiF is suitable for symmetric algorithms with a slow or incomplete diffusion layer, such as ciphers based on the Addition-Rotation-XOR (ARX) design principle. The APLICA team gained more insights into the theoretical and practical aspects of the MiF technique and simplified its application. These advances made it possible to achieve the best-to-date single-key differential attacks against the block cipher families CHAM and KATAN.

CryptoLux developed practical attacks against white-box implementations of ARX-based ciphers using implicit functions and quadratic-affine encodings, which were introduced at CRYPTO 2022. In the white-box model, the attacker is assumed to have direct access to (and full control over) the implementation of a cryptographic algorithm and its execution environment, which includes the ability to tamper with the implementation in any way. The involved CryptoLux researchers found various attacks against the white-box techniques from CRYPTO 2022 that only use the round functions as oracles and do not rely on their description. These attacks were experimentally verified on white-box instances of the lightweight block ciphers Speck-32/64 and Speck-64/128 and led to the conclusion that a single ARX round is too weak to be used as a white-box round.

The CryptoLux group also contributed to an assessment of the efficiency (i.e., execution time and code size) of ten authenticated encryption algorithms on the 32-bit RISC-V platform. These ten algorithms were final-round candidates of the LightWeight Cryptography (LWC) standardization project of the U.S. National Institute of Standards and Technology (NIST). Two implementation options were considered, namely pure software implementation using the RV32B ("BitManip") extension in addition to the base RV32I instruction set and hardware/software co-design where the most performance-critical operations of the underlying low-level primitive were accelerated through the integration of custom instructions. Experimental results showed that, in both implementation
scenarios, the permutation-based designs ASCON, SPARKLE, TinyJAMBU, and Xoodyak are particularly efficient.

Top-3 academic publications in 2022

1. Alex Biryukov, Gleb Naumenko, and Sergei Tikhomirov.
   Analysis and Probing of Parallel Channels in the Lightning Network.
   Financial Cryptography and Data Security - FC 2022, vol. 13411 of Lecture Notes in Computer Science, pp. 337-357, Springer Verlag, 2022.

2. Alex Biryukov, Je Sen Teh, and Aleksei Udovenko.
   Advancing the Meet-in-the-Filter Technique: Applications to CHAM and KATAN.
   Selected Areas in Cryptography - SAC 2022, Lecture Notes in Computer Science, Springer Verlag, 2022.

3. Luan Cardoso dos Santos, François Gérard, Johann Großschädl, and Lorenzo Spignoli.
   Rivain-Prouff on Steroids: Faster and Stronger Masking of the AES.
   Smart Card Research and Advanced Applications - CARDIS 2022, vol. 13820 of Lecture Notes in Computer Science, pp. 123-145. Springer Verlag, 2022.

4.9 Foundations of Model-Driven Engineering (FMDE)

Head of research group: Prof. Dr. Pierre Kelsen

FMDE is a small research group: besides the head (Pierre Kelsen) it comprised 2 members in 2022: Qin Ma (research scientist) and Christian Glodt (research and development specialist). The research group explores fundamental questions in the area of model-driven engineering but also interests itself in concrete applications (e.g., enterprise architecture and smart grids).

Summary of the group's achievements in 2022

In 2022 Pierre Kelsen Pierre Kelsen was teaching the following courses: Algorithms 1 (Binfo), Programming Fundamentals 1 and Algorithms & Complexity (Bics), Formal Methods and Model-Driven Software Development (MICS, two lectures). Pierre KELSEN was heading the Laboratory of Advanced Software SYstems (LASSY) and acting as a member of the staff delegation. At the end of 2022 he took over the direction of the Master in Information and Computer Sciences (MICS).

In 2022, Qin Ma co-organized the 12th International Workshop on Enterprise Modeling and Information Systems Architectures (EMISA 2022) and its affiliated event EE Challenge 2022. Research wise, she continued her collaboration with colleagues from TU Eindhoven, the University of Duisburg-Essen, and the Mexico Autonomous Institute of Technology. In addition to research activities in the field of smart grids initiative valuation and validation and verification of domain specific modeling languages/methods, Qin Ma and her co-authors also extended their activity into the field of regulatory assessment during business development of energy sector projects by capitalizing on contextual requirements engineering techniques. Teaching wise, Qin Ma became the responsible teacher of the Model-Driven Software Development course in the MICS program. In parallel, she kept teaching the lab sessions of the Programming Fundamentals 1 course in the BICS program. Funding application wise, Qin Ma participated in an FNR INTER CORE proposal writing jointly with LIST, TU Wien, and Ghent University. Qin Ma was also a PC member of the 27th International Conference on Exploring Modeling Methods for Systems Analysis and Development (EMMSAD 2022), the 8th International Conference on Future Internet of Things and Cloud (FiCloud 2022), and the 12th International Workshop on Enterprise Modeling and Information Systems Architectures (EMISA 2022).

Christian Glodt continued working on improving the web-based Fudomo tool. He also maintained and improved "Accord", the research information database of the DCS. In addition, he participated in the organisation of lab sessions for the "Programming Fundamentals 1" course and supervised a student project in the "Bachelor in Computer Science (BICS)".

Three most interesting publications in 2022

1. Sybren de Kinderen, Monika Kaczmarek-Heß, Qin Ma, and Iván S. RazoZapata. "Model-based valuation of smart grid initiatives: Foundations, open issues, requirements, and a research outlook". In: Data and Knowledge Engineering 141 (2022).

2. Qin Ma, Monika Kaczmarek-Heß, and Sybren de Kinderen. "Validation and verification in domain-specific modeling method engineering: an integrated life-cycle view". In: Software and Systems Modeling (2022).

3. Sybren de Kinderen, Qin Ma, Monika Kaczmarek-Heß, and Rik Eshuis. "Beyond Business Development: Regulatory Assessment of Energy Sector Projects with Contextual Requirements Engineering". In: Lecture Notes in Business Information Processing. Springer, 2022, pp. 183–198.

4.10   Individual and Collective Reasoning Group (ICR)

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

ICR is part of the Interdisciplinary Lab for Intelligent and Adaptive Systems in DCS and pursues a dedicated cross-disciplinary perspective. It collaborates in particular with the Departments of Philosophy and Law, the C2DH, SnT, and LIST, and is strongly connected to leading international research centres, like the Institute of Logic and Computation at TU Vienna, or the Institute for Logic and Cognition at Zhejiang University in Hangzhou. The main research areas are Normative reasoning in multi-agent contexts, Computational Law, AI and Ethics, Defeasible inference, Formal Argumentation, and Explainable AI, with a growing interest in Neuro-symbolic computation. ICR is also a driving force behind the AI Robolab of the DCS.

Summary of the group's achievements in 2022

ICR hosted in 2022 20 researchers: 1 full professor, 1 visiting professor, 2 research scientists, 7 postdocs, 1 R&D specialist, and 9 PhD students. The year 2022 was furthermore marked by several important career steps.

Réka Markovich, who enriched the ICR project portfolio multiple times, was promoted to become a research scientist with her own independent research group within DCS: "Computational Law and Machine Ethics (CLAiM)", an area whose importance is well recognized in Luxembourg.

Amro Najaar, who was heading the AIRobolab activities, accepted a permanent position as a senior researcher at LIST. This allows him to continue his fruitful collaboration with ICR and to help implementing the strategic goal of strengthening the links between LIST and UL. In particular, together with Igor Tschappi, the current responsible for the AIRobolab, he is active in the FNR INTER project EXPECTATION, concerned with personalized XAI in the context of decentralized knowledge.

Leon van der Torre himself was granted a prestigious "Bao Yugang Chair" visiting professorship at Zhejiang Univ, strengthening the existing ZLAIRE collaboration thread.

Emil Weydert, together with Alexander Steen, a former ICR member now professor in Greifswald, launched the "Dov Gabbay Prize for Logic and Foundations" to honour the tremendous role of ICR's long-term visitor. The jury consists of top European researchers covering all areas of Logic.

Aleks Knoks acquired, together with Thomas Raleigh from Philosophy, a well-targeted FNR Core project: "The Epistemology of AI Systems (EAI)". He was also invited to teach the course "Defeasible Logics with Applications to Normative Systems and Philosophy" at the prominent European Summer School for Logic, Language, and Information (ESSLLI 2022) at Galway.

Pere Pardo hit the ground running by developing (supported by Emil Weydert) a new multi-faceted course in Knowledge Representation and Reasoning (Intelligent Systems II) for the 3rd year of the BICS.

Christian Franck joined ICR as a research scientist. His software engineering experience is crucial for the computational realization and testing of the theoretical accounts developed and investigated in the group.

The arrival of Davide Liga extended the research scope from argumentative reasoning and argument mining to argument generation using language transformer models (see Chat-GPT), with a specific focus on legal reasoning.

Sana Nouzri has been heavily involved in the Computational Creativity Hub, which is using AI&Art as an icebreaker for presenting the emerging AI-world. The CCH was established in the context of Esch2022 and became the flagship of DCS outreach activities in 2022. In particular, she organized highly successful visits, educational events, and workshops for students, scientists, business people, and high-level societal stakeholders.

The AURELEE project was concluded with a major event, the "Workshop on Automated Reasoning with Legal Entities" in July. It brought together leading figures in Automated Theorem Proving and was combined with an extended doctoral course to educate the next generation.

A crucial event for the research program of ICR was also the publication of the "Handbook of Legal AI" in 2022, edited by Leon van der Torre and former members of ICR. Some relevant publications:

G. Casini, L. Robaldo, L. van der Torre, S.Villata (eds). *Handbook of Legal AI.* College Publications, 2022.

Huimin Dong, Beishui Liao, Réka Markovich, Leon van der Torre. *Defeasible Deontic Logic: Arguing about Permission and Obligation.* Journal of Applied Logics 9(4):1025-1086, 2022.

Wolfgang Dvorák, Tjitze Rienstra, Leon van der Torre, Stefan Woltran. *Non-Admissibility in Abstract Argumentation.* COMMA 2022, pp. 128-139, 2022.

Pere Pardo, Christian Straßer. Modular orders on defaults in formal argumentation. Journal of Logic and Computation, OUP 2022.

Aleks Knoks. *Conciliatory views, higher-order disagreements, and defeasible logic.* Synthese 200(2), 173: 1–23, Springer 2022.

4.11   Knowledge Discovery and Mining (MINE)

Head of research group: Prof. Christoph Schommer

Description: MINE is a research group with an interdisciplinary approach to research and act as a bridge and research facilitator for the field of Artificial Intelligence and in particular in the application of Machine Learning and Natural Language Processing. We collaborate with colleagues from all 3 faculties as well as with colleagues from C2DH, Scienteens Lab, and our industry partners such as LuxAI, European Investment Bank, Script, and CISCO.

Activities:
The year 2022 was mainly marked by the cultural year 'Esch 2022 - European Capital of Culture' and the related 12 projects (software developments; cooperation with LuxAI) carried out at the AI&Art Pavilion by researchers, students, and artists. We welcomed several professors, such as Prof. Manuela Naveau and her team from the Art University Linz + Ars Electronica, Prof. Yolanda Spinola, Guest Professor of the University of Seville, and Prof. Tim Landgraf, FU Berlin, several national and international artists (e.g., Sergio Albia, Barcelona), H.E. Stephan Müller, Ambassador of the Grand Duchy of Luxembourg in Belgium and H.E. Thomas Lambert, Ambassador of the Kingdom of Belgium in Luxembourg, the Business Club Belgium-Luxembourg (BCBL) and the Belgian Business Club Luxembourg (BBCL), and a number of Luxembourg Associations such as Arcus and WIDE. We also organised a 3-day hybrid conference AIFA (AI and the Future of Arts) in November 2022 with 40 speakers from 11 countries. Besides, many interviews with press (newspaper, radio), podcasts, and photo shootings rounded off this great cultural year.

Several new members joined the research group: Aria Nourbaksh (PhD candidate, Project C21, with CISCO and SCRIPT), Yasi Yousefi and Faria Ferooz (both PhD candidates, Project Last-JD with University of Bologna), and Dr Salima Lamsiyah (PostDoc researcher). Prof. Schommer became a member of the FNR PRIDE project 'Deep Data Science of Digital History' (PI: Prof. Fickers, C2DH), the IBPG project 'C21' (PI: Prof. Koenig, FHSE)

In teaching, we organised two doctoral workshops: 'Machine Learning for Art Production' (Prof. Schommer) and 'Innovation in Art History for interdisciplinary research' (Egberdien van der Peijl). On Master level, 3 courses in Data Science, Information Retrieval, and Machine Learning were performed with 100 students in total; on Bachelor level, we offered 2 Bachelor courses in Database Management and Natural Language Processing (this was done by Dr Salima Lamsiyah). Finally, Prof. Schommer made an integrative contribution to courses in Finance, Philosophy and Medicine and gave a 20h course at the University of Singapore (SUTD).

4 Master's students defended their dissertation projects or more than 5 Bachelor's students defended their dissertation projects. At the end of the year, the MINE consisted of 1 professor, 1 PostDoc researcher and 6 PhD students. 5 doctoral students were co-supervised.

Publications:

- Nina Hosseini Kivanani et al.: A comparative study of automatic classifiers to recognize speakers based on fricatives. 1st Interdisciplinary Conference on Voice Identity (VoiceID): Perception, Production, and Computational Approaches, Zurich, Switzerland. 4-6 July 2022.
- Nina Hosseini Kivanani et al.: IRRMA: An Image Recommender Robot Meeting Assistant. 20th International Conference on Practical Applications of Agents and Multi-Agent Systems (PAAMS). 13-15 July 2022.
- Nina Hosseini Kivanani et al.: The Prosody of Cheering in Sport Events. Interspeech 2022, 18-22 September 2022.
- Nina Hosseini Kivanani et al.: XAI: Using Smart Photobooth for Explaining History of Art. International Conference on Human-Agent Interaction, 5-8 December 2022, Christchurch, New Zealand.
- C. Schommer et al.: Deep Mining Covid-19 Literature. Applied Informatics, 5th International Conference, ICAI 2022, Arequipa, Peru, 27-29 October, Springer Cham.

4.12   Parallel Computing and Optimisation Group (PCOG)

Head of research group: Prof. Dr. Pascal Bouvry

Deputy Head of research group: Dr. Grégoire Danoy

Solving today's scientific and real-world problems not only requires High Performance Computing (HPC), but also new generations of Artificial Intelligence algorithms. PCOG conducts research in parallel computing, search and optimisation techniques, to provide efficient, scalable and robust solutions to state-of-the-art, large-scale discrete/combinatorial problems. The main application domains are security, trust and reliability; reliable scheduling and routing on new generations of networks; sustainable development and systems biomedicine; unmanned autonomous vehicles (UAV), smart cities. In addition, PCOG is at the heart of the digital strategy of the university by managing the HPC-related developments and the associated facility since 2007. Detailed information about the group is available at http://pcog.uni.lu/.

Summary of the group's achievements in 2022

At the end of 2022, PCOG counted 25 members (1 professor, 3 research scientists, 1 partnership development officer, 1 project officer, 7 postdocs, 8 PhD students, 1 R&D Specialist,

1 team coordinator, 2 infrastructure engineers) and produced a total of 16 peer-reviewed publications (4 journal articles, and 12 conference articles) and 2 books. In 2022, two PhD students defended their theses entitled « On Trustworthy AI and Localized Complex Network Analytics» and «The European Legal Approach to Open Science and Research Data».

PCOG has run five research projects in 2022.The second ILNAS/ANEC Research Programme which focuses on the Aerospace, ICT and Construction pillars, the FNR CORE ADARS (Automating the Design of Autonomous Robot Swarms), the FNR CORE COMOC (A Concurrent Model of Computation for Trustworthy GPU Programming), the FNR CORE CBD (Cloud-based Computational Decision By Leveraging Artificial Ultra Intelligence) and the H2020 PRACE-6IP, the 6th implementation phase of the « Partnership for Advanced Computing » which is a permanent pan-European High Performance Computing service.

PCOG acquired three new research projects in 2022: (1) FNR/ANR INTER ADHOC (High Performance Decomposition Algorithms for Combinatorial Optimization and Machine Learning, 2023-2026) ; (2) FNR/ANR INTER UltraBO (Ultra-scale Computing for solving Big Optimization Problems, 2023-2026) and FNR POLLUX SERENITY (SpacE data bRokEriNg optImizaTion sYstem, 2023-2026).

PCOG was selected by the EuroHPC Joint Undertaking to design and implement the first pan-European Master's programme in HPC (EUMaster4HPC), leading a consortium of European universities, research/supercomputing centres and industrial partners. The first cohort of students started in September 2022.

PCOG also manages the Master in Technopreneurship (MTECH), in partnership with ILNAS (Luxembourg's standards body), the Luxembourg Lifelong Learning Center (LLLC) and the Chambre des Salariés Luxembourg (CSL).

PCOG team members taught in several Bachelor, Master and PhD programs (BICS, BINFO, MICS, MTECH, Doctoral School in Computer Science), and organized the HPC workshop.

PCOG is in charge of the management of the High-Performance Computing (HPC) facility of the University, those developments as well as the associated expert IT team managing and supporting it, are led by Pascal Bouvry who is acting as "Chargé de Mission auprès du Recteur". The University of Luxembourg, Luxprovide and Luxinnovation also joined forces to become the national HPC competence centre as part of the EURO-HPC network.

Three high impact publications in 2022

1. **Talbot, P., Pinel, F. G., & Bouvry, P.** (2022). A Variant of Concurrent Constraint Programming on GPU. *Proceedings of the AAAI Conference on Artificial Intelligence, 36*(4), 3830-3839. https://doi.org/10.1609/aaai.v36i4.20298

2. **Felten, F.; Danoy, G.; Talbi, E. and Bouvry, P.** (2022). Metaheuristics-based Exploration Strategies for Multi-Objective Reinforcement Learning. In *Proceedings of the 14th International Conference on Agents and Artificial Intelligence - Volume 2: ICAART*; SciTePress, pages 662-673. DOI: 10.5220/0010989100003116 – **Best Student Paper Award Nomination**

3. **Nunes Alegre, L., Felten, F., Talbi, E-G., Danoy, G., Nowé, A., Bazzan, A., & C. da Silva, B.** (2022). MO-Gym: A Library of Multi-Objective Reinforcement Learning Environments. In *Proceedings of the 34th Benelux Conference on Artificial Intelligence BNAIC/Benelearn 2022*

4.13 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 designing and implementing proactive computing principles into the development of innovative autonomic software systems for multiple 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 2022

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

Top academic publication in 2022

Samira Chaychi, Sandro Reis and Denis Zampuniéris. Software Model for Robot Programming and Example of Implementation for Navigation System. In Proc. IEEE 9th International Conference on Automation, Robotics and Applications (ICARA 2023), March 2023.

In this paper, we consider a problem which is the lack of separation of concerns in robotic systems, and we propose a software model to address it and solve the current challenges. This model is based on proactive scenarios, coded through dynamic sets of condition-action rules. Each scenario embeds the required rules and can be assembled dynamically with others, allowing the proactive system to achieve a unique objective or behavior and instruct the robot accordingly. Furthermore, a scenario is not aware of the existence of the other scenarios. In fact, it only contains information about a predefined central scenario, which oversees global decision making. We use ROS, the main robotic operating system, to help us to implement the robot simulator and test the model.
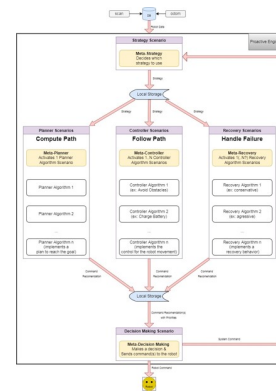
4.14 Security and Networking Lab (SECAN-Lab)

Head of research group: Prof. Dr. Thomas Engel

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

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

Headed by Prof. Dr. Thomas Engel, SECAN-Lab is composed of a balanced team of established high-level research associates, doctoral candidates and research management professionals spanning across a variety of fields, and with many contributing with a significant industry expertise gained at both national and international levels.

Summary of the group's achievements in 2022

In 2022, SECAN-Lab conducted research in the scope of 7 publicly and industry-funded projects. In particular, we were able to win two new projects during this year, CANDI and FNA, allowing us to consolidate our research on communication in 5G networks. The

INTER project CANDI, funded by ANR and FNR, focuses on Fifth generation (5G) cellular networks, which are currently being widely deployed across the world, connecting not only traditional users of mobile broadband networks, but also billions of Internet of Things (IoT) devices, while supporting a wide range of novel services, applications, and vertical industries. An important feature of 5G is the capability of two neighboring IoT devices to communicate directly (i.e., via D2D – device-to-device communication), even in the absence of a base station. In the current standard specifications, this feature is limited to 1-hop communication only. However, many emerging verticals, such as Smart Factories, Smart Farming, Public Safety, and others, require more extensive coverage and better energy efficiency. This can be achieved by allowing IoT devices to adjust their transmit power and possibly communicate their information via multi-hop D2D relaying. The Cellular Ad Hoc Networking for Decentralized IoT Architectures (CANDI) project will address this issue by developing multi-hop ad hoc communications using cellular technology. The project will build on existing D2D specifications and standards and leverage recent cellular innovations, as well as wireless ad hoc network concepts, in order to enable multi-hop relaying for next-generation decentralized cellular networks. The Erasmus+ project FNA- Future Network Academy, with academic partners, aims to provide educational resources to different levels (undergraduates and in-service training) and to different audiences (scientific students, entrepreneurs students, policymakers), beyond the natural audience of network specialists.

We successfully completed the EU projects HiedTec and 5G-MOBIX. HiedTec had the main aim of developing concepts for adapting the educational system to the digital generation while considering the specific conditions of each partner country and creating centers for innovative educational technologies Secan-lab's research group contributed mainly to the creation of a sustainable academic network for sharing experiences and exchanging good practices in the field of innovative educational technologies and didactic models. The project finished in December 2022 with the Final Evaluation report, where methodology, quality of results, guidance and overall project outputs were evaluated by Secan-lab. 5G-MOBIX focused on the worldwide 5G Fora and verticals in the V2X ecosystem to generate some genuine exchange among the leaders of these ecosystems. The project has been very successful at creating, initiating, and attracting worldwide 5G Fora executives to work together since 2018. In 2022, Secan-lab successfully completed the main task, deliverable D7.6, and presented it in front of the EU officers during the project's final event.

We also continued working on the EU project CITIES2030, the INTER 5G-INSIGHT project, and the FNR Bridge SETICA project. Cities2030 enables cities and regions to improve food system resilience via a participative approach and generate short supply chains driven by local investments. The blockchain technology for the food chain and sentiment analyses is Secan-lab's contribution. In 2022, the major contribution of Secan-lab was developing a sentiment analysis solution for the project, data security, and blockchain security. 5G-INSIGHT aims to provide security solutions for 5G and beyond vehicular networks with a particular focus on cross-border areas (i.e., the France-Luxembourg border-crossing case). In 2022, SECAN-lab worked to conclude the study on the security challenges of 5G-V2X at the cross border, which contributed to completing the task that SECAN-lab led and closing a work package. SECAN-lab significantly progressed in the work package it led. SECAN-lab has employed deep and federated learning for developing mechanisms to detect intra-slice and inter-slice attacks for 5G-Vehicle-to-everything (V2X) sliced networks. SECAN-lab has also successfully collaborated with other partners in the consortium to propose two contributions regarding detecting V2X attacks at the edge and 5G-V2X testbed. The goal of SETICA is to develop an automotive Time Sensitive Networking (TSN) profile which includes answering challenging research questions and a thorough evaluation. In 2022, Secan-lab built a gPTP-based physical testbed, which allowed to complete of tasks related to (i) the

evaluation of high-risk attacks, ii) the evaluation of gPTP-compliant security controls, and iii) the evaluation of an intrusion detection system for gPTP. Secan-lab has also initialized a work related to the creation of a risk matrix for automotive TSN.

All findings were published in project deliverables, and research papers, and presented in various workshops and conferences. Specifically, in terms of academic contributions, SECAN-Lab has also been very successful in 2022 with 21 publications in international workshops, conferences, journals, and books. Team members were involved as (Co-)Chairs or program committee members in 7 international conferences and workshops, including the Privacy Enhancing Technologies Symposium (PETS), the ACM Conference on Computer and Communication Security, the IEEE Global Communications Conference (GLOBECOM), and the IEEE International Conference on Communications.

Regarding our educational mission, team members have taught extensively within the University of Luxembourg's BSc and MSc programs and supervised numerous bachelor and master student projects and theses.

Three most interesting publications in 2022

1. Valerie Fetzer, Marcel Keller, Sven Maier, Markus Raiber, Andy Rupp, Rebecca Schwerdt: PUBA: Privacy-Preserving User-Data Bookkeeping and Analytics. Proc. Priv. Enhancing Technol. 2022(2): 447-516 (2022)

   In this paper we propose Privacy-preserving User-data Bookkeeping & Analytics (PUBA), a building block destined to enable the implementation of business models (e.g., targeted advertising) and regulations (e.g., fraud detection) requiring user-data analysis in a privacy-preserving way. In PUBA, users keep an unlinkable but authenticated cryptographic logbook containing their historic data on their device. This logbook can only be updated by the operator while its content is not revealed. Users can take part in a privacy-preserving analytics computation, where it is ensured that their logbook is up-to-date and authentic while the potentially secret analytics function is verified to be privacy-friendly. Taking constrained devices into account, users may also outsource analytic computations (to a potentially malicious proxy not colluding with the operator). We model our novel building block in the Universal Composability framework and provide a practical protocol instantiation. To demonstrate the flexibility of PUBA, we sketch instantiations of privacy-preserving fraud detection and targeted advertising, although it could be used in many more scenarios, e.g. data analytics for multi-modal transportation systems. We implemented our bookkeeping protocols and an exemplary outsourced analytics computation based on logistic regression using the MP-SPDZ MPC framework. Performance evaluations using a smartphone as user device and more powerful hardware for operator and proxy suggest that PUBA for smaller logbooks can indeed be practical.

2. Abdelwahab Boualouache and Thomas Engel. "Federated learning-based scheme for detecting passive mobile attackers in 5g vehicular edge computing." Annals of Telecommunications (2022): 1-20.

   Detecting passive attacks is always considered difficult in vehicular networks. Passive attackers can eavesdrop on the wireless medium to collect beacons. These beacons can be exploited to track the positions of vehicles not only to violate their location privacy but also for criminal purposes. In this paper, we propose a novel federated

learning-based scheme for detecting passive mobile attackers in 5G vehicular edge computing. We first identify a set of strategies that can be used by attackers to efficiently track vehicles without being visually detected. We then build an efficient machine learning (ML) model to detect tracking attacks based only on the receiving beacons. Our scheme enables federated learning (FL) at the edge to ensure collaborative learning while preserving the privacy of vehicles. Moreover, FL clients use a semi-supervised learning approach to ensure accurate self-labeling. Our experiments demonstrate the effectiveness of our proposed scheme to detect passive mobile attackers quickly and with high accuracy. Indeed, only 20 received beacons are required to achieve 95% accuracy. This accuracy can be achieved within 60 FL rounds using 5 FL clients in each FL round. The obtained results are also validated through simulations.

3. Alessio Buscemi, Ion Turcanu, German Castignani, and Thomas Engel. Preventing Frame Fingerprinting in Controller Area Network Through Traffic Mutation. In 2022 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 385-390). IEEE.

The continuous increase of connectivity in commercial vehicles is leading to a higher number of remote access points to the Controller Area Network (CAN) - the most popular in-vehicle network system. This factor, coupled with the absence of encryption in the communication protocol, poses serious threats to the security of the CAN bus. Recently, it has been demonstrated that CAN data can be reverse engineered via frame fingerprinting, i.e., identification of frames based on statistical traffic analysis. Such a methodology allows fully remote decoding of in-vehicle data and paves the way for remote pre-compiled vehicle-agnostic attacks. In this work, we propose a first solution against CAN frame fingerprinting based on mutating the traffic without applying modifications to the CAN protocol. The results show that the proposed methodology halves the accuracy of CAN frame fingerprinting.

4.15   Security and Trust of Software Systems (SaToSS)

Head of research group: Prof. Sjouke Mauw

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

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

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

Summary of the group's achievements in 2022

In 2022, the SaToSS group counted 18 researchers (1 professor, 1 assistant professor, 8 post-docs, 8 PhD students). The group had 9 externally funded projects: 2 FNR INTER projects (SURCVS on secure voting systems, and SLANT on NLP security), 2 FNR PRIDE projects (SP-squared on deep learning, and DRIVEN on social analysis) , 2 AFR projects (PriML on privacy in machine learning, and ATTEST on secure attestation and erasure of remote memory), 1 project funded by ESA (ATMonSAT on CubeSat security), 1 FNR CORE project (HETERS for privacy preservation in social networks) and 1 IAS project aiming to promote interdisciplinary research (GENERIC for gene network disovery). The group has also secured fundings of an FNR CORE project AVVA which will start in 2022 for privacy verification in E-voting. In 2022, the group has successfully completed the FNR INTER project SLANT and the ESA project ATMonSAT. The group has contributed to the organization of a number of scientific events (e.g., VTSA 2022). In 2022, SaToSS continued its active involvement in teaching and student supervision for bachelor and master programs in Computer Science (BINFO, BICS, MICS, MSSI). The group also continues its high visibility in high-ranking academic venues (e.g., CSF and NeurIPS)

Three most interesting publications in 2022

1. **Is eve nearby? analysing protocols under the distant-attacker assumption. Reynaldo Gil-Pons, Ross Horne, Sjouke Mauw**, Alwen Tiu, and Rolando Trujillo, in Proceedings of the 35th IEEE Computer Security Foundations Symposium (CSF): 17-32.
   Abstract: Various modern protocols tailored to emerging wire-less networks, such as body area networks, rely on the proximity and honesty of devices within the network to achieve their security goals. However, there does not exist a security framework that supports the formal analysis of such protocols, leaving the door open to unexpected flaws. In this article we introduce such a security framework, show how it can be implemented in the protocol verification tool Tamarin, and use it to find previously unknown vulnerabilities on two recent key exchange protocols.

1. **Unlinkability of an improved key agreement protocol for emv 2nd gen payments. Ross Horne, Sjouke Mauw, and Semen Yurkov**, in Proceedings of the 35th IEEE Computer Security Foundations Symposium (CSF): 348-363.
   Abstract: To address known privacy problems with the EMV standard, EMVCo have proposed a Blinded Diffie-Hellman key establishment protocol, which is intended to be part of a future 2nd Gen EMV protocol. We point out that active attackers were not previously accounted for in the privacy requirements of this proposal protocol, and demonstrate that an active attacker can compromise unlinkability within a distance of 100cm. Here, we adopt a strong definition of unlinkability that does account for active attackers and propose an enhancement of the protocol proposed by EMVCo. We prove that our protocol does satisfy strong unlinkability, while preserving authentication.

1. **Iterative structural inference of directed graphs. Aoran Wang, Jun Pang**, In Proceedings of the 36th Annual Conference on Neural Information Processing Systems (NeurIPS).
   Abstract: In this paper, we propose a variational model, iterative Structural Inference of Directed Graphs (iSIDG), to infer the existence of directed interactions from observational agents' features over a time period in a dynamical system. First, the iterative process in our model feeds the learned interactions back to encourage our model to

eliminate indirect interactions and to emphasize directional representation during learning. Second, we show that extra regularization terms in the objective function for smoothness, connectiveness, and sparsity prompt our model to infer a more realistic structure and to further eliminate indirect interactions. We evaluate iSIDG on various datasets including biological networks, simulated fMRI data, and physical simulations to demonstrate that our model is able to precisely infer the existence of interactions, and is significantly superior to baseline models.

4.16   Security, Reasoning and Validation (SerVal)

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

The SerVal – SEcurity, Reasoning and VALidation Research Group is headed by Professor Yves Le Traon and mixes researchers from SnT and DCS. SerVal conducts research on Software Engineering and Software Security, with a focus on data intensive, mobile and complex systems.

Researchers in the team leverage various techniques around three main pillars including:

• Software Testing (Mutation Testing, Search-Based Testing, ...)
• Data Analytics, predictive and prescriptive techniques (Decision Support Services)
• Machine Learning System Engineering and Security

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 next generations of information systems for banking and public administration, IoT, Fintech, Industry 4.0, and Smart Grid infrastructures.

Summary of the group's achievements in 2022

SerVal has been successful in several dimensions in 2022.

The scientific group has now a steady size of around 35 researchers and published 30 papers in top venues (rank A*) such as ICSE, TSE, EMSE, ECCV, IJCAI, AAAI. This represents the double of 2021, which was still marked by COVID. More importantly, 2022 marked an important milestone in SERVAL efforts in AI (Artificial Intelligence) research with its first publications in the field top venues. Alongside those achievements, an excellent thesis award from the university was awarded to a defending PhD student directly involved in those successes.

In project acquisition, SERVAL pursued its successful partnership with Luxemburgish (Creos, CEBI, BGL) and international (Paypal) actors but also secured new collaborations (Ceratizit, STATEC). SERVAL also acquired several FNR project fundings (1AFR, 1 CORE, 1 Bridge, 2 JUMP) and was part of the consortium of two successful Horizon Europe projects and one ERASMUS+.

Main publications and achievements in 2022

1. Martin Gubri, Maxime Cordy, Mike Papadakis, Yves Le Traon, Koushik Sen: LGV:nBoosting Adversarial Example Transferability from Large Geometric Vicinity.

ECCV (4) 2022: 603-618 Computer Vision–ECCV 2022: 17th European Conference, Tel Aviv, Israel

2. Salah Ghamizi, Maxime Cordy, Mike Papadakis, Yves Le Traon: Adversarial Robustness in Multi-Task Learning: Promises and Illusions. AAAI 2022: 697-705

3. Aayush Garg, Renzo Degiovanni, Matthieu Jimenez, Maxime Cordy, Mike Papadakis, Yves Le Traon:Learning from what we know: How to perform vulnerability prediction using noisy historical data. Empirical Software Engineering 27 (7), 169

4. Multi-objective Robust Machine Learning For Critical Systems With Scarce Data: **Excellent thesis award**, Salah Ghamizi.

4.17 Software engineering and Artificial intelligence Group on Ecosystem management (SAGE)

Head of research group: Prof. Dr. Nicolas Guelfi

General information

We are announcing the creation of SAGE, a new research group part of the LASSY laboratory. Our group focuses on methods and tools for Software Engineering and Artificial Intelligence applied to ecosystem management IT systems. Ecosystem management encompasses plenty of society-critical software applications, e.g. decision-making applications for restoration of degraded ecosystems, monitoring and prediction software applications for the natural ecosystem disruptions (flood, forest fire, etc.). In this critical context, our group focuses on the development of rigorous methods, and open-source tools to deal with the large amount of heterogeneous Earth Observation data. Moreover, our group studies the integration of artificial intelligence in the software engineering research area. We develop open source tools to support our languages and to allow for research collaboration or technology transfer with industrial partners, policymakers, governmental and non-governmental organizations. SAGE aims to offer novel and efficient approaches for engineers to ensure the rigorous system development of ecosystem management software applications based on artificial intelligence. Specific fields are currently under important development:

• software engineering methods and tools for neural networks engineering
• software engineering methods and tools for natural ecosystems restoration

A new lecture on the SAGE topics has been pre-designed, submitted and accepted to be included in the 3rd semester of the MICS - Master in Computer Science for 2023/2024.

Highlights in 2022

The sabbatical of professor Nicolas Guelfi took place from February 15 to August 15, 2022 at the Center Universitaire Informatique of the University of Geneva. The main collaborations took place with the professors Didier Buchs and Giovanna di Marzo as well as the members of their teams. During the period of the sabbatical leave, the activities and the results can be summarized in four points :

1. Contribution to local education: the teams he has been collaborating with were in charge of several bachelor and master courses. He has been integrated in the teaching team that allowed him to observe and partly contribute to the concerned courses. He also had the opportunity to be part of the mid-term PhD thesis jury of the PhD students which are under the supervision of Professor Didier Buchs.

2. Contribution to Requirements Engineering Methodologies: he has been working on a journal paper on MESSIR which is a Flexible Scientific Approach to Requirements Engineering.

3. Software Engineering for Deep Learning exploration: he has explored the state of the art on deep learning systems engineering both on the scientific aspect and on the technical one.

4. Tasks for University of Luxembourg: he spent one third of my sabbatical on tasks that concerned the courses he is in charge of at University of Luxembourg that he treated remotely.

Another highlight was the creation of a new lecture in the first semester of the BiCS for the introduction to BiCS students on the Bachelor Semester Projects expected work and deliverables.

Last but not least, a new Doctoral Candidate, Tiago Sousa has joined the team on the topic of Ecosystem Resilience Analysis with Alloy, Model-Driven Engineering and Deep Learning. Inline with the new SAGE team purpose.

Three most interesting publications (or other achievements) in 2022

1. Guelfi Nicolas. "The MESSIR Flexible Scientific Approach to Requirements Engineering". Software 1(1):80-106. March 2022. This paper presents and defines the MESSIR methodology, a flexible scientific approach to requirements engineering. The MESSIR methodology has been used for teaching at bachelor and master-level in the last 10 years in the team of professor N. Guelfi.

2. Launch of a new lecture for BiCS semester 1 students to introduce them to the concepts and rules of Bachelor Semester Projects. The intention of this new lecture is to prepare fresh students about the further bachelor semester projects by practicing step-by-step parts of the mandatory deliverables, i.e. scientific & technical report.

3. Research project for the sabbatical of Prof. N. Guelfi. The aim and motivation of this sabbatical is to extend his research domain to the learning domain and the artificial intelligence mainly related to deep learning with neurons in order to set the basis for a novel methodological approach for the engineering of intelligent systems.

4.18   Systems and Control Engineering (SCE)

Head of research group: Prof. Dr. Jürgen Sachau

The Systems and Control Engineering group is affiliated to the department of computer science, as member of the European Distributed Energy Resources Laboratories (DERlab) sharing labs with Electrical Engineering. The works are devoted to power systems and control technology for reliable large-scale grid integration of renewable energies, including storage and sector-coupling for thermal and transport energy.

Summary of the group's achievements in 2022

With progressing feed-in of renewable energies (RE), sector coupling and electrification of mobility, balancing in the power grid structures is evolving, in cooperation of short-term storage, intermediate storage and long-term storage or backup. The extended foundations for reinforcing the power network structures with inverter-coupled storage in view of

- avoidance of overloads in the grid structure
- maintaining voltage quality and reliable protection
- decentral phase stability, complementing frequency control by large generators
- decoupling smart grid stability and blackout bridging from cybersecurity
- locally interacting energy balance controls for RE, demand side management and sector coupling and
- providing flexibility in control and energy markets

are completing.

For both radial and meshed power grid configurations, cost and time intensive network enlargement with substations and cables can be avoided resp. deferred. Cooperative distributed balancing and control is thus fostering grid integration of renewable power generation and sector coupling towards climate neutrality, as for Luxembourg's National Energy and Climate Plan.

Cooperation with Eurosolar and the Swiss Solar Agency have been continued with Prof. Sachau as member of the Norman Foster PlusEnergyBuildings committee and the Eurosolar Solarprize committee. In extension of previous work as scientific officer of DG Research, Brussels and of the EC-JRC Energy Institute, Ispra, and his recent delegation, Prof. Sachau has further elaborated on the standards established. Detailed analysis reveals coverage with and performance of distributed storage in the grid structures, giving feedback to both storage and distribution system operators. It allows for investment planning, project development and follow-up in line with the EC guidelines.

Consultations with Luxembourg's grid operator, its Haut Commissariat Protection Nationale and the Market Regulator are concluded, as well as alignment of data methods for spatial and temporal aggregation by Eurostat, Luxembourg, and for the European Investment Bank, Luxembourg.

4.19   Team Leprévost

LACS : Prof. Dr. Franck Leprévost & Ali Osman Topal (Post-Doc) & Raluca Chitic (PhD Student) & Enea Mancellari (PhD Student)

Summary of the achievements in 2022

The composition of the group evolved in 2022. Raluca Chitic's contract terminated in August, and she successfully defended her PhD on October 13th, 2022. We looked for a new PhD student, what led to the arrival of Enea Mancellari mid-November 2022.

In terms of publications, the two tutorials released in 2021 by F. Leprévost underwent a thorough revision during summer 2022, and a new tutorial was written and published in parallel. Three articles in conferences or journals of computer science were accepted and published. Two other articles were published on different topics: one is a position paper

about the role of universities in the time of wokism, and the other is an application of logic to a statement made in art history.

Talks:

- Ali Osman Topal, "Strategy and Feasibility Study for the Construction of High-Resolution Images Adversarial against Convolutional Neural Networks". Presentation to the *14th Asian Conference on Intelligent Information and Database Systems, ACIIDS 2022, Ho Chi Minh City, Vietnam, November 28-30, 2022*

List of published articles:

1. Franck Leprévost, Ali Osman Topal, Elmir Avdusinovic, and Raluca Chitic. Strategy and Feasibility Study for the Construction of High-Resolution Images Adversarial against Convolutional Neural Networks. *Intelligent Information and Database Systems – 14th Asian Conference, ACIIDS 2022, Ho Chi Minh City, Vietnam, November 28-30, 2022*, Proceedings Part I, p. 285-298. LNAI 13757, Springer (2022). https://link.springer.com/content/pdf/10.1007/978-3-031-21743-2_23?pdf=chapter%20toc

1. Raluca Chitic, Ali Osman Topal, and Franck Leprévost. Empirical perturbation Analysis of Two Adversarial Attacks: Black-Box versus White-Box. Appl. Sci. 2022, 12, 7339, C*omputing and Artificial Intelligence, Special Issue "Explainable Artificial Intelligence",* https://doi.org/10.3390/app12147339 (2022). https://www.mdpi.com/2076-3417/12/14/7339

1. Franck Leprévost, Ali Osman Topal, Elmir Avdusinovic, and Raluca Chitic. A Strategy creating High Resolution Adversarial Images against Convolutional Neural Networks, and a Feasibility Study on 10 CNNs. *Journal of Information and Telecommunication*, (2022). https://doi.org/10.1080/24751839.2022.2132586
https://www.tandfonline.com/doi/full/10.1080/24751839.2022.2132586

2. Franck Leprévost. Raison d'être des universités occidentales à l'heure du wokisme. *Causeur*, 19/2/2022
https://www.causeur.fr/raison-detre-des-universites-occidentales-a-lheure-du-wokisme-225081

3. Franck Leprévost. Le de La Tour italien de Cuzin – Une réflexion logique sur l'avéré en histoire de l'art.
Arts et Sciences, Volume 6, N° 4 (2022) https://www.openscience.fr/Le-de-La-Tour-italien-de-Cuzin-Une-reflexion-logique-sur-l-avere-en-l-histoire-2321

List of publications - Books:

- Franck Leprévost. *Order Matters! A Hands-On Tutorial on Linear Algebra.* Ed. Amazon. ISBN : 139798595860642 (2021, revised edition 2022).
- Franck Leprévost. *How Big is Big? How Fast is Fast? A Hands-On Tutorial on Mathematics of Computation.* Ed. Amazon (2021, revised edition 2022).
- Franck Leprévost. *What Counts? A Hands-On Tutorial on Calculus.* Ed. Amazon (2022).

4.20   Team Müller

Head of research group: Prof. Dr. Volker Müller

Volker Müller is interested in algorithmic aspects of common number-theoretic problems – especially about a simultaneous version of the classical Chinese Remainder Theorem (CRT). Research on the Simultaneous Chinese Remaindering (S-CRT), a generalization of the well-known Chinese Remainder Theorem popular in number theory, has been continued and several new small (mostly theoretical) improvements could be proven. A thorough statistical analysis of simulated data was done which led to new insights. The examinations finally lead to the theorem that S-CRT is in its general form NP-hard, which appeared in Jim's dissertation. In addition, a link between the S-CRT and the integer factorization problem was detected. Both these observations are currently investigated further to see their potential impact on practical algorithms. In 2022, Jim Barthel could finally finish his PhD research on these variants of the given algorithmic problem and was successfully defending his work in September leading to a doctoral degree. Currently, there is no other PhD student working in the team, but for 2023 a new PhD student will be hired to continue with the mentioned research directions.

As programme director of the "Bachelor in Applied Information Technology" and its life-long learning variant "Bachelor in Applied Information Technology – Continuing Education Programme", Volker Müller was strongly involved in smooth organization of the two programmes and also teaching several courses in the programme. More than 40 BINFO students could be graduated in 2022 after having finished their final Bachelor project linking applied scientific training with professional needs.

Organizational Structure

The Department of Computer Science is organized according to the following structure.

- 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. The head is also seconded by a Departmental Head of Teaching, to whom tasks in relation to teaching management are delegated. The roles of vice-head and Departmental Head of Teaching can be assumed by one person. Together, they perform the daily management of the department.
- DCS forms two sub-committees: an education management committee (EMC) and a research management committee (RMC). The purpose of the EMC is to coordinate all teaching-related activities of DCS. The purpose of the RMC is to represent DCS in discussions and decisions with regards to research coordination and its general and financial management.
- The head of DCS is the head of the RMC and the Departmental Head of Teaching is head of the EMC. The head of DCS is a regular member of the EMC and the vice-head is a regular member of the RMC. Further, these committees are formed by the heads of the educational programs (EMC) and by the lab heads (RMC).
- Besides these committees, the general DCS professors meeting is the final decision body of DCS.
- The head and vice-head/Departmental Head of Teaching are supported by the secretary team of the department and whenever needed by a research facilitator of the faculty.
- The head and vice-head/Departmental Head of Teaching of DCS represent DCS at the various UL levels. The internal communication within DCS is based on an effective communication infrastructure. Short summaries of the DCS professors meeting and the meetings of the EMC and RMC are made available. DCS labs organize DCS resources and competencies with a long-term view, and are governed by the following guidelines.
- There are three hierarchical levels within DCS: DCS (all members of DCS) + LAB (a substructure of DCS) + GRP (a research group consisting of a DCS 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. DCS can delegate responsibilities to other entities (such as the management team, heads of studies, labs, heads of labs, ad-hoc groups, individuals). Research groups are named after their main topic(s) of study.
- The purpose of a LAB is at least to coordinate and distribute tasks, and to distribute money and share resources (like rooms). Moreover, labs can be used for PR and visibility, to represent its members within DCS, 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 professors as 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. DCS can allocate resources to professors that are not member of any lab.
- The set of LABS remains stable for long term (e.g. at least 4 years). DCS decides on the discontinuation of existing labs and the creation of new labs. A group of professors can propose to DCS to create a new lab.
- A certain percentage of the DCS 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 are not assigned to labs, but to professors.
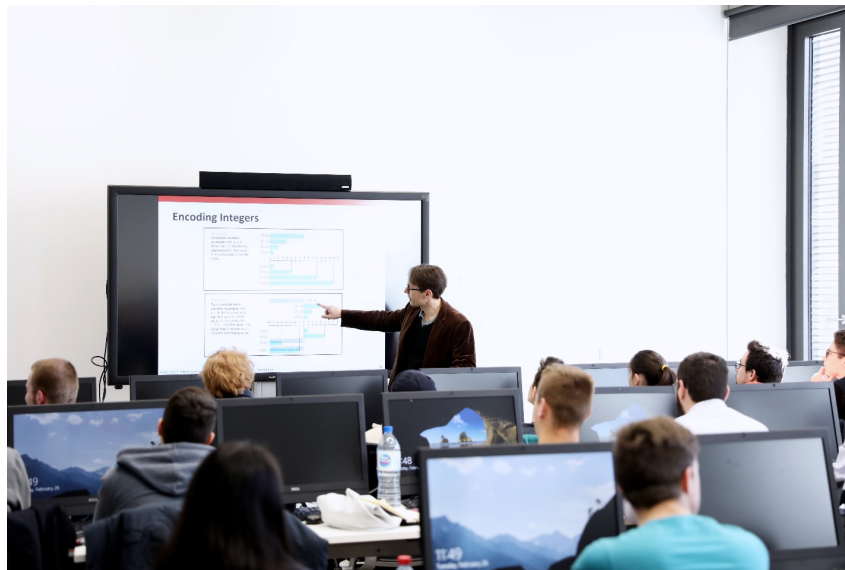
Education

The DCS educational offer in computer science aims at meeting the quickly growing societal needs for academic and professional education in computer science. DCS offers a spectrum of study programs suited to the needs of different groups of students:

- Academically-oriented programs, at the bachelor (BICS, see section 6.6) and master level (MICS, see section 6.2), suited for students with a strong academic background willing primarily to continue their studies towards a master program (when in a bachelor program) or a PhD (when in a master program).
- Professionally-oriented programs at the bachelor level (BINFO, see section 6.7) and Master level (ISM, see section 6.4), designed mainly for students intending to enter the job market with a training well suited to meet the needs of local companies and institutions.
- Lifelong learning programs, both at the bachelor (BINFO-CEP, see section 6.8) and at the master level (MISSM, see section 6.3 and MTECH, see section 6.5), that are organised with a partner: the Chambre des Salariés (CSL), the Luxembourg Institute of Science and Technology (LIST) or the Luxembourg Institute of Standardisation, Accreditation, Safety and Quality of Products and Services (ILNAS). These programs target students with a substantial professional experience validated through the procedure of recognition of prior education and professional experience.
- A Doctoral program in Computer Science and Computer Engineering (see section 6.1) to train Doctoral Candidates from DCS and SnT on a wide range of advanced and interdisciplinary subjects including the fundamentals of teaching. In addition to its own study programs, DCS is also contributing to the teaching in programs managed by other depart-

ments such as the engineering and mathematics departments.

For the purpose of quality assurance and to further improve the quality of teaching in all its facets, DCS has initiated the certification of its study programs by international agencies. The MICS, BINFO and BINFO-CEP were the first programs to undergo the accreditation process of the Accreditation, Certification and Quality Assurance Institute (ACQUIN), which they obtain without reservation in 2021.

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 Department of Computer Science (DCS) 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, Software Engineering, High Performance Computing and Big Data.

The DP-CSCE now hosts over 210 doctoral candidates of 46 different nationalities, which makes it the biggest doctoral programme of the University of Luxembourg.

6.2 Master in Information and Computer Sciences (MiCS)

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

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

• Artificial Intelligence
• Communication Systems
• Information Security
• Reliable Software Systems

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

6.3 Master in Information System Security Management (MISSM)

The MISSM (Master in Information System Security Management) allows professionals to increase their knowledge and develop their skills to analyse, interpret and provide adequate solutions in the field of information security.

It is a lifelong learning Master degree programme with a well-established reputation in Luxembourg and the Greater Region. Created in 2007, together with market stakeholders, the MISSM graduates every year between 12 and 18 professionals in the field of security management. The ISSM master is specifically aimed at training CISOs, which is why the program covers all interdisciplinary aspects related to this role. The focus is on the implementation of best practices and standards for security management, complemented by the acquisition of knowledge in the technical, legal, and social fields.

Thanks to our teaching team, composed of academics and professionals, we provide the interdisciplinary, applied and academic
background (technical, managerial, legal...) required for security officers to face the challenges of nowadays security threats.

Since 2017, the Information Security Education Day (ISED) is organized: this event primarily targets the current and former students of the MISSM. It is a yearly event aiming at providing new knowledge on a hot-topic related to security and privacy and is the ideal forum where academics and practitioners can learn about the different facets of a key-topic, exchange and discuss ideas, and compare experiences. The 2022 ISED theme was: "Demystifying the Dark Web: Challenges and Threats » and attracted around 70 attendees.

6.4 Interdisciplinary Space Master

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

The domains covered by industry and public research institutes include:

- The space segment comprises developing and manufacturing micro and nano satellites, structures, electronic equipment, space robotics and systems for space resource utilisation and in-space manufacturing.
- The ground segment comprises ground station development, mechanical and electrical ground support equipment, and communication networks.
- The service segment embraces teleport, satellite broadband, risk management and automatic identification system (AIS) services, remote sensing and space-based data analytics.

To respond to a growing need for people educated to contribute to these fields in Luxembourg and Europe, the Interdisciplinary Space Master (ISM) has been created in 2019 at UL in close collaboration with the Luxembourg Space Agency (LSA). Through a project-based learning approach, graduates will understand the science that motivates the space sector industry and what is technically required to establish and manage space missions.

Students will also learn the computer skills required to interpret observations from space (big data, machine learning, artificial intelligence). This master's degree is an innovative balance between teaching and learning about business and technology. It provides a solid grounding in all aspects of the space value chain, in space engineering and computing, but also introduces students to business and project management, enabling them to work in established space companies and start-ups or even to set up their own space company in Luxembourg".

The space value chain is a commercial space venture that includes commercial or research operations on the Moon and near-Earth asteroids. More specifically, courses will touch upon space systems engineering, space operations, space data mining and intelligent systems, satellite communications, and robotics. Theoretical and practical concepts in business, entrepreneurship, finance and project management are also components of the study programme. UL professors deliver the lectures with guest lectures from renowned partner universities and industry experts with significant experience working in the space sector. During the Master, students will use cutting edge Labs, such as the LunaLab, CubeSat Lab, Concurrent Design Facility, Sat ComLab and Zero-G Lab. In the fourth semester of the master, the students will work on their Master's thesis, which can also be done in collaboration with our research groups or an external partner such as a company or an agency. To gain additional work experience, students are also encouraged to do one or several voluntary internships in space companies. The ISM is already running for four cohorts and has attracted a distinctive mix of international students with interdisciplinary backgrounds.

Luxembourg Space ecosystem strongly demands experts from this Interdisciplinary Master, as proven by the high employability percentage of previous ISM graduates.

6.5 Master in Technopreneurship (MTECH)

The Master in Technopreneurship (MTECH) at the University of Luxembourg is developed in partnership with the Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS) and the Luxembourg Lifelong Learning Center (LLLC) of the Chambre des Salariés (CSL). The Master MTECH is extremely innovative. On one hand, it provides students with a base of knowledge on topics reflecting current issues and those at the cutting edge of Smart ICT, and on the other hand, it serves as a catalyst for growth in the ICT Industry by offering practical examples and case studies illustrating the use of technical standardisation as a tool to give common technical language, build trust, and foster effectiveness in Smart ICT. The Master degree is also supported by the European standardisation organisations, namely the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC), as well as the European Telecommunications Standards Institute (ETSI).

The second promotion of the MTECH will start in February 2023.

6.6 Bachelor in Computer Science (BiCS)

Since the academic year 2017-2018, the Department of Computer Science (DCS) offers a bachelor programme in computer science (BiCS). This study programme is meant for students interested in learning the foundational theoretical aspects of computer science and developing skills to make use of such theories in practical contexts.

In the end, students who have successfully completed the programme will be ready to pursue studies in a master programme on computer science either at the University of Luxembourg or any other world-class university.

The main strengths of the BiCS are:

- programme designed from the international standard ACM / IEEE CS 2013,
- scientific quality to enhance interest and strengths in science and technology for the future,
- project-based learning as a signature pedagogy, in line with the university's drive for "research-based teaching",
- applied multilingualism for effective integration into the Luxembourgish or international labour market.

The BiCS programme brings:

- greater focus on key skills needed for computer scientists,
- more systematic consideration and implementation of the internationally recognised standards in computer science education,
- better offer to industry and societal requirements
- more thoughtful selection of specific types of pedagogies necessary to train highly effective students.

A R&D laboratory known as BicsLab is attached to the study programme. The goals of this lab are:

- provide a common space for BiCS students where they can develop their own ideas and initiatives,
- develop industrial collaborations,
- host selected Bachelor Semester Projects (BSPs) to be done in partnership with industrial partners,
- provide an initial R&D support structure for selected BiCS students.

The BiCSLab is supported by the BiCS programme and industrial partners with whom collaborations agreements are signed. More about the BicsLab can be found at https://bicslab. uni.lu.

At the end of the academic year 2021-2022 (i.e. by July 2022), 21 students got graduated (19 male and 2 female), wich represents an increment of 28% with respect to the previous academic year.

Regarding the academic year 2022-2023 (i.e. September 2022):

- 165 candidates applied to the programme (25% female, 75% male).
- 98 were retained (acceptance rate of 59%), with a distribution of:
  - 26% female, and 74% male,
  - 30% Non-EU and 70% EU,
  - 43% Luxembourg, 17% Greater Region, and 22% from other EU countries.

Finally, 72 accepted candidates decided to start the programme (joining rate: 75%), with a distribution of 23% female, and 77% male.

More information and news about BiCS can be found at https://bics.uni.lu.

6.7 Bachelor in Applied Information Technology (BINFO)

The Bachelor in Applied Information Technology (BINFO) is a practice-oriented study program that equips students with highly sought-after professional skills for entering the job market in both public and private sectors. Through a combination of theoretical lectures and practical projects, students gain a mastery of essential professional skills and applied IT knowledge that enables them to continuously develop throughout their careers. BINFO's curriculum covers both relevant IT-related technologies and human-focused education, with a bilingual program in English and French that fosters cultural diversity and mobility through a semester abroad. The main learning objectives of the BINFO are the following:

- Be competent in software programming and, more widely, in methods required to develop computer systems.
- Acquire a specialization in one application domain of computer science such as big data, mobile and web applications, banking information technology or distributed applications, especially deepening applied knowledge on the latest trends in the IT industry.
- Be able to efficiently communicate orally and in writing, in English and French, in cross cultural professional environments.
- Understand how companies operate and be well prepared for a professional career, through a final 3-month Bachelor project done in professional partner institutions and teaching delivered by experienced practitioners.
- Be able to work autonomously, analyze and anticipate issues, propose solutions in various professional situations.

In the Winter semester 2022-2023, a total of 165 students are registered within the BINFO program (74 in the first year, 42 in the second, and 49 students in the third year). The number of BINFO graduates in 2022 is 32. More information on the programme can be found at https://binfo.uni.lu. In 2021, the BINFO programme was accredited by the German accreditation agency ACQUIN until September 2028.

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

The "Bachelor in Applied Information Technology - Continuous Education Programme" (BINFO-CEP) is a practice-oriented, part-time study program designed to meet the needs of the Luxembourgish labor market for continued professional development. The program is offered in partnership with the Lifelong Learning Center of the *Chambre des Salariés* (CSL). Applicants must have a minimum of 6 years of professional experience in the IT domain, which is recognized in the program with the acknowledgment of a certain number of ECTS credits. BINFO-CEP combines theoretical lectures and practical projects to train students in essential areas such as programming, web applications, and software engineering. The program's goal is to empower students for continuous training and further professional development throughout their careers. BINFO-CEP offers a bilingual program in English and French with classmates and instructors from diverse cultural and professional backgrounds, creating a rich human experience beyond technical training in relevant IT-related technologies.

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

- Be competent in software programming and, more widely, in methods required to develop computer systems.

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

In the Winter semester 2022-2023, a total of 24 students are registered within the BINFO-CEP program (10 in the first, 14 students in the second/third year). The number of BINFO-CEP graduates in 2022 is 9. More information on the programme can be found at https://binfo-cep.uni.lu . In 2021, the BINFO-CEP programme was accredited by the German accreditation agency ACQUIN until September 2028.

Publication List

The publications listed in this chapter have been obtained from ORBilu, the official publication record repository of the university. Please note that the list of books includes those where a DCS member contributed as an editor.

Publication Category	Quantity	Section
Books	6	A.1 (p.48)
Book Chapters	3	A.2 (p.49)
Journal Articles	67	A.3 (p.49)
Conference Papers	111	A.4 (p.54)
Theses	36	A.5 (p.64)
Total	*223*	

Table A.1: Overview of publications per category
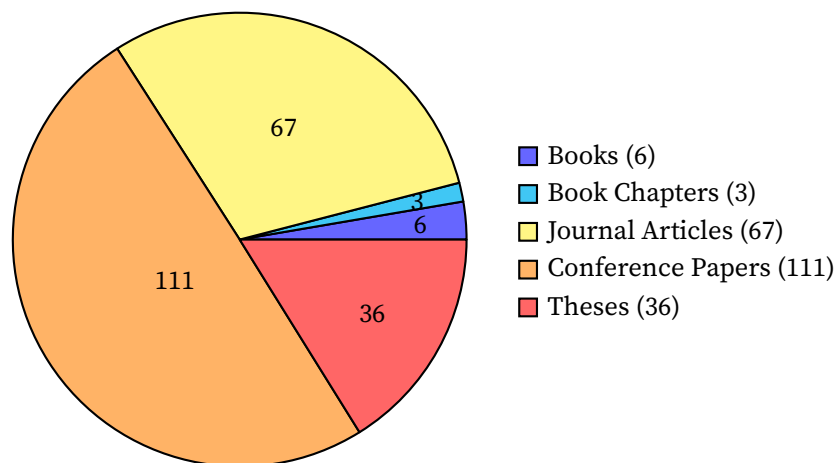
Figure A.1: Distribution of Types of Publications

A.1   Books

[1] Raymond Bisdorff. *Algorithmic Decision Making with Python Resources: From multicriteria performance records to decision algorithms via bipolar-valued outranking digraphs.* 2022-04. ISBN: 978-3-030-90927-2. URL: http://hdl.handle.net/10993/48296.

[2] Jean-Guillaume Dumas, Pascal Lafourcade, Etienne Roudeix, Ariane Tichit, and Sébastien Varrette. *Les NFT en 40 questions: Des réponses claires et détaillées pour comprendre les Non Fungible Tokens*. 2022-02. ISBN: 978-2-1008-3304-7. URL: http://hdl.handle.net/10993/50367.

[3] Jean-Guillaume Dumas, Pascal Lafourcade, Ariane Tichit, and Sébastien Varrette. *Les blockchains en 50 questions*. 2022-02. ISBN: 978-2-1008-3450-1. URL: http://hdl.handle.net/10993/50368.

[4] Luis A. Leiva, Cedric Pruski, Réka Markovich, Amro Najjar, and Christoph Schommer, eds. *Artificial Intelligence and Machine Learning - 33rd Benelux Conference on Artificial Intelligence, BNAIC/Benelearn 2021, Esch-sur-Alzette, Luxembourg, November 10-12, 2021, Revised Selected Papers*. 2022. ISBN: 978-3-030-93841-3. URL: http://hdl.handle.net/10993/54510.

[5] Beishui Liao, Réka Markovich, and Yí Wáng, eds. *Logics for New-Generation AI*. 2022. URL: http://hdl.handle.net/10993/54508.

[6] Hong Mei, Jian Lv, Zhi Jin, Xuandong Li, Guanglai Gao, Jun Pang, et al., eds. *Proceedings of the 13th Asia-Pacific Symposium on Internetware*. 2022. ISBN: 978-1-4503-9780-3. URL: http://hdl.handle.net/10993/52117.

A.2 Book Chapters

[7] Jean Botev, Ada Diaconescu, Heiko Hamann, Stephen Marsh, and Francisco J. Rodríguez Lera. "Editorial: Socio-Technical Ecologies – Design for Human-Machine Systems". In: *Frontiers in Robotics and AI | Socio-Technical Ecologies: Design for Human-Machine Systems*. Frontiers, 2022. URL: http://hdl.handle.net/10993/52876.

[8] Franck Leprevost, Ali Osman Topal, Elmir Avdusinovic, and Ioana Raluca Chitic. "Strategy and Feasibility Study for the Construction of High Resolution Images Adversarial Against Convolutional Neural Networks". In: *ACIIDS 2022: Intelligent Information and Database Systems*. Springer, 2022-12-08, pp. 285–298. URL: http://hdl.handle.net/10993/53022.

[9] Anthony Stein, Sven Tomforde, Jean BOTEV, and Peter R. Lewis. "Lifelike Computing Systems Workshop (LIFELIKE 2022)". In: *Proceedings of the Lifelike Computing Systems Workshop (LIFELIKE 2022)*. CEUR WS, 2022. URL: http://hdl.handle.net/10993/57163.

A.3 Journal Articles

[10] Ryuta Arisaka, Jérémie Dauphin, Ken Satoh, and Leon van der Torre. "Multi-agent Argumentation and Dialogue". In: *IfCoLog Journal of Logics and Their Applications* 9 (2022), pp. 853–886. URL: http://hdl.handle.net/10993/54191.

[11] Matteo Barborini, Matteo Calandra, Francesco Mauri, Ludger Wirtz, and Pier Luigi Cudazzo. "Excitonic-insulator instability and Peierls distortion in one-dimensional semimetals". In: *Physical Review. B* 105 (2022), p. 075122. URL: http://hdl.handle.net/10993/50683.

[12] Jim Jean-Pierre Barthel and Volker Müller. "A Conjecture on Primes in Arithmetic Progressions and Geometric Intervals". In: *American Mathematical Monthly* 129 (2022-10-06), pp. 979–983. URL: http://hdl.handle.net/10993/53879.

[13]   Davide Basile, Maurice H. ter Beek, Sami LAZREG, Maxime CORDY, and Axel Legay. "Static detection of equivalent mutants in real-time model-based mutation testing: An Empirical Evaluation". In: *Empirical Software Engineering* 27 (2022-12). URL: http://hdl.handle.net/10993/58903.

[14]   Abdelwahab Boualouache, Bouziane Brik, Qiang Tang, Abdelaziz, Sylvain Cherrier, Sidi-Mohammed Senouci, et al. "5G Vehicle-to-Everything at the Cross-Borders: Security Challenges and Opportunities". In: *IEEE Internet of Things Journal* (2022-12). URL: http://hdl.handle.net/10993/54375.

[15]   Abdelwahab Boualouache and Thomas Engel. "A Survey on Machine Learning-based Misbehavior Detection Systems for 5G and Beyond Vehicular Networks". In: *IEEE Communications Surveys and Tutorials* (2022-12). URL: http://hdl.handle.net/10993/54374.

[16]   Lukas Brückner, Luis A. Leiva, and Antti Oulasvirta. "Learning GUI Completions with User-defined Constraints". In: *ACM Transactions on Interactive Intelligent Systems* 12 (2022). URL: http://hdl.handle.net/10993/50489.

[17]   Alfredo Capozucca, Jean-Michel Bruel, Manuel Mazzara, and Bertrand Meyer. "Special Issue on New Paradigms of Software Production and Deployment". In: *SN Computer Science* 3 (2022-01-13). URL: http://hdl.handle.net/10993/50019.

[18]   Jorge Alfonso Charry Martinez, Matteo Barborini, and Alexandre Tkatchenko. "Correlated Wave Functions for Electron–Positron Interactions in Atoms and Molecules". In: *Journal of Chemical Theory and Computation* 18 (2022), pp. 2267–2280. URL: http://hdl.handle.net/10993/50675.

[19]   Jorge Alfonso Charry Martinez, Felix Moncada, Matteo Barborini, Laura Milena Pedraza González, Marcio Teixeira Varella, Alexandre Tkatchenko, et al. "The three-center two-positron bond". In: *Chemical Science* (2022), pp. -. URL: http://hdl.handle.net/10993/52620.

[20]   Ninghan Chen, Xihui Chen, and Jun Pang. "A multilingual dataset of COVID-19 vaccination attitudes on Twitter". In: *Data in Brief* 44 (2022-10), p. 108503. URL: http://hdl.handle.net/10993/52165.

[21]   Ninghan Chen, Xihui Chen, Zhiqiang Zhong, and Jun Pang. "Exploring Spillover Effects for COVID-19 Cascade Prediction". In: *Entropy* 24 (2022). URL: http://hdl.handle.net/10993/50679.

[22]   Raluca Chitic, Ali Osman Topal, and Franck Leprevost. "Empirical Perturbation Analysis of Two Adversarial Attacks: Black Box versus White Box". In: *Applied Sciences* 12 (2022), p. 7339. URL: http://hdl.handle.net/10993/52264.

[23]   Christian Colot, François Robinet, Geoffrey Nichil, and Raphaël Frank. "Connected Vehicle Platforms for Dynamic Insurance". In: *in Proceedings of the 6th International Conference on Intelligent Traffic and Transportation* (2022-08). URL: http://hdl.handle.net/10993/52859.

[24]   Klen Čopič Pucihar, Nuwan T. Attygalle, Matjaž Kljun, Christian Sandor, and Luis A. Leiva. "Solids on Soli: Millimetre-Wave Radar Sensing through Materials". In: *Proceedings of the ACM on Human-Computer Interaction* (2022). URL: http://hdl.handle.net/10993/50488.

[25]   Jean-Sébastien Coron, François Gerard, Simon Montoya, and Rina Zeitoun. "High-order Table-based Conversion Algorithms and Masking Lattice-based Encryption". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2022). URL: http://hdl.handle.net/10993/55063.

[26]   Mauro Dalle Lucca Tosi and Julio Cesar dos Reis. "Understanding the evolution of a scientific field by clustering and visualizing knowledge graphs". In: *Journal of Information Science* 48 (2022), pp. 71–89. URL: http://hdl.handle.net/10993/52019.

[27]   Nadia Daoudi, Kevin Allix, Tegawendé François D Assise Bissyande, and Jacques Klein. "A Deep Dive inside DREBIN: An Explorative Analysis beyond Android Malware Detection Scores". In: *ACM Transactions on Privacy and Security* 25 (2022-05). URL: http://hdl.handle.net/10993/49254.

[28]   Nadia Daoudi, Kévin Allix, Tegawendé François D Assise Bissyande, and Jacques Klein. "Assessing the opportunity of combining state-of-the-art Android malware detectors". In: *Empirical Software Engineering* 28 (2022-12). URL: http://hdl.handle.net/10993/53606.

[29]   Saharnaz Dilmaghani, Mathias Brust, Carlos H. Ribeiro, Emmanuel Kieffer, Grégoire Danoy, and Pascal Bouvry. "From communities to protein complexes: A local community detection algorithm on PPI networks". In: *PLoS ONE* 17 (2022-01), pp. 1–17. URL: http://hdl.handle.net/10993/51663.

[30]   Huimin Dong, Beishui Liao, Réka Markovich, and Leon van der Torre. "Defeasible Deontic Logic: Arguing about Permission and Obligation". In: *IfCoLog Journal of Logics and Their Applications* 9 (2022), pp. 957–1018. URL: http://hdl.handle.net/10993/54193.

[31]   Gabriel Duflo, Grégoire Danoy, El-Ghazali Talbi, and Pascal Bouvry. "Learning to Optimise a Swarm of UAVs". In: *Applied Sciences* 12 (2022). URL: http://hdl.handle.net/10993/52566.

[32]   Valerie Fetzer, Marcel Keller, Sven Maier, Markus Raiber, Andy Rupp, and Rebecca Schwerdt. "PUBA: Privacy-Preserving User-Data Bookkeeping and Analytics". In: *Proceedings on Privacy Enhancing Technologies* 2022 (2022). URL: http://hdl.handle.net/10993/50223.

[33]   Aayush Garg, Renzo Gaston Degiovanni, Matthieu Jimenez, Maxime Cordy, Mike Papadakis, and Yves Le Traon. "Learning from what we know: How to perform vulnerability prediction using noisy historical data". In: *Empirical Software Engineering* (2022-09-20). URL: http://hdl.handle.net/10993/45529.

[34]   Nicolas Guelfi. "The MESSIR Flexible Scientific Approach to Requirements Engineering". In: *Software* 1 (2022-03-07), pp. 80–106. URL: http://hdl.handle.net/10993/52469.

[35]   Mathieu Guillaume, Marcos Cramer, Leon van der Torre, and Christine Schiltz. "Reasoning on conflicting information: An empirical study of Formal Argumentation". In: *PLoS ONE* 17 (2022). URL: http://hdl.handle.net/10993/54190.

[36]   Cengis Hasan, Ross James Horne, Sjouke Mauw, and Andrzej Mizera. "Cloud removal from satellite imagery using multispectral edge-filtered conditional generative adversarial networks". In: *International Journal of Remote Sensing* 43 (2022), pp. 1881–1893. URL: http://hdl.handle.net/10993/52849.

[37]   Ganglin Hu, Jun Pang, and Xian Mo. "Effective attributed network embedding with information behavior extraction". In: *PeerJ Computer Science* 8 (2022), e1030. URL: http://hdl.handle.net/10993/52118.

[38]   Qiang Hu, Yuejun Guo, Maxime Cordy, Xiaofei Xie, Lei Ma, Mike Papadakis, et al. "An Empirical Study on Data Distribution-Aware Test Selection for Deep Learning Enhancement". In: *ACM Transactions on Software Engineering and Methodology* (2022). URL: http://hdl.handle.net/10993/50265.

[39]   Timotheus Kampik, Juan Carlos Nieves, and Dov M. Gabbay. "Ensuring reference independence and cautious monotony in abstract argumentation". In: *International Journal of Approximate Reasoning* 140 (2022), pp. 173–210. URL: http://hdl.handle.net/10993/54261.

[40]   Benjamin Kap, Marharyta Aleksandrova, and Thomas Engel. "The Effect of Noise Level on the Accuracy of Causal Discovery Methods with Additive Noise Models". In: *Communications in Computer and Information Science* 1530 (2022). URL: http://hdl.handle.net/10993/50417.

[41]   Ahmed Khanfir, Anil Koyuncu, Mike Papadakis, Maxime Cordy, Tegawendé François D Assise Bissyande, Jacques Klein, et al. "iBiR: Bug Report driven Fault Injection". In: *ACM Transactions on Software Engineering and Methodology* (2022-05-13). URL: http://hdl.handle.net/10993/54378.

[42]   Kisub Kim, Sankalp Ghatpande, Kui Liu, Anil Koyuncu, Dongsun Kim, Tegawendé François D Assise Bissyande, et al. "DigBug—Pre/post-processing operator selection for accurate bug localization". In: *Journal of Systems and Software* 189 (2022-07). URL: http://hdl.handle.net/10993/52228.

[43]   Sybren de Kinderen, Monika Kaczmarek-Heß, Qin Ma, and Iván S. Razo-Zapata. "Model-based valuation of smart grid initiatives: Foundations, open issues, requirements, and a research outlook". In: *Data and Knowledge Engineering* 141 (2022-09). URL: http://hdl.handle.net/10993/53303.

[44]   Ali Kishk, Maria Irene Pires Pacheco, Tony Heurtaux, Lasse Sinkkonen, Jun Pang, Sabrina Fritah, et al. "Review of Current Human Genome-Scale Metabolic Models for Brain Cancer and Neurodegenerative Diseases." In: *Cells* 11 (2022). URL: http://hdl.handle.net/10993/52436.

[45]   Aleks Knoks. "Conciliatory views, higher-order disagreements, and defeasible logic". In: *Synthese* 200 (2022-04-15), pp. 1–23. URL: http://hdl.handle.net/10993/50870.

[46]   Luis A. Leiva, Hota, and Antti Oulasvirta. "Describing UI Screenshots in Natural Language". In: *ACM Transactions on Intelligent Systems and Technology* (2022). URL: http://hdl.handle.net/10993/52281.

[47]   Luis A. Leiva, Morteza Shiripour, and Antti Oulasvirta. "Modeling How Different User Groups Perceive Webpage Aesthetics". In: *Universal Access in the Information Society* (2022). URL: http://hdl.handle.net/10993/51957.

[48]   Franck Leprevost, Ali Osman Topal, Elmir Avdusinovic, and Ioana Raluca Chitic. "A strategy creating high-resolution adversarial images against convolutional neural networks and a feasibility study on 10 CNNs". In: *Journal of Information and Telecommunication* 7 (2022-10-22), pp. 89–119. URL: http://hdl.handle.net/10993/55235.

[49]   Joe Lorentz, Thomas Hartmann, Assaad Moawad, François Fouquet, Djamila Aouada, and Yves Le Traon. "CalcGraph: taming the high costs of deep learning using models". In: *Software and Systems Modeling* (2022-10-25). URL: http://hdl.handle.net/10993/52860.

[50]   Qin Ma, Monika Kaczmarek-Heß, and Sybren de Kinderen. "Validation and verification in domain-specific modeling method engineering: an integrated life-cycle view". In: *Software and Systems Modeling* (2022-10). URL: http://hdl.handle.net/10993/53322.

[51]   Juliano Maranhão, Giovanni Casini, Gabriella Pigozzi, and Leon van der Torre. "Normative Change: An AGM Approach". In: *IfCoLog Journal of Logics and Their Applications* 9 (2022), pp. 787–852. URL: http://hdl.handle.net/10993/54192.

[52] Sjouke Mauw, Yunior Ramirez Cruz, and Rolando Trujillo Rasua. "Preventing active re-identification attacks on social graphs via sybil subgraph obfuscation". In: *Knowledge and Information Systems* 64 (2022-02-27), pp. 1077–1100. URL: http://hdl.handle.net/10993/53953.

[53] Xian Mo, Jun Pang, and Zhiming Liu. "THS-GWNN: a deep learning framework for temporal network link prediction". In: *Frontiers of Computer Science* 16 (2022-02), p. 162304. URL: http://hdl.handle.net/10993/49140.

[54] Atefeh Nirumand, Bahman Zamani, Behrouz Tork-Ladani, Jacques Klein, and Tegawendé François D Assise Bissyande. "A model-based framework for interapp Vulnerability analysis of Android applications". In: *Software: Practice and Experience* (2022-11), pp. 1–42. URL: http://hdl.handle.net/10993/54304.

[55] Milos Ojdanic, Wei Ma, Thomas Laurent, Thierry Titcheu Chekam, Anthony Ventresque, and Mike Papadakis. "On the use of commit-relevant mutants". In: *Empirical Software Engineering* 27 (2022-05-30). URL: http://hdl.handle.net/10993/53863.

[56] Milos Ojdanic, Ezekiel Soremekun, Renzo Gaston Degiovanni, Mike Papadakis, and Yves Le Traon. "Mutation Testing in Evolving Systems: Studying the relevance of mutants to code evolution". In: *ACM Transactions on Software Engineering and Methodology* (2022-05-11). URL: http://hdl.handle.net/10993/53860.

[57] Paul Ortiz, Sylvain Kubler, Éric Rondeau, Katie McConky, Alexander Alexandrovich Shukhobodskiy, Giuseppe Colantuono, et al. "Greenhouse gas emission reduction in residential buildings: A lightweight model to be deployed on edge devices". In: *Journal of cleaner production* 368 (2022), pp. 133092–. URL: http://hdl.handle.net/10993/53206.

[58] Pere Pardo Ventura and Christian Strasser. "Modular Orders on Defaults in Formal Argumentation". In: *Journal of Logic and Computation* (2022-11-17). URL: http://hdl.handle.net/10993/52826.

[59] François Robinet, Yussef Akl, Kaleem Ullah, Farzad Nozarian, Christian Müller, and Raphaël Frank. "Striving for Less: Minimally-Supervised Pseudo-Label Generation for Monocular Road Segmentation". In: *IEEE Robotics and Automation Letters* 7 (2022-10), pp. 10628–10634. URL: http://hdl.handle.net/10993/52626.

[60] Marcelo Luis Ruiz Rodriguez, Sylvain Kubler, Andrea de Giorgio, Maxime Cordy, Jérémy Robert, and Yves Le Traon. "Multi-agent deep reinforcement learning based Predictive Maintenance on parallel machines". In: *Robotics and Computer-Integrated Manufacturing* (2022). URL: http://hdl.handle.net/10993/54345.

[61] Delwende Arthur Sawadogo, Tegawendé François D Assise Bissyande, Naouel Moha, Kevin Allix, Jacques Klein, Li Li, et al. "SSPCATCHER: Learning to catch security patches". In: *Empirical Software Engineering* 27 (2022-08). URL: http://hdl.handle.net/10993/54305.

[62] Daniel Stolfi Rosso, Mathias Brust, Grégoire Danoy, and Pascal Bouvry. "SuSy-EnGaD: Surveillance System Enhanced by Games of Drones". In: *Drones* 6 (2022). URL: http://hdl.handle.net/10993/50504.

[63] Daniel Stolfi Rosso and Grégoire Danoy. "An Evolutionary Algorithm to Optimise a Distributed UAV Swarm Formation System". In: *Applied Sciences* 12 (2022-10-11). URL: http://hdl.handle.net/10993/52964.

[64] Xiaoyu Sun, Xiao Chen, Li Li, Haipeng Cai, John Grundy, Jordan Samhi, et al. "Demystifying Hidden Sensitive Operations in Android apps". In: *ACM Transactions on Software Engineering and Methodology* (2022-12). URL: http://hdl.handle.net/10993/54303.

[65]   Je Sen TEH and Alexei BIRYUKOV. "Differential cryptanalysis of WARP". In: *Journal of Information Security and Applications* 70 (2022-11), p. 103316. U R L: http://hdl.handle.net/10993/57996.

[66]   Haoye Tian, Yinghua Li, Weiguo Pian, Abdoul Kader Kabore, Kui Liu, Andrew Habib, et al. "Predicting Patch Correctness Based on the Similarity of Failing Test Cases". In: *ACM Transactions on Software Engineering and Methodology* (2022). U R L: http://hdl.handle.net/10993/52239.

[67]   Haoye Tian, Kui Liu, Yinghua Li, Abdoul Kader Kabore, Anil Koyuncu, Andrew Habib, et al. "The Best of Both Worlds: Combining Learned Embeddings with Engineered Features for Accurate Prediction of Correct Patches". In: *ACM Transactions on Software Engineering and Methodology* (2022). U R L: http://hdl.handle.net/10993/54368.

[68]   Leon van der Torre and Xavier Parent. "Detachment in Normative Systems: Examples, Inference Patterns, Properties". In: *IfCoLog Journal of Logics and Their Applications* 9 (2022), pp. 1019–1062. U R L: http://hdl.handle.net/10993/54472.

[69]   Vinu Ellampallil Venugopal, Martin Theobald, Damien Tassetti, Samira Chaychi, and Amal Tawakuli. "Targeting a light-weight and multi-channel approach for distributed stream processing". In: *Journal of Parallel and Distributed Computing* 167 (2022-07-25), pp. 77–96. U R L: http://hdl.handle.net/10993/54419.

[70]   Kai Wang, Jun Pang, Dingjie Chen, Yu Zhao, Dapeng Huang, Chen Chen, et al. "A Large-scale Empirical Analysis of Ransomware Activities in Bitcoin". In: *ACM Transactions on the Web* 16 (2022-05), pp. 1–29. U R L: http://hdl.handle.net/10993/49139.

[71]   John G. Woods and Dov M. Gabbay. "The Law of Evidence and Labelled Deduction: Ten Years Later". In: *Journal of Applied Logic* 9 (2022), pp. 887–956. U R L: http://hdl.handle.net/10993/54260.

[72]   Dapeng Yan, Kui Liu, Yuqing Niu, Li Li, Zhe Liu, Zhiming Liu, et al. "Crex: Predicting patch correctness in automated repair of C programs through transfer learning of execution semantics". In: *Information and Software Technology* 152 (2022-12), pp. 1–12. U R L: http://hdl.handle.net/10993/54302.

[73]   Chenyi Zhang and Jun Pang. "Modal characterisation of simulation relations in probabilistic concurrent games". In: *Science of Computer Programming* 215 (2022-03), p. 102762. U R L: http://hdl.handle.net/10993/49150.

[74]   Zhiqiang Zhong, Guadalupe Gonzalez, Daniele Grattarola, and Jun Pang. "Unsupervised network embedding beyond homophily". In: *Transactions on Machine Learning Research* (2022-12). U R L: http://hdl.handle.net/10993/53475.

[75]   Zhiqiang Zhong, Sergey Ivanov, and Jun Pang. "Simplifying Node Classification on Heterophilous Graphs with Compatible Label Propagation". In: *Transactions on Machine Learning Research* (2022-10). U R L: http://hdl.handle.net/10993/53259.

[76]   Zhiqiang Zhong, Cheng-Te Li, and Jun Pang. "Personalised meta-path generation for heterogeneous graph neural networks". In: *Data Mining and Knowledge Discovery* 36 (2022), pp. 2299–2333. U R L: http://hdl.handle.net/10993/52908.

A.4   Conference Papers

[77]   Matteo Acclavio, Ross James Horne, Sjouke Mauw, and Lutz Straßburger. "A Graphical Proof Theory of Logical Time". In: *Proc. 7th International Conference on Formal Structures for Computation and Deduction (FSCD 2022)*. Ed. by Amy P. Felty.

Schloss Dagstuhl – Leibniz-Zentrum fur Informatik, 2022, 22:1–22:25. URL: http://hdl.handle.net/10993/53956.

[78]	Boladji Vinny Adjibi, Fatou Ndiaye Mbodji, Kevin Allix, Jacques Klein, and Tegawendé François D Assise Bissyande. "The Devil is in the Details: Unwrapping the Cryptojacking Malware Ecosystem on Android". In: *2022 IEEE 22nd International Working Conference on Source Code Analysis and Manipulation (SCAM)*. IEEE, 2022-10, pp. 153–163. URL: http://hdl.handle.net/10993/54308.

[79]	Benoît Alcaraz, Nina Hosseini Kivanani, and Amro Najjar. "IRRMA: An Image Recommender Robot Meeting Assistant". In: *IRRMA: An Image Recommender Robot Meeting Assistant*. 2022-07, pp. 449–453. URL: http://hdl.handle.net/10993/52428.

[80]	Malik Ruzayq M Alsahli, Alex Borgognoni, Luan Cardoso Dos Santos, Hao Cheng, Christian Franck, and Johann Groszschädl. "Lightweight Permutation-Based Cryptography for the Ultra-Low-Power Internet of Things". In: *Innovative Security Solutions for Information Technology and Communications, 15th International Conference, SECITC 2022, Virtual Event, December 8-9, 2022, Revised Selected Papers*. Ed. by Giampaolo Bella, Mihai Doinea, and Helge Janicke. Springer Verlag, 2022-12, pp. 17–36. URL: http://hdl.handle.net/10993/54270.

[81]	Monica Patricia Arenas Correa, Muhammed Ali Bingol, Huseyin Demirci, Georgios Fotiadis, and Gabriele Lenzini. "A Secure Authentication Protocol for Cholesteric Spherical Reflectors using Homomorphic Encryption". In: *Lecture Notes in Computer Science*. Vol. 13503. Springer, 2022-10-06, p. 23. URL: http://hdl.handle.net/10993/52067.

[82]	Yusuf Arslan, Kevin Allix, Clément Lefebvre, Andrey Boytsov, Tegawendé François D Assise Bissyande, and Jacques Klein. "Exploiting Prototypical Explanations for Undersampling Imbalanced Datasets". In: *2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA)*. 2022, pp. 1449–1454. URL: http://hdl.handle.net/10993/54386.

[83]	Yusuf Arslan, Bertrand Lebichot, Kevin Allix, Lisa Veiber, Clement Lefebvre, Andrey Boytsov, et al. "Towards Refined Classifications Driven by SHAP Explanations". In: *Machine Learning and Knowledge Extraction*. Ed. by Andreas Holzinger, Peter Kieseberg, A. Min Tjoa, and Edgar Weippl. Springer, 2022-08-11, pp. 68–81. URL: http://hdl.handle.net/10993/52114.

[84]	Yusuf Arslan, Bertrand Lebichot, Kevin Allix, Lisa Veiber, Clément Lefebvre, Andrey Boytsov, et al. "On the Suitability of SHAP Explanations for Refining Classifications". In: *In Proceedings of the 14th International Conference on Agents and Artificial Intelligence (ICAART 2022)*. 2022-02. URL: http://hdl.handle.net/10993/48926.

[85]	Aryobarzan Atashpendar, Christian Grevisse, Jean Botev, and Steffen Rothkugel. "Semantic and Interactive Search in an Advanced Note-Taking App for Learning Material". In: *Proceedings of the 24th International Conference on Human-Computer Interaction (HCI International)*. Springer, 2022-06. URL: http://hdl.handle.net/10993/51355.

[86]	Fabien Bernier, Matthieu Jimenez, Maxime Cordy, and Yves Le Traon. "Faster and Cheaper Energy Demand Forecasting at Scale". In: *Has it Trained Yet? Workshop at the Conference on Neural Information Processing Systems*. 2022-12-02. URL: http://hdl.handle.net/10993/53152.

[87]	Alexei Biryukov, Luan Cardoso Dos Santos, Daniel Feher, Vesselin Velichkov, and Giuseppe Vitto. "Automated Truncation of Differential Trails and Trail Clustering in ARX". In: *Selected Areas in Cryptography - 28th International Conference, Revised Selected Papers*. Springer, 2022. URL: http://hdl.handle.net/10993/49785.

[88] Alexei Biryukov, Gleb Naumenko, and Sergei Tikhomirov. "Analysis and Probing of Parallel Channels in the Lightning Network". In: *inancial Cryptography and Data Security - 26th International Conference, FC 2022*. Springer, 2022-05-02. URL: http://hdl.handle.net/10993/48066.

[89] Kerstin Bongard, Jean-Louis Sterckx, Arianna Rossi, Verena Distler, Salvador Rivas, and Vincent Koenig. "An (Un)Necessary Evil - Users' (Un)Certainty about Smartphone App Permissions and Implications for Privacy Engineering". In: *2022 7th IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*. IEEE, 2022. URL: http://hdl.handle.net/10993/51593.

[90] Jean Botev and Kirstie Bellman. "A Dialogue on Socio-Technical Systems and Situation Awareness". In: *Proceedings of 12th IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*. 2022. URL: http://hdl.handle.net/10993/52172.

[91] Abdelwahab Boualouache, Taki Eddine Toufik Djaidja, Sidi-Mohammed Senouci, Yacine Ghamri-Doudane, and Thomas Engel. "Deep Learning-based Intra-slice Attack Detection for 5G-V2X Sliced Networks". In: *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*. 2022-08-25. URL: http://hdl.handle.net/10993/53010.

[92] Abdelwahab Boualouache, Thomas Engel, Abdelwahab Boualouache, and Thomas Engel. "Federated Learning-based Inter-slice Attack Detection for 5G-V2X Sliced Networks". In: *2022 IEEE 96th Vehicular Technology Conference: (VTC2022-Fall)*. IEEE, 2022-09. URL: http://hdl.handle.net/10993/54376.

[93] Sergiu Bursuc and Sjouke Mauw. "Contingent payments from two-party signing and verification for abelian groups". In: *Conference Proceedings 2022 IEEE 35th Computer Security Foundations Symposium (CSF)*. IEEE Computer Society, 2022, pp. 179–194. URL: http://hdl.handle.net/10993/53262.

[94] Alessio Buscemi, Ion Turcanu, German Castignani, and Thomas Engel. "On Frame Fingerprinting and Controller Area Networks Security in Connected Vehicles". In: *IEEE Consumer Communications & Networking Conference, Virtual Conference 8-11 January 2022*. 2022-01. URL: http://hdl.handle.net/10993/48391.

[95] Alessio Buscemi, Ion Turcanu, German Castignani, and Thomas Engel. "Preventing Frame Fingerprinting in Controller Area Network Through Traffic Mutation". In: *IEEE ICC 2022 Workshop - DDINS, Seoul 16-20 May 2022*. 2022-05. URL: http://hdl.handle.net/10993/50606.

[96] Ninghan Chen, Xihui Chen, Jun Pang, Liyousew Borga, Conchita d'Ambrosio, and Claus Vögele. "Measuring COVID-19 Vaccine Hesitancy: Consistency of Social Media with Surveys". In: *Proceedings of the 2022 International Conference on Social Informatics*. 2022-10-12, pp. 196–210. URL: http://hdl.handle.net/10993/53570.

[97] Hao Cheng, Georgios Fotiadis, Johann Groszschädl, and Peter Y A Ryan. "Highly Vectorized SIKE for AVX-512". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*. Vol. 2022. Ruhr-Universität Bochum, 2022-02, pp. 41–68. URL: http://hdl.handle.net/10993/52467.

[98] Hao Cheng, Johann Groszschädl, Ben Marshall, Dan Page, and Thinh Pham. "RISC-V Instruction Set Extensions for Lightweight Symmetric Cryptography". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems*. Vol. 2023. Ruhr-Universität Bochum, 2022-11, pp. 193–237. URL: http://hdl.handle.net/10993/54822.

[99] Jean-Sébastien Coron and Agnese Gini. "Provably Solving the Hidden Subset Sum Problem via Statistical Learning". In: *Mathematical Cryptology*. Vol. 1. 2022-03. URL: http://hdl.handle.net/10993/47775.

[100] Jiamin Cui, Kai Hu, Qingju Wang, Meiqin Wang, and Steven Galbraith. "Integral Attacks on Pyjamask-96 and Round-Reduced Pyjamask-128". In: *Topics in Cryptology - CT-RSA 2022 - The Cryptographers' Track at the RSA Conference 2022, San Francisco, CA, USA, February 7-10, 2022, Proceedings*. Springer, 2022, pp. xxx–xxx. URL: http://hdl.handle.net/10993/49482.

[101] Mauro Dalle Lucca Tosi, Vinu Ellampallil Venugopal, and Martin Theobald. "Convergence time analysis of Asynchronous Distributed Artificial Neural Networks". In: *5th Joint International Conference on Data Science Management of Data (9th ACM IKDD CODS and 27th COMAD)*. 2022, pp. 314–315. URL: http://hdl.handle.net/10993/52020.

[102] Renzo Gaston Degiovanni, Mike Papadakis, Renzo Gaston Degiovanni, and Mike Papadakis. "μBert: Mutation Testing using Pre-Trained Language Models". In: *μBert: Mutation Testing using Pre-Trained Language Models*. IEEE, 2022, pp. 160–169. URL: http://hdl.handle.net/10993/51744.

[103] Taki Eddine Toufik Djaidja, Bouziane Brik, Abdelwahab Boualouache, and Sidi Mohammed Senouci. "DRIVE-B5G: A Flexible and Scalable Platform Testbed for B5G-V2X Networks". In: *DRIVE-B5G: A Flexible and Scalable Platform Testbed for B5G-V2X Networks*. 2022-12. URL: http://hdl.handle.net/10993/53070.

[104] Taki Eddine Toufik Djaidja, Bouziane Brik, Abdelwahab Boualouache, and Sidi Mohammed Senouci. "DRIVE-B5G: A Flexible and Scalable Platform Testbed for B5G-V2X Networks". In: *DRIVE-B5G: A Flexible and Scalable Platform Testbed for B5G-V2X Networks*. 2022-12. URL: http://hdl.handle.net/10993/53521.

[105] Xengie Cheng Doan, Annika Selzer, Arianna Rossi, Wilhelmina Maria Botes, and Gabriele Lenzini. "Context, Prioritization, and Unexpectedness: Factors Influencing User Attitudes About Infographic and Comic Consent". In: *Web Conference Companion Volume (ACM)*. ACM, 2022-04-26. URL: http://hdl.handle.net/10993/51193.

[106] Mateusz Dubiel, Sylvain Daronnat, and Luis A. Leiva. "Conversational Agents Trust Calibration: A User-Centred Perspective to Design". In: *Conversational Agents Trust Calibration: A User-Centred Perspective to Design*. 2022. URL: http://hdl.handle.net/10993/51739.

[107] Gabriel Duflo, Grégoire Danoy, El-Ghazali Talbi, and Pascal Bouvry. "A Framework of Hyper-Heuristics based on Q-Learning". In: *International Conference in Optimization and Learning (OLA2022)*. 2022. URL: http://hdl.handle.net/10993/51246.

[108] Elona Marcelle Eugénie DUPONT, Kseniya CHERENKOVA, Anis KACEM, Sk Aziz ALI, Ilya Arzhannikov, Gleb Gusev, et al. "CADOps-Net: Jointly Learning CAD Operation Types and Steps from Boundary-Representations". In: *Proceedings - 2022 International Conference on 3D Vision, 3DV 2022*. Institute of Electrical and Electronics Engineers Inc., 2022. URL: http://hdl.handle.net/10993/58901.

[109] Wolfgang Dvorak, Tjitze Rienstra, Leon van der Torre, and Stefan Woltran. "Non-Admissibility in abstract argumentation". In: *Frontiers in Artificial Intelligence and Applications*. Vol. 353. IOS Press BV, 2022, pp. 128–139. URL: http://hdl.handle.net/10993/54189.

[110] Ehsan Ebrahimi. "Post-quantum Security of Plain OAEP Transform". In: *The International Conference on Practice and Theory of Public-Key Cryptography (PKC), Japan 8-11 March 2022*. 2022-03. URL: http://hdl.handle.net/10993/48606.

[111] Ehsan Ebrahimi and Jeroen van Wier. "Post-quantum Plaintext-awareness". In: *Lecture Notes in Computer Science*. Vol. 13512. Springer, 2022-09-28, pp. 260–285. URL: http://hdl.handle.net/10993/52660.

[112] Martina Fazio, Piergiorgio Vitello, Juan Diego Pineda Jaramillo, Richard Connors, and Francesco Viti. "A Classification Approach Using Machine Learning for Predicting Traffic Flows in Areas with Missing Sensors". In: *Transportation Research Board 101st Annual Meeting*. 2022. URL: http://hdl.handle.net/10993/54423.

[113] Florian Felten, Grégoire Danoy, El-Ghazali Talbi, and Pascal Bouvry. "Metaheuristics-based Exploration Strategies for Multi-Objective Reinforcement Learning". In: *Proceedings of the 14th International Conference on Agents and Artificial Intelligence*. SCITEPRESS - Science and Technology Publications, 2022, pp. 662–673. URL: http://hdl.handle.net/10993/50373.

[114] Florian Felten, El-Ghazali Talbi, and Grégoire Danoy. "MORL/D: Multi-Objective Reinforcement Learning based on Decomposition". In: *International Conference in Optimization and Learning (OLA2022)*. 2022. URL: http://hdl.handle.net/10993/51247.

[115] Christof Ferreira Torres, Hugo Jonker, and Radu State. "Elysium: Context-Aware Bytecode-Level Patching to Automatically Heal Vulnerable Smart Contracts". In: *International Symposium on Research in Attacks, Intrusions and Defenses, Limassol, Cyprus 26-28 October 2022*. 2022. URL: http://hdl.handle.net/10993/51740.

[116] Salah Ghamizi, Maxime Cordy, Mike Papadakis, and Yves Le Traon. "Adversarial Robustness in Multi-Task Learning: Promises and Illusions". In: *Proceedings of the thirty-Sixth AAAI Conference on Artificial Intelligence (AAAI-22)*. 2022. URL: http://hdl.handle.net/10993/48724.

[117] Salah Ghamizi, Maxime Cordy, Mike Papadakis, and Yves Le Traon. "On Evaluating Adversarial Robustness of Chest X-ray Classification: Pitfalls and Best Practices". In: *The Thirty-Seventh AAAI Conference on Artificial Intelligence (AAAI- 23) - SafeAI Workshop, Washington, D.C., Feb 13-14, 2023*. 2022. URL: http://hdl.handle.net/10993/53623.

[118] Reynaldo Gil Pons, Ross James Horne, Sjouke Mauw, Rolando Trujillo-Rasua, and Alwen Tiu. "Is Eve nearby? Analysing protocols under the distant-attacker assumption". In: *IEEE Computer Security Foundations Symposium, August 7 - 10, 2022, Haifa, Israel*. 2022. URL: http://hdl.handle.net/10993/50132.

[119] Kristian Gjosteen, Thomas Haines, Johannes Mueller, Peter Roenne, and Tjerand Silde. "Verifiable Decryption in the Head". In: *ACISP 2022*. 2022. URL: http://hdl.handle.net/10993/51841.

[120] Christian Grevisse. "Flash, who? On the Obsolescence of Digital Technology and Its Impact on E-learning Applications: A Case Study." In: *Proceedings of the XVII Latin American Conference on Learning Technologies (LACLO)*. IEEE, 2022-10. URL: http://hdl.handle.net/10993/53403.

[121] Martin Gubri, Maxime Cordy, Mike Papadakis, Yves Le Traon, and Koushik Sen. "Efficient and Transferable Adversarial Examples from Bayesian Neural Networks". In: *The 38th Conference on Uncertainty in Artificial Intelligence*. 2022. URL: http://hdl.handle.net/10993/49232.

[122] Martin Gubri, Maxime Cordy, Mike Papadakis, Yves Le Traon, and Koushik Sen. "LGV: Boosting Adversarial Example Transferability from Large Geometric Vicinity". In: *Computer Vision – ECCV 2022*. Springer Nature Switzerland, 2022, pp. 603–618. URL: http://hdl.handle.net/10993/53418.

[123] Sarra Habchi, Guillaume Haben, Mike Papadakis, Maxime Cordy, and Yves Le Traon. "A Qualitative Study on the Sources, Impacts, and Mitigation Strategies of Flaky Tests". In: *A Qualitative Study on the Sources, Impacts, and Mitigation Strategies of Flaky Tests*. 2022-04. URL: http://hdl.handle.net/10993/55847.

[124] Sarra Habchi, Guillaume Haben, Jeongju Sohn, Adriano Franci, Mike Papadakis, Maxime Cordy, et al. "What Made This Test Flake? Pinpointing Classes Responsible for Test Flakiness". In: *What Made This Test Flake? Pinpointing Classes Responsible for Test Flakiness*. 2022-10. URL: http://hdl.handle.net/10993/55849.

[125] Guillaume HELBECQUE, Jan GMYS, Tiago CARNEIRO PESSOA, Nouredine MELAB, and Pascal BOUVRY. "A performance-oriented comparative study of the Chapel high-productivity language to conventional programming environments". In: *PMAM '22: Proceedings of the Thirteenth International Workshop on Programming Models and Applications for Multicores and Manycores*. Association for Computing Machinery, 2022-04-18, pp. 21–29. URL: http://hdl.handle.net/10993/55211.

[126] Sviatlana Hoehn, Sjouke Mauw, and Nicholas Asher. "BelElect: A New Dataset for Bias Research from a "Dark" Platform". In: *Vol. 16 (2022): Proceedings of the Sixteenth International AAAI Conference on Web and Social Media*. AAAI, 2022. URL: http://hdl.handle.net/10993/52563.

[127] Nicolas Huber, Ralf Kuesters, Toomas Krips, Julian Liedtke, Johannes Mueller, Daniel Rausch, et al. "Kryvos: Publicly Tally-Hiding Verifiable E-Voting". In: *2022 ACM SIGSAC Conference on Computer and Communications Security*. 2022. URL: http://hdl.handle.net/10993/52513.

[128] Soheil Human, Martin Degeling, Christiana Santos, Harshvardhan Pandit, Morel, Arianna Rossi, et al. "Data Protection and Consenting Communication Mechanisms: Current Proposals and Challenges". In: *IEEE eXplore*. 2022-06-06. URL: http://hdl.handle.net/10993/51194.

[129] Ahmet Serdar Karadeniz, Sk Aziz Ali, Anis Kacem, Elona Dupont, Djamila Aouada, Ahmet Serdar Karadeniz, et al. "TSCom-Net: Coarse-to-Fine 3D Textured Shape Completion Network". In: *TSCom-Net: Coarse-to-Fine 3D Textured Shape Completion Network*. 2022. URL: http://hdl.handle.net/10993/52299.

[130] Patrick Keller and Nicolas Navet. "Approximating WCRT through the aggregation of short simulations with different initial conditions: application to TSN". In: *30th International Conference on Real-Time Networks and Systems (RTNS '22)*. 2022-06. URL: http://hdl.handle.net/10993/51041.

[131] Ahmed Khanfir, Matthieu Jimenez, Mike Papadakis, and Yves Le Traon. "CODEBERT-NT: code naturalness via CodeBERT". In: *22nd IEEE International Conference on Software Quality, Reliability and Security (QRS'22)*. 2022-12-05. URL: http://hdl.handle.net/10993/53506.

[132] Emmanuel Kieffer, Gabriel Duflo, Grégoire Danoy, Sébastien Varrette, and Pascal Bouvry. "A RNN-Based Hyper-Heuristic for Combinatorial Problems". In: *A RNN-Based Hyper-Heuristic for Combinatorial Problems*. 2022. URL: http://hdl.handle.net/10993/51074.

[133] Sybren de Kinderen, Qin Ma, Monika Kaczmarek-Heß, and Rik Eshuis. "Beyond Business Development: Regulatory Assessment of Energy Sector Projects with Contextual Requirements Engineering". In: *Lecture Notes in Business Information Processing*. Springer, 2022, pp. 183–198. URL: http://hdl.handle.net/10993/53305.

[134] Aleks Knoks and Thomas Raleigh. "XAI and philosophical work on explanation: A roadmap". In: *Proceedings of 1st Workshop on Bias, Ethical AI, Explainability and the Role of Logic and Logic Programming*. Vol. 3319. CEUR-WS.org, 2022, pp. 101–106. URL: http://hdl.handle.net/10993/53884.

[135] Utkarsh Kunwar, Sheetal Borar, Moritz Berghofer, Julia Kylmälä, Ilhan Aslan, Luis A. Leiva, et al. "Robust and Deployable Gesture Recognition for Smartwatches". In: *Proceedings of the ACM Conference on Intelligent User Interfaces (IUI)*. 2022. URL: http://hdl.handle.net/10993/50487.

[136] Kayhan Latifzadeh and Luis A. Leiva. "Gustav: Cross-device Cross-computer Synchronization of Sensory Signals". In: *Adjunct Proceedings of the 35th Annual ACM Symposium on User Interface Software and Technology*. 2022. URL: http://hdl.handle.net/10993/51958.

[137] Sami Lazreg, Vladyslav Bohlachov, Loveneesh Rana, Andreas Hein, and Maxime Cordy. "Variability-Aware Design of Space Systems: Variability Modelling, Configuration Workflow and Research Directions". In: *Proceedings of VAMOS 22*. 2022-02. URL: http://hdl.handle.net/10993/54244.

[138] Guiyin Li, Fengyi Zhu, Jun Pang, Tian Zhang, Minxue Pan, and Xuandong Li. "Functional scenario classification for Android applications using GNNs". In: *Proceedings of the 13th Asia-Pacific Symposium on Internetware*. ACM, 2022, pp. 1–9. URL: http://hdl.handle.net/10993/52116.

[139] Xu Li, Dov M. Gabbay, and Réka Markovich. "Dynamic Deontic Logic for Permitted Announcements". In: *19th International Conference on Principles of Knowledge Representation and Reasoning, KR 2022*. International Joint Conferences on Artificial Intelligence, 2022, pp. 226–235. URL: http://hdl.handle.net/10993/54258.

[140] Tomer Libal. "The LegAi Editor: A Tool for the Construction of Legal Knowledge Bases". In: *Legal Knowledge and Information Systems - JURIX 2022: The Thirty-fifth Annual Conference, Saarbrücken, Germany, 14-16 December 2022. Frontiers in Artificial Intelligence and Applications 362, IOS Press 2022*. 2022. URL: http://hdl.handle.net/10993/53269.

[141] Tomer Libal and Tereza Novotná. "An Evaluation of Methodologies for Legal Formalization". In: *Lecture Notes in Computer Science 13283, Springer 2022,* 2022. URL: http://hdl.handle.net/10993/53302.

[142] Davide Liga and Monica Palmirani. "Transfer Learning for Deontic Rule Classification: the Case Study of the GDPR". In: *INTERNATIONAL CONFERENCE ON LEGAL KNOWLEDGE AND INFORMATION SYSTEMS, Saarbrücken 14-16 December 2022*. EasyChair, 2022. URL: http://hdl.handle.net/10993/53791.

[143] Cedric Lothritz, Bertrand Lebichot, Kevin Allix, Lisa Veiber, Tegawendé François D Assise Bissyande, Jacques Klein, et al. "LuxemBERT: Simple and Practical Data Augmentation in Language Model Pre-Training for Luxembourgish". In: *Proceedings of the Language Resources and Evaluation Conference, 2022*. 2022-06, pp. 5080–5089. URL: http://hdl.handle.net/10993/51815.

[144] Jieting Luo, Beishui Liao, and Dov M. Gabbay. "Value-based practical reasoning: Modal Logic + Argumentation". In: *Frontiers in Artificial Intelligence and Applications*. Vol. 353. IOS Press BV, 2022, pp. 248–259. URL: http://hdl.handle.net/10993/54257.

[145] Wei Ma, Mengjie Zhao, Ezekiel Soremekun, Qiang Hu, Jie M. Zhang, Mike Papadakis, et al. "GraphCode2Vec: generic code embedding via lexical and program dependence analyses". In: *Proceedings of the 19th International Conference on Mining Software Repositories*. 2022-05-22, pp. 524–536. URL: http://hdl.handle.net/10993/53862.

[146] David Mestel. "Beware of Greeks bearing entanglement? Quantum covert channels, information flow and non-local games". In: *35th IEEE Computer Security Foundations Symposium*. 2022. URL: http://hdl.handle.net/10993/51245.

[147] David Mestel, Johannes Mueller, and Pascal Reisert. "How Efficient are Replay Attacks against Vote Privacy? A Formal Quantitative Analysis". In: *35th IEEE Computer Security Foundations Symposium*. 2022. U R L: http://hdl.handle.net/10993/51209.

[148] Johannes Mueller. "Breaking and Fixing Vote Privacy of the Estonian E-Voting Protocol IVXV". In: *Workshop on Advances in Secure Electronic Voting 2022*. 2022. U R L: http://hdl.handle.net/10993/49442.

[149] Amro Najjar, Nina Hosseini Kivanani, Igor Tchappi Haman, Yazan Mualla, Egberdien Van der Peijl, Daniel Karpati, et al. "XAI: Using Smart Photobooth for Explaining History of Art". In: *XAI: Using Smart Photobooth for Explaining History of Art*. 2022-12, pp. 256–259. U R L: http://hdl.handle.net/10993/53192.

[150] Fernando Kaway Carvalho Ota, Farouk Damoun, Sofiane Lagraa, Patricia Becerra-Sanchez, Jean Hilger, Radu State, et al. "Event-Driven Interest Detection for Task-Oriented Mobile Apps". In: *Mobile and Ubiquitous Systems: Computing, Networking and Services*. Springer International Publishing, 2022, pp. 582–598. U R L: http://hdl.handle.net/10993/55185.

[151] Stéven Picard and Jean Botev. "Rhythmic Stimuli Effects on Subjective Time Perception in Immersive Virtual Environments". In: *Proceedings of the 13th ACM Multimedia Systems Conference (MMSys)*. 2022. U R L: http://hdl.handle.net/10993/52490.

[152] Yihao Qin, Shangwen Wang, Kui Liu, Bo Lin, Hongjun Wu, Li Li, et al. "PEELER: Learning to Effectively Predict Flakiness without Running Tests". In: *Proceedings of the 38th IEEE International Conference on Software Maintenance and Evolution*. 2022-10, pp. 1–12. U R L: http://hdl.handle.net/10993/52227.

[153] François Robinet, Claudia Parera, Christian Hundt, and Raphaël Frank. "Weakly-Supervised Free Space Estimation through Stochastic Co-Teaching". In: *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV) Workshops, 2022*. 2022-01-04, pp. 618–627. U R L: http://hdl.handle.net/10993/50199.

[154] Arianna Rossi, Regis Chatellier, Stefano Leucci, Rossana Ducato, and Estelle Hary. "What if data protection embraced foresight and speculative design?" In: *DRS2022: Bilbao*. 2022. U R L: http://hdl.handle.net/10993/52739.

[155] Arianna Rossi, Archana Kumari, and Gabriele Lenzini. "Unwinding a Legal and Ethical Ariadne's Thread Out of the Twitter Scraping Maze". In: *Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT)*. Ed. by Stefan Schiffner, Sebastien Ziegler, and Adrian Quesada Rodriguez. Springer, 2022, pp. 179–203. U R L: http://hdl.handle.net/10993/52830.

[156] Jordan Samhi, Tegawendé François D Assise Bissyande, and Jacques Klein. "TriggerZoo: A Dataset of Android Applications Automatically Infected with Logic Bombs". In: *19th International Conference on Mining Software Repositories, Data Showcase, (MSR 2022)*. 2022-05-23. U R L: http://hdl.handle.net/10993/50528.

[157] Jordan Samhi, Jun Gao, Nadia Daoudi, Pierre Graux, Henri Hoyez, Xiaoyu Sun, et al. "JuCify: A Step Towards Android Code Unification for Enhanced Static Analysis". In: *44th International Conference on Software Engineering (ICSE 2022)*. 2022-05-21. U R L: http://hdl.handle.net/10993/49267.

[158] Jordan Samhi, Li Li, Tegawendé François D Assise Bissyande, and Jacques Klein. "Difuzer: Uncovering Suspicious Hidden Sensitive Operations in Android Apps". In: *44th International Conference on Software Engineering (ICSE 2022)*. 2022-05-21. U R L: http://hdl.handle.net/10993/49268.

[159] Aymene Selamnia, Bouziane Brik, Sidi-Mohammed Senouci, and Abdelwahab Boualouache. "Edge Computing enabled Intrusion Detection for C-V2X Networks using Federated Learning". In: *The 2022 IEEE Global Communications Conference (GLOBECOM)*. 2022-12. URL: http://hdl.handle.net/10993/53069.

[160] Aymene Selamnia, Bouziane Brik, Sidi-Mohammed Senouci, Abdelwahab Boualouache, and Shajjad Hossain. "Edge Computing-enabled Intrusion Detection for C-V2X Networks using Federated Learning". In: *The 2022 IEEE Global Communications Conference (GLOBECOM)*. 2022-12. URL: http://hdl.handle.net/10993/53520.

[161] Thibault Jean Angel Simonetto, Salijona Dyrmishi, Salah Ghamizi, Maxime Cordy, and Yves Le Traon. "A Unified Framework for Adversarial Attack and Defense in Constrained Feature Space". In: *Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence, IJCAI-22*. International Joint Conferences on Artificial Intelligence Organization, 2022, pp. 1313–1319. URL: http://hdl.handle.net/10993/53045.

[162] Joshgun Sirajzade, Pascal Bouvry, and Christoph Schommer. "Deep Mining Covid-19 Literature". In: *Applied Informatics, 5th International Conference, ICAI 2022, Arequipa, Peru, October 27–29, 2022, Proceedings*. Springer Cham, 2022, pp. 121–133. URL: http://hdl.handle.net/10993/52855.

[163] Maciej Skorski, Alessandro Temperoni, and Martin Theobald. "Robust and Provable Guarantees for Sparse Random Embeddings". In: *Advances in Knowledge Discovery and Data Mining - 26th Pacific-Asia Conference, PAKDD 2022, Chengdu, China, May 16-19, 2022, Proceedings, Part II*. Springer, 2022-05-18, pp. 211–223. URL: http://hdl.handle.net/10993/53911.

[164] Badr Souani, Ahmed Khanfir, Alexandre Bartel, Kevin Allix, Yves Le Traon, and Zhou Jianying. "Android Malware Detection Using BERT". In: *Applied Cryptography and Network Security Workshops*. Springer, 2022-09-24, pp. 575–591. URL: http://hdl.handle.net/10993/52627.

[165] Daniel Stolfi Rosso and Grégoire Danoy. "Optimising Autonomous Robot Swarm Parameters for Stable Formation Design". In: *Proceedings of the Genetic and Evolutionary Computation Conference*. 2022-07-08, pp. 1281–1289. URL: http://hdl.handle.net/10993/52967.

[166] Ningyuan Sun, Jean Botev, Yara Khaluf, and Pieter Simoens. "Theory of Mind and Delegation to Robotic Virtual Agents". In: *Proceedings of the 31st IEEE International Conference on Robot and Human Interactive Communication (RO-MAN)*. 2022. URL: http://hdl.handle.net/10993/52171.

[167] Zeyu Sun, JieM. Zhang, Yingfei Xiong, Mark Harman, Mike PAPADAKIS, and Lu Zhang. "Improving Machine Translation Systems via Isotopic Replacement". In: *ICSE '22: Proceedings of the 44th International Conference on Software Engineering*. 2022, pp. 1181–1192. URL: http://hdl.handle.net/10993/57662.

[168] Pierre Talbot, Frederic Pinel, and Pascal Bouvry. "A Variant of Concurrent Constraint Programming on GPU". In: *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 36. 2022-06, pp. 3830–3839. URL: http://hdl.handle.net/10993/51988.

[169] Amal Tawakuli and Thomas Engel. "The Impact Of Distributed Data Preprocessing On Automotive Data Streams". In: *2022 IEEE 96th Vehicular Technology Conference: (VTC2022-Fall)*. IEEE, 2022-09. URL: http://hdl.handle.net/10993/52313.

[170] Amal Tawakuli, Daniel Kaiser, and Thomas Engel. "Transforming IoT Data Preprocessing: A Holistic, Normalized and Distributed Approach". In: *The Fifth International Workshop on Data: Acquisition To Analysis*. 2022. URL: http://hdl.handle.net/10993/52454.

[171] Jan Thoemel, Panagiotis Karakatsanis, Mariusz Ludwikowski, Rui Zong, Rodrigo Lucas Weber, Rudolf Schmidt, et al. "Mission to Mars Using Space-Sourced Propellant". In: *Proceedings of the International Astronautical Congress, IAC*. 2022. URL: http://hdl.handle.net/10993/52663.

[172] Haoye Tian, Xunzhu Tang, Andrew Habib, Shangwen Wang, Kui Liu, Xin Xia, et al. "Is this Change the Answer to that Problem? Correlating Descriptions of Bug and Code Changes for Evaluating Patch Correctness". In: *Is this Change the Answer to that Problem? Correlating Descriptions of Bug and Code Changes for Evaluating Patch Correctness*. 2022. URL: http://hdl.handle.net/10993/52135.

[173] Haoye Tian, Xunzhu Tang, Andrew Habib, Shangwen Wang, Kui Liu, Xin Xia, et al. "Is this Change the Answer to that Problem? Correlating Descriptions of Bug and Code Changes for Evaluating Patch Correctness". In: *Is this Change the Answer to that Problem? Correlating Descriptions of Bug and Code Changes for Evaluating Patch Correctness*. 2022. URL: http://hdl.handle.net/10993/52538.

[174] Juan Carlos de la Torre, José Miguel Aragó-Jurado, Javier Jareño, Sébastien Varrette, and Bernabe Dorronsoro. "Obfuscating LLVM Intermediate Representation Source Code with NSGA-II". In: *15th Intl. Conf. on Computational Intelligence in Security for Information Systems (CISIS'22)*. Springer, 2022-09. URL: http://hdl.handle.net/10993/51829.

[175] Sébastien Varrette, Hyacinthe Cartiaux, Sarah Peter, Emmanuel Kieffer, Teddy Valette, and Abatcha Olloh. "Management of an Academic HPC Research Computing Facility: The ULHPC Experience 2.0". In: *6th High Performance Computing and Cluster Technologies Conference (HPCCT 2022)*. Association for Computing Machinery (ACM), 2022-07. URL: http://hdl.handle.net/10993/51857.

[176] Sébastien Varrette, Hyacinthe Cartiaux, Teddy Valette, and Abatcha Olloh. "Aggregating and Consolidating two High Performant Network Topologies: The ULHPC Experience". In: *ACM Practice and Experience in Advanced Research Computing (PEARC'22)*. Association for Computing Machinery (ACM), 2022-07. URL: http://hdl.handle.net/10993/51828.

[177] Sébastien Varrette, Emmanuel Kieffer, and Frederic Pinel. "Optimizing the Resource and Job Management System of an Academic HPC and Research Computing Facility". In: *21st IEEE Intl. Symp. on Parallel and Distributed Computing (ISPDC'22)*. IEEE Computer Society, 2022-07. URL: http://hdl.handle.net/10993/51494.

[178] Giuseppe Vitto and Alexei Biryukov. "Dynamic Universal Accumulator with Batch Update over Bilinear Groups". In: *Topics in Cryptology - CT-RSA 2022 - Cryptographers' Track at the RSA Conference 2022*. Springer, 2022. URL: http://hdl.handle.net/10993/49497.

[179] Shaun Wallace, Tianyuan Cai, Brendan Le, and Luis A. Leiva. "Debiased Label Aggregation for Subjective Crowdsourcing Tasks". In: *Extended Abstracts of the SIGCHI Conference on Human Factors in Computing Systems (CHI EA)*. 2022. URL: http://hdl.handle.net/10993/50486.

[180] Aoran Wang and Jun Pang. "Iterative structural inference of directed graphs". In: *Proceedings of the 36th Annual Conference on Neural Information Processing Systems (NeurIPS'22)*. 2022. URL: http://hdl.handle.net/10993/54290.

[181] Ben Weintraub, Christof Ferreira Torres, Cristina Nita-Rotaru, and Radu State. "A Flash(bot) in the Pan: Measuring Maximal Extractable Value in Private Pools". In: *ACM Internet Measurement Conference, Nice, France 25-27 October 2022*. 2022. URL: http://hdl.handle.net/10993/52579.

[182] Elliott Wobler, Bohlachov Vladyslav, Tiago Sousa, Balazs Farkas, Spyridon Skevas, and Jan Thoemel. "The "Daffodil" Mission: GNSS-Reflectometry with a 1.5U Cube-Sat". In: *Proceedings of the 73rd International Astronautical Congress*. International Astronautical Federation, 2022. URL: http://hdl.handle.net/10993/52664.

[183] Liuwen Yu and Dov M. Gabbay. "Case-Based Reasoning via Comparing the Strength Order of Features". In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Vol. 13283 LNAI. Springer Science and Business Media Deutschland GmbH, 2022, pp. 143–151. URL: http://hdl.handle.net/10993/54259.

[184] Liuwen Yu, Mirko Zichichi, Réka Markovich, and Amro Najjar. "Enhancing Trust in Trust Services: Towards an Intelligent Human-input-based Blockchain Oracle (IHiBO)". In: *Proceedings of the 55th Annual Hawaii International Conference on System Sciences*. 2022-01. URL: http://hdl.handle.net/10993/50022.

[185] Liuwen Yu, Mirko Zichichi, Réka Markovich, and Amro Najjar. "Intelligent Human-input-based Blockchain Oracle (IHiBO)". In: *Proceedings of the 14th International Conference on Agents and Artificial Intelligence, ICAART 2022, Volume 1*. 2022. URL: http://hdl.handle.net/10993/54249.

[186] Olivier Georges Rémy Zeyen and Jun Pang. "Target Control of Boolean Networks with Permanent Edgetic Perturbations". In: *Proceedings of the 61st International Conference on Decision and Control (CDC 2022)*. IEEE, 2022, pp. 4236–4243. URL: http://hdl.handle.net/10993/54016.

[187] Marzena Zygis, Sarah Wesolek, Nina Hosseini Kivanani, and Manfred Krifka. "The Prosody of Cheering in Sport Events". In: *Proc. Interspeech 2022*. 2022-09, pp. 5283–5287. URL: http://hdl.handle.net/10993/52712.

A.5 Theses

[188] Opeyemi Priscilla Akinyemi. ""Dark Cookie" - A serious game to train users to spot and interact with dark patterns in cookie banners". MA thesis. Unilu - University of Luxembourg, 2022-08-29. URL: http://hdl.handle.net/10993/52802.

[189] Ilaria Angela Amantea. "Methods and tools for analysis and management of risks and regulatory compliance in the healthcare sector: the Hospital at Home – HaH". PhD thesis. Unilu - University of Luxembourg, 2022-06-16. URL: http://hdl.handle.net/10993/52167.

[190] Jim Jean-Pierre Barthel. "TOPICS IN COMPUTATIONAL NUMBER THEORY AND CRYPTANALYSIS - On Simultaneous Chinese Remaindering, Primes, the MiNTRU Assumption, and Functional Encryption". PhD thesis. Unilu - University of Luxembourg, 2022-09-02. URL: http://hdl.handle.net/10993/52658.

[191] Paul-Lou Benedick. "Towards a Unified and Robust Data-Driven Approach. A Digital Transformation of Production Plants in the Age of Industry 4.0". PhD thesis. Unilu - University of Luxembourg, 2022-04-27. URL: http://hdl.handle.net/10993/50919.

[192] Alessio Buscemi. "Automation of Controller Area Network Reverse Engineering: Approaches, Opportunities and Security Threats". PhD thesis. Unilu - University of Luxembourg, 2022-03-04. URL: http://hdl.handle.net/10993/50805.

[193] Tong Cao. "ANALYZING THE PRIVACY AND SECURITY OF PROOF-OF-WORK CRYPTOCURRENCIES". PhD thesis. Unilu - University of Luxembourg, 2022-02-25. URL: http://hdl.handle.net/10993/50653.

[194] Luan Cardoso Dos Santos. "Design, Cryptanalysis and Protection of Symmetric Encryption Algorithms". PhD thesis. Unilu - University of Luxembourg, 2022. URL: http://hdl.handle.net/10993/52955.

[195] Ioana Raluca Chitic. "Evolutionary Algorithm-based Adversarial Attacks Against Image Classification Convolutional Neural Networks". PhD thesis. Unilu - University of Luxembourg, 2022-10-13. URL: http://hdl.handle.net/10993/52582.

[196] Claudio Cimarelli. "PERCEPTION FOR SURVEILLANCE: LEARNING SELF-LOCALISATION AND INTRUDERS DETECTION FROM MONOCULAR IMAGES OF AN AERIAL ROBOT IN OUTDOOR URBAN ENVIRONMENTS". PhD thesis. Unilu - University of Luxembourg, 2022. URL: http://hdl.handle.net/10993/52554.

[197] Aditya Shyam Shankar Damodaran. "Protocols for Stateful Zero-Knowledge". PhD thesis. Unilu - University of Luxembourg, 2022-11-17. URL: http://hdl.handle.net/10993/53066.

[198] Fatima Ezzahra El Orche. "New Security Primitives and Better Performance through Parameter Trade-Offs". PhD thesis. Ecole Normale Supérieure of Paris, 2022-10-25. URL: http://hdl.handle.net/10993/53433.

[199] Christof Ferreira Torres. "From Smart to Secure Contracts: Automated Security Assessment and Improvement of Ethereum Smart Contracts". PhD thesis. Unilu - University of Luxembourg, 2022. URL: http://hdl.handle.net/10993/51118.

[200] Salah Ghamizi. "Multi-objective Robust Machine Learning For Critical Systems With Scarce Data". PhD thesis. Unilu - University of Luxembourg, 2022-09-07. URL: http://hdl.handle.net/10993/52248.

[201] Agnese Gini. "On the hardness of the hidden subset sum problem: algebraic and statistical attacks". PhD thesis. Unilu - University of Luxembourg, 2022-07-07. URL: http://hdl.handle.net/10993/51778.

[202] Shohreh Haddadan. "ARGUMENT MINING AND ITS APPLICATIONS IN POLITICAL DEBATES". PhD thesis. Unilu - University of Luxembourg, 2022-04-04. URL: http://hdl.handle.net/10993/50959.

[203] Benjamin Jahic. "SEMKIS: A CONTRIBUTION TO SOFTWARE ENGINEERING METHODOLOGIES FOR NEURAL NETWORK DEVELOPMENT". PhD thesis. Unilu - University of Luxembourg, 2022-04-05. URL: http://hdl.handle.net/10993/50986.

[204] Ekaterina Kamlovskaya. "Australian Indigenous Life Writing: Analysing Discourses with Word Embedding Modelling". PhD thesis. Unilu - University of Luxembourg, 2022-10-28. URL: http://hdl.handle.net/10993/50751.

[205] Laurent Lesage. "Data Analysis for Insurance: Recommendation System Based on a Multivariate Hawkes Process". PhD thesis. Unilu - University of Luxembourg, 2022-04-26. URL: http://hdl.handle.net/10993/51179.

[206] Davide Liga. "Hybrid Artificial Intelligence to extract patterns and rules from argumentative and legal texts". PhD thesis. UNIBO - Università di Bologna, 2022-06-16. URL: http://hdl.handle.net/10993/52142.

[207] Bowen Liu. "Post-quantum Remote Device Authentication and Data Analysis Protocols for IoT". PhD thesis. Unilu - University of Luxembourg, 2022-10-17. URL: http://hdl.handle.net/10993/54188.

[208] Philippe Ludivig. "Figuring out where you are on the Moon: The selection and validation of different pose-estimation techniques for lunar surface robotics." PhD thesis. Unilu - University of Luxembourg, 2022-03-14. URL: http://hdl.handle.net/10993/52050.

[209] Xavier Mazur. "Controllability of complex flow networks". PhD thesis. Unilu - University of Luxembourg, 2022-02-25. URL: http://hdl.handle.net/10993/51162.

[210] Ludovica Paseri. "The European Approach to Open Science and Research Data". PhD thesis. Unilu - University of Luxembourg, 2022-06-17. URL: http://hdl.handle.net/10993/51952.

[211] Inês Pinto Gouveia. "Architectural Support for Hypervisor-Level Intrusion Tolerance in MPSoCs". PhD thesis. Unilu - University of Luxembourg, 2022-02-21. URL: http://hdl.handle.net/10993/50822.

[212] Ines Pinto Gouveia. "Architectural Support for Hypervisor-Level Intrusion Tolerance in MPSoCs". PhD thesis. Unilu - University of Luxembourg, 2022-02-21. URL: http://hdl.handle.net/10993/50866.

[213] Julien Polge. "Investigating the Industry 4.0 paradigm change in brownfield manufacturing facilities: from data-driven approaches to blockchain-based traceability". PhD thesis. Unilu - University of Luxembourg, 2022-07-01. URL: http://hdl.handle.net/10993/51575.

[214] Ahmad Rida. "APPLICATION OF NEAR FIELD TECHNOLOGY IN HEAVY COMMERCIAL VEHICLE TIRE MONITORING SYSTEM". PhD thesis. Unilu - University of Luxembourg, 2022-09-08. URL: http://hdl.handle.net/10993/53249.

[215] Timothée Riom. "A Software Vulnerabilities Odysseus: Analysis, Detection, and Mitigation". PhD thesis. Unilu - University of Luxembourg, 2022-09-28. URL: http://hdl.handle.net/10993/52875.

[216] François Robinet. "Minimizing Supervision for Vision-Based Perception and Control in Autonomous Driving". PhD thesis. Unilu - University of Luxembourg, 2022-10-04. URL: http://hdl.handle.net/10993/52331.

[217] Najmeh Soroush. "Verifiable, Secure and Privacy-Preserving Computation". PhD thesis. Unilu - University of Luxembourg, 2022-03-22. URL: http://hdl.handle.net/10993/51452.

[218] Tiago Sousa. "Modeling and Predicting the Resilience of Ecosystems". MA thesis. Unilu - University of Luxembourg, 2022-09. URL: http://hdl.handle.net/10993/54865.

[219] Lorenzo Spignoli. "Side-Channel Countermeasures in the Probing Model". PhD thesis. Unilu - University of Luxembourg, 2022-11-22. URL: http://hdl.handle.net/10993/54486.

[220] Borce Stojkovski. "User Experience Design for Cybersecurity & Privacy: addressing user misperceptions of system security and privacy". PhD thesis. Unilu - University of Luxembourg, 2022-04-26. URL: http://hdl.handle.net/10993/50982.

[221] Amal Tawakuli. "TRANSFORMING DATA PREPROCESSING: A HOLISTIC, NORMALIZED AND DISTRIBUTED APPROACH". PhD thesis. Unilu - University of Luxembourg, 2022-09-26. URL: http://hdl.handle.net/10993/52262.

[222] Giuseppe Vitto. "Security, Scalability and Privacy in Applied Cryptography". PhD thesis. Unilu - University of Luxembourg, 2022. URL: http://hdl.handle.net/10993/50228.

[223] Zhiqiang Zhong. *Leveraging Graph Machine Learning for Social Network Analysis*. 2022-04-04. URL: http://hdl.handle.net/10993/50811.

Research Projects

This chapter lists research projects that were ongoing during 2022, and whose principal investigator is a DCS member. It is structured to summarize the projects by funding source.

- EC - Erasmus+ - KA2
- EC - ERASMUS-EMJM-UN
- EC - EIC Pathfinder
- EC - ERC - Stg
- EC - H2020
- EC - H2020 and MECO
- EC - H2020 - FET Open
- EC - H2020 - Marie Curie
- EC - H2020 FET - ERA-NET Cofund
- EC - HEU
- EC - JUST
- ESA
- EU - COST Action
- FNR
- FNR - AFR
- FNR - AFR PhD
- FNR - AFR PhD and ILNAS
- FNR - Bridges
- FNR - CORE
- FNR - CORE - Core International
- FNR - CORE - Core Junior
- FNR - Industrial Fellowships
- FNR - INTER
- FNR - INTER MOBILITY
- FNR - JUMP
- FNR - OPEN
- FNR - PRIDE
- FNR (Luxembourg)/NCBiR (Poland)
- UL
- UL and Esch2022
- UL - University of Luxembourg - Institute for Advanced Studies (IAS) - Audacious projects
- Other Funding Source

B.1   EC - Erasmus+ - KA2 Projects

Modernisation of Higher Education in central Asia through new technologies

 https://hiedtec.ecs.uni-ruse.bg/?cmd=gsIndex

Acronym:	HiedTec
Reference:	R-AGR-3536-10
PI:	Thomas ENGEL
Funding:	European Commission - Erasmus+ - Key Action 2: Cooperation for innovation and the exchange of good practices
Budget:	988.773,00 €
Duration:	15 Nov 2018 – 14 Nov 2022
Members:	• Thomas ENGEL (Principal Investigator) • Aurel MACHALEK (Researcher) • Stefanie OESTLUND (Project Coordinator) • Latif LADID (Program Coordinator)
Area:	Communicative Systems
Partners:	• Ala-Too Intenational University • Almaty Technological University • Andijan Machine-Building Institute • Innovativa University of Euroasia • International University for the Humanities and Development • Issykkul State University named after K. Tynystanov • Khorog State University • Kyrgyz State Technical University • L.N.Gumilyov Euroasian National University • Ministry of Education and Science of the Kyrgyz Republic • Ministry of Education and Science of the Rep. of Kazakhstan • Ministry of Education and Science of the Rep. of Tajikistan • Ministry of Education of Turkmenistan Turkmenistan • Ministry of Higher and Secondary specialized education • Oguz Han Engineering and Technology University • State Power Engineering Institute of Turkmenistan • Tajik Technical University • Tashkent State University of Economics • Tashkent University of Information Technology • Technological University of Tajikistan • University of Coimbra • University of Pavia • University of Russe

Description

In order to respond to:

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

Main project outcomes and products:

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

Impact:

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

Results

The project ”Modernization of Higher Education in Central Asia through New Technologies” had the main aim of developing concepts for adapting the educational system to the digital generation, while considering the specific conditions of each partner country and creating centers for innovative educational technologies. The Secan-lab research group contributed mainly to the creation of a sustainable academic network for sharing experiences and exchanging good practices in the field of innovative educational technologies and didactic models. The project finished in December 2022.

B.2   EC - ERASMUS-EMJM-UN Projects

Erasmus Mundus Joint Master in Cybersecurity

Acronym:	CYBERUS
Reference:	U-AGR-8123-00 (10)
PI:	Tegawendé François d Assise BISSYANDE
Funding:	European Commission - Erasmus Mundus Joint Masters
Budget:	5.174.400,00 €
Duration:	1 Jan 2022 – 31 Dec 2026
Members:	• Tegawendé François d Assise BISSYANDE (Principal Investigator) • Yves LE TRAON (Supervisor / Scientific Advisor) • Stefanie OESTLUND (Project Manager)
Areas:	• Computer science and informatics • Information Science and Engineering (ENG)
Partners:	• TALLINNA TEHNIKAÜLIKOOL • Université Libre de Bruxelles • Université de Bretagne-Sud

Description

The CYBERUS EMJM in Cybersecurity jointly submitted by Université Bretagne Sud (UBS, coordinator), France, Université du Luxembourg (UL), Luxembourg and Université Libre de Bruxelles (ULB), Belgium, intends to take up 5 key challenges: Increasing digital threats, Cybersecurity skills shortages, EU cohesion, Digital sovereignty and Gender imbalance.

This highly integrated programme builds on the 3 Partners' proven cybersecurity expertise and a network of 47 international associated partners, many of whom key actors in cybersecurity. It plans to recruit 128 students with a balance between EU and non EU countries. CYBERUS has a strong focus on cybersecurity (105 ECTS out of 120) while offering a broad base of cybersecurity skills at UBS and two specialisation tracks: IoT Cybersecurity (with mobility to ULB) and Software Cybersecurity (with mobility to UL). Students will also conduct a 5-month internship at an approved institution anywhere in the world. CYBERUS will prepare students for top jobs through a combination of technological and social cybersecurity skills along with transversal skills. The teaching approach aims at excellence and rests on 8 pillars: a) subject depth and breadth, b) best practices; c) awareness of the green transition; d) skills continuum; e) commonness and specialisation; f) development of individual learning and professional pathways through differentiation; g) teaching and training and research; h) (vertical) technological skills and soft skills.

It is a win-win programme for all: students who will benefit from tight links between academia and the economic sector to improve their skills and find job opportunities, researchers who will regularly benchmark their knowledge and their skills to remain on the cutting edge, HEIs which will increase capacity to cooperate at EU/international level and better align educational practice with employer needs and industry which will find its much-needed talents among graduates and improve its workforce.

B.3   EC - EIC Pathfinder Projects

Context-aware adaptive visualizations for critical decision making

Acronym:	SYMBIOTIK
PI:	Luis A. LEIVA
Funding:	European Commission - European Innovation Council Pathfinder
Budget:	4.000.000,00 €
Duration:	1 Apr 2022 – 31 Mar 2025
Members:	• Luis A. LEIVA (Principal Investigator) • Saravanakumar DURAISAMY (Post-Doc)
Area:	Computer Science & ICT Security
Partners:	• AEGIS IT • Telefonica • Université Catholique de Louvain (UCL-PEDI)

Description

The latest neuroscience evidence suggests that emotions are essential not only to dealing effectively with social-emotional interactions, but they also perform important regulatory and helpful biasing functions within the body and the brain, aiding in rational decision-making and perception. However, developing empathic machines, equipped with emotion sensing and expressing capabilities has been an out-of-reach vision only realized in science fiction novels and movies alike. The project SYMBIOSIS will achieve the real breakthroughs needed to bring emotional intelligence for critical decision-making tasks in information visualization. We will quantify accurate information from user's behavioral signals and use those to reason and detect the affective tone of the user's context. Equipped with this information, we will bring context sensing capabilities to information visualization, which will allow users to react to critical inputs and will factor in affective reasoning and decision-making processes. The project will cover to practical use cases: (1) supporting the so- called Novice-to-Expert transition and (2) enabling human-centric perception analysis for situation- and time-sensitive tasks. Regarding (1), we will develop develop a neuro-physiological feedback loop to determine how different types of users interact with dashboard controls and how changes in visual design can affect performance and decision making in the above-mentioned situation- and time-sensitive contexts. The psychological understanding of this transition will inform the design of interventions that aid users in becoming experts faster, e.g., by understanding a large number of important visual primitives including graphical layouts and visual features. Regarding (2), we will place Human Information Processing under extensive scrutiny, using experimental psychology and cognitive neuroscience as the main framework for measuring aspects like attention (e.g., reaction times, eye tracking) and reasoning (e.g., neurophysiological changes in users). This will allow machines to determine the specific use conditions that allow for enhanced performance, smarter decisions, and quicker emergency response times around critical situations in information visualization.

B.4   EC - ERC - Stg Projects

naTurAl Program rEpair

Acronym:	TAPE
PI:	Tegawendé François d Assise BISSYANDE
Funding:	European Commission - European Research Council - Starting grant
Budget:	1.493.613,00 €
Duration:	1 May 2020 – 30 Apr 2025
Member:	Tegawendé François d Assise BISSYANDE (Principal Investigator)
Area:	Computer Science & ICT Security

Description

Error-free software is a myth. Therefore, automatically generating patches for identified program defects is a research endeavor that holds great promise. TAPE explores an ambitious research agenda on automating the repair of semantic bugs, under natural practitioner constraints: (1) buggy code should be fixed right after the developer writes it, (2) with no assumption on complete test suites to expose bugs, and (3) at best, by supposing that the bug is identified and reported by a user in natural language.

Indeed, ten years ago, the seminal works on test-based program repair claimed that test suites represented an affordable approximation to program specifications. Since then, this direction in the literature has expanded rapidly. Unfortunately, (1) the assumption that tests cases are readily available still does not hold in practice, leading to research that is misaligned with industry settings. Similarly, (2) although test-based repair bots may be helpful for continuous integration cycles, the reality is that bug reports written in natural language remain the concerns to address on a daily basis. Finally, (3) an ultimate goal in software development is to limit the number of bugs that are left over in releases. Thus, it is essential to develop approaches for repairing programs just-in-time while they are being created in the development environment.

TAPE ambitiously proposes to develop Information retrieval, code search and patch generation techniques for "Natural Program Repair". • First, the repair is natural in the sense that its workflow is designed and implemented in line with the natural process of software development; today, literature processes remain artificial in various ways. • Second, the repair is natural in that it leverages natural artefacts (e.g., bug reports) produced during software development. • Third, the repair is natural as it is embedded in the development cycle where it naturally suggests patches just-in-time.

B.5 EC - H2020 Projects

5G for cooperative & connected automated MOBIility on X-border corridors

 ⧉ https://www.5g-mobix.com/

Acronym:	5G-MOBIX
Reference:	R-AGR-3457-10
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	21.410.205,15 €
Duration:	1 Nov 2018 – 31 Jul 2022
Members:	• Thomas ENGEL (Principal Investigator) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Latif LADID (Program Coordinator) • Alessio BUSCEMI (Post-Doc) • Ridha SOUA (Post-Doc)
Area:	Communicative Systems
Partners:	• AEVAC - Asociación Española del Vehículo Autónomo Conectado • AKKA Informatique et Systemes • ASELSAN Elektronik Sanayi ve Ticaret A.S. • Aalto Korkeakoulusaatio S.R. • Alsa Grupo, S.L.U. • Associação CCG/ZGDV – Centro de Computação Gráfica • Auto-Estradas Norte Litoral • Ayuntamiento de Vigo • Brisa Inovacao e Tecnologia, S.A. • COSMOTE KINITES TILEPIKOINONIES A.E. • CTAG - Centro Tecnológico de Automoción de Galicia • DAIMLER AG • DEKRA Testing and Certification, S.A.U. • Dalian Roiland Technology Co.,Ltd • Dalian University of Technology • Datang Telecom Technology • ERTICO - ITS • Eindhoven University of Technology • Electronics and Telecommunications Research Institute (ETRI) • Ericsson Arastirma Gelistirme ve Bilisim Hizmetleri A.S. • Ericsson Hellas • FONDATION PARTENARIAL MOV'EOTEC (VeDecoM)

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

Description

5G-MOBIX aims at executing CCAM trials along x-border and urban corridors using 5G core technological innovations to qualify the 5G infrastructure and evaluate its benefits in the CCAM context as well as defining deployment scenarios and identifying and responding to standardisation and spectrum gaps. 5G-MOBIX will first define the critical scenarios needing advanced connectivity provided by 5G, and the required features to enable those advanced CCAM use cases. The matching between the advanced CCAM use cases and the expected benefit of 5G will be tested during trials on 5G corridors in different EU countries as well as China and Korea. Those trials will allow running evaluation and impact assessments and defining also business impacts and cost/benefit analysis. As a result of these evaluations and also internation consultations with the public and industry stakeholders,

5GMOBIX will propose views for new business opportunity for the 5G enabled CCAM and recommendations and options for the deployment. Also the 5G-MOBIX finding in term of technical requirements and operational conditions will allow to actively contribute to the standardisation and spectrum allocation activities. 5G-MOBIX will evaluate several CCAM use cases, advanced thanks to 5G next generation of Mobile Networks. Among the possible scenarios to be evaluated with the 5G technologies, 5G-MOBIX has raised the potential benefit of 5G with low reliable latency communication, enhanced mobile broadband, massive machine type communication and network slicing. Several automated mobility use cases are potential candidates to benefit and even more be enabled by the advanced features and performance of the 5G technologies, as for instance, but limited to: cooperative overtake, highway lane merging, truck platooning, valet parking, urban environment driving, road user detection, vehicle remote control, see through, HD map update, media & entertainment.

Results

We completed the main task, deliverable D7.6 - Report on the international cooperation and results -, and we presented it in front of the EU officers during the project's final event in the Hague (5th – 6th December).

ChronoPilot

Acronym:	ChronoPilot
PI:	Jean BOTEV
Funding:	European Commission - Horizon 2020
Budget:	3.000.000,00 €
Duration:	21 Sep 2021 – 20 Sep 2025
Members:	• Jean BOTEV (Principal Investigator) • Sahar NIKNAM (Doctoral Candidate) • Stéven PICARD (Doctoral Candidate)
Area:	Computer Science & ICT Security
Partners:	• Ghent University • Justus-Liebig-University Giessen • Panteion University of Social and Political Sciences • University of Lübeck

Description

The ChronoPilot project aims to investigate time perception in individuals and groups of humans, as well as in hybrid systems consisting of humans and machines, such as software agents and robots. ChronoPilot will explore the different dimensions of time perception, and develop a time modulation toolkit capable of improving both the quality and the process of decision-making. By exploring novel methods in the field of cognitive science, and applying mediated-reality technologies such as virtual/augmented reality (VR/AR) and body

sensors to different human sensory channels, ChronoPilot's team will develop innovative approaches to control the plasticity of time perception. We aim at a comprehensive understanding, through modeling of key variables and the interplay of different senses in subjective human time perception. On the basis of fundamental knowledge from psychology, we will develop ChronoPilot—a prototype technology for time modulation—and will be able to extend/compress human subjective time adaptively, whenever required.

INformation in the EU's DIgitalised Gouvernance

 ⧉ https://www.norface.net/project/indigo/

Acronym:	INDIGO
Funding:	European Commission - Horizon 2020
Duration:	1 Nov 2020 – 21 Oct 2023
Members:	• Davide LIGA (Researcher)
	• Réka MARKOVICH (Scientific Advisor)
	• Leon VAN DER TORRE (Scientific Advisor)

Description

INDIGO is a project on pressing issues affecting the future of democratic governance in Europe and the relation between the individual and the public sphere. INDIGO undertakes a structured analysis and develops an innovative approach to analysing and addressing the impact of digitalisation of the multijurisdictional implementation of policies in Europe through joint information systems and the use of advanced machine learning systems based on algorithms on possibilities of steering of decision-making by democratic legislation, individual participation, the protection of fundamental rights and the enforcement of the rule of law through independent judicial review. The objectives and outcome are, first, to map the profoundly transformative impact of innovative information technologies on rule-making and decision-making procedures and their impact on constitutional values enshrined in EU public law. Second, to develop future-proof regulatory approaches to realising these values in an age of technological innovation. INDIGO will thereby develop pathways to ensure that the use of information technology will both enhance the rule of law, democracy, transparency and the protection of fundamental individual rights as well as efficiency in problem solving and provision of public goods.

Results

Davide Liga was hired as a postdoctoral researcher for WP7 of INDIGO on the technological aspect and challenges. He has been working on an overview of the different technologies used in the automated decision-making practices in public administration law.

B.6   EC - H2020 and MECO Projects

National Competence Centres in the framework of EuroHPC

 ⧉ https://www.eurocc-access.eu/

Acronym:	EUROCC1
Reference:	R-AGR-3839
PI:	Pascal BOUVRY
Funding:	European Commission - Horizon 2020, MECO
Budget:	56.329.833,85 €
Duration:	1 Sep 2020 – 31 Dec 2022
Members:	• Pascal BOUVRY (Principal Investigator) • Johnatan Eliabeth PECERO SANCHEZ (Researcher) • Eleni LIAKIDOU (Project Coordinator)
Area:	Computer Science & ICT Security
Partners:	• AARHUS UNIVERSITET • Bayerische Akademie der Wissenschaften • DANMARKS TEKNISKE UNIVERSITET • FORSCHUNGSZENTRUM JULICH GMBH • Gauss Centre for Supercomputing (GCS) e.V. • INITS UNIVERSITÄRERS GRÜNDERSERVICE WIEN GMBH • INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLO-GIES • IT-UNIVERSITETET I KOBENHAVN • KEEMILISE JA BIOLOOGILISE FUUSIKA INSTITUUT • KOBENHAVNS UNIVERSITET • LUXINNOVATION • Luxprovide • NATIONAL INFRASTRUCTURES FOR RESEARCH AND TECHNOLOGY • OPENHAGEN BUSINESS SCHOOL • ROSKILDE UNIVERSITET • RUDER BOSKOVIC INSTITUTE • SICOS BW GMBH • SVEUCILISTE JOSIPA JURJA STROSSMAYERA U OSIJEKU FAKUL-TET ELEKTROTEHNIKE, RACUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK • SVEUCILISTE U RIJECI-TEHNICKI FAKULTET • SVEUCILISTE U ZAGREBU FAKULTET ELEKTROTEHNIKE I RACU-NARSTVA • SVEUCILISTE U ZAGREBU SVEUCILISNI RACUNSKI CENTAR • SYDDANSK UNIVERSITET • Sofia University "St. Kliment Ohridski"

- TALLINNA TEHNIKAÜLIKOOL
- TARTU ULIKOOL
- Technical University of Ostrava
- Technische Universitaet Wien
- Technische Universität Graz
- The Cyprus Institute
- UNIVERSITY OF NATIONAL AND WORLD ECONOMY
- UNIVERSITÄT FÜR BODENKULTUR WIEN
- UNIVERSITÄT INNSBRUCK
- University of Stuttgart
- Universität Wien

Description

The EuroCC activity will bring together the necessary expertise to set up a network of National Competence Centres in HPC across Europe in 31 participating, member and associated states, to provide a broad service portfolio tailored to the respective national needs of industry, academia and public administrations. All of this to support and increase strongly the national strengths of High Performance Computing (HPC) competences as well as High Performance Data Analytics (HPDA) and Artificial Intelligence (AI) capabilities and to close existing gaps to increase usability of these technologies in the different states and thus provide a European excellence baseline.

B.7   EC - H2020 - FET Open Projects

ChronoPilot

Acronym:	ChronoPilot
PI:	Jean BOTEV
Funding:	European Commission - Horizon 2020 - Future and Emerging Technologies
Budget:	3.000.000,00 €
Duration:	1 Sep 2021 – 31 Aug 2025
Member:	Jean BOTEV (Principal Investigator)
Area:	Computer Science & ICT Security

Description

The ChronoPilot project aims to investigate time perception in individuals and groups of humans, as well as in hybrid systems consisting of humans and machines, such as software agents and robots. ChronoPilot will explore the different dimensions of time perception, and develop a time modulation toolkit capable of improving both the quality and the process of decision-making. By exploring novel methods in the field of cognitive science, and applying mediated-reality technologies such as virtual/augmented reality (VR/AR) and body

sensors to different human sensory channels, ChronoPilot's team will develop innovative approaches to control the plasticity of time perception. We aim at a comprehensive understanding, through modeling of key variables and the interplay of different senses in subjective human time perception. On the basis of fundamental knowledge from psychology, we will develop ChronoPilot—a prototype technology for time modulation—and will be able to extend/compress human subjective time adaptively, whenever required.

B.8   EC - H2020 - Marie Curie Projects

LAST-JD: Rights of Internet of Everything

⤤ https://www.last-jd-rioe.eu/

Acronym:	LAST-JD RoIE
Funding:	European Commission - Horizon 2020 - Marie Curie
Budget:	3.834.322,00 €
Duration:	1 Nov 2019 – 31 Oct 2023
Members:	• Réka MARKOVICH (Researcher) • Leon VAN DER TORRE (Supervisor / Scientific Advisor) • Liuwen YU (PhD student)
Partners:	• APIS EUROPE • CARETEK SRL • CONSOFT SISTEMI SPA • Consiglio Nazionale delle Ricerche • KU Leuven • LUH - GOTTFRIED WILHELM LEIBNIZ UNIVERSITAET HANNOVER • MYKOLAROMERIS UNIVERSITY • Tuotempo SRL • UNIVERSITA DEGLI STUDI DEL PIEMONTE ORIENTALE AMEDEO AVOGADRO • UNIVERSITY OF PITTSBURGH • Universidad Politecnica de Madrid • University of Barcelona • University of Bologna • University of Turin • Wien University

Description

Internet of Everything (IoE) extends the concept of Internet of Things (IoT) to encompass not only devices but also individuals and data.

Proper study of IoE cannot be limited to engineering and computer science. It is a topic

that should be investigated using a variety of different scientific and interdisciplinary approaches as well as technical, legal, economic, ethical, and philosophical points of view.

How shall the algorithms which are at the core of IoE be governed? And what about privacy, intellectual property, data ownership, behavioral control, fundamental rights, and ethical principles? These are all critical issues that need to be examined to ensure that the IoE marketplace produces a sustainable technological environment in which we all will live.

Study will be conducted at a number of research institutes and will include working with industrial partner organizations.

Results

Liuwen Yu has completed her 3rd year and has started the 4th one exhibiting great progress.

B.9   EC - H2020 FET - ERA-NET Cofund Projects

Brainsourcing for Affective Attention Estimation

Acronym:	BANANA
PI:	Luis A. LEIVA
Funding:	European Commission - Horizon 2020 FET - ERA-NET Cofund
Budget:	1.795.107,37 €
Duration:	1 Feb 2022 – 31 Jan 2025
Members:	• Luis A. LEIVA (Principal Investigator) • Kayhan LATIFZADEH (Doctoral Candidate) • Bereket Abera YILMA (Post-Doc)
Area:	Brain-Computer Interfaces
Partners:	• Jaume I University • Opole University of Technology • University of Helsinki

Description

Attention estimation and annotation are tasks aimed at revealing which parts of some content are likely to draw the users' interest. Previous approaches have tackled these incredibly challenging tasks using a variety of behavioral signals, from dwell-time to clickthrough data, and computational models of visual correspondence to these behavioral signals. However, the signals are rough estimations of the real underlying attention and affective preferences of the users. Indeed, users may attend to some content simply because it is salient, but not because it is really interesting, or simply because it is outrageous. Project BANANA will use brain-computer interfaces (BCIs) to infer users' preferences and their attentional correlates towards visual content, as measured directly from the human brain.

We aim for a scientific breakthrough by proposing the first-of-its-kind affective visual atten-

tion annotation via brainsourcing, i.e. crowdsourced BCI signal acquisition. First, our approach will allow accurate estimation of user preferences, attention allocation, and –critically– the affective component of attention, directly measured from the natural and implicit brain potentials evoked in response to users experiencing digital contents. Then, we will utilize the resulting data in a crowdsourcing setting to reveal how multiple users react to different stimuli and how their attention and affective responses are distributed. These collective responses will produce unified, consistent measures as a result. Our technology will be used in several downstream tasks such as segmentation of users' attention while looking at images, identification of key events, and video summarisation. We will pilot BANANA with different user groups to test and prove its effectiveness, using objective benchmarks and evaluation strategies.

B.10   EC - HEU Projects

SLICES Preparatory Phase

Acronym:	SLICES-PP
PI:	Pascal BOUVRY
Funding:	European Commission - Horizon Europe
Budget:	3.000.000,00 €
Duration:	1 Sep 2022 – 31 Dec 2025
Member:	Pascal BOUVRY (Principal Investigator)
Area:	Computer Science & ICT Security

B.11   EC - JUST Projects

Analytics for Decisions of Legal Cases

 https://site.unibo.it/adele/en

Acronym:	ADELE
Funding:	European Commission
Duration:	1 Feb 2021 – 31 Jul 2023
Members:	• Réka MARKOVICH (Researcher) • Leon VAN DER TORRE (Researcher)
Partners:	• APIS JSC Europe • European University Institute • LIBRe Foundation

- Union of Bulgarian Jurists
- University of Bologna
- University of Turin

Description

Project ADELE is premised on the ongoing paradigm shift towards cognitive computing and human-centered AI which is transforming many socio-economic activities, including justice. The project applies legal analytics (LA) – a blend of datascience, machine learning and natural language processing techniques – to judicial decisions: it aims to(1) develop methods to extract knowledge and engage in outcome predictions, and there from (2) build a pilot tool to support legal research and decision-making processes in the judiciary. (PI: Giovanni Sartor, University of Bologna. UL is the WP leader of the Legal Analysis.)

Results

UL is leading the WP responsible for ontology development. In 2022, we developed the ontologies on VAT, the final version of which will be delivered together with the ontologies of patent and trademark in 2023.

B.12   ESA Projects

Autonomous trustworthy monitoring and diagnosis of CubeSat health

Acronym:	ATMonSAT
PI:	Andrzej MIZERA
Funding:	European Space Agency
Duration:	1 May 2021 – 31 Oct 2022
Member:	Andrzej MIZERA (Principal Investigator)
Area:	Information Security

Description

The objective is to harness state-of-the-art explainable AI and operating system technology to build in an additional layer of dependability, accountability and intelligence between the critical core of a CubeSat and the environment it controls. Our initial evaluation found current operating systems deployed on CubeSats, e.g., FreeRTOS, are not fit for a future in which Launching States increasingly transfer liability for collisions resulting from failures or even cyber attacks to CubeSat Operators. We propose a novel solution that is verified,

hence dependable, and which builds auditable real-time anomaly detection and overall health monitoring into the critical core of a CubeSat.

More precisely, this project will result in a framework with the following contributions, which required us to balance the key requirements of verifiability and adaptability:

(A) Trustworthy auditing of system health for post-disaster diagnostics. We will develop a method for automated root-cause analysis for disasters (e.g., tumbling and collisions), leveraging the diverse I/O used to maintain a Cubesat. We anticipate insurers will re- quire such an analysis to resolve liability disputes, e.g., to prove that a fault is not due to negligence during CubeSat development and operations.

(B) A hardware-isolated, dependable layer for autonomous disaster recovery. Instead of a set of hard-coded rules for disaster recovery, we will develop suitable AI mechanisms for onboard data analysis that take all I/O into account (not only telemetry). The framework must also adapt to unforeseen scenarios based on new data. Such a mechanism can make swift decisions in response to unexpected failures and perceived risks. Hardware-isolation ensures that monitors cannot be tampered with even when control software is compromised.

Autonomous trustworthy monitoring and diagnosis of CubeSat health

Acronym:	ESA Open Discovery Ideas
PI:	Andrzej MIZERA
Funding:	European Space Agency
Duration:	1 May 2021 – 31 Oct 2022
Member:	Andrzej MIZERA (Principal Investigator)

Description

The objective of this project is to harness state-of-the-art explainable AI and operating system technology to build in an additional layer of dependability, accountability and intelligence between the critical core of a CubeSat and the environment it controls. The initial evaluation found current operating systems deployed on CubeSats, e.g., FreeRTOS, are not fit for a future in which Launching States increasingly transfer liability for collisions resulting from failures or even cyber-attacks to CubeSat Operators. In this project, we propose a novel solution that is verified, hence dependable, and which builds auditable real-time anomaly detection and overall health monitoring into the critical core of a CubeSat.

Autonomous trustworthy monitoring and diagnosis of CubeSat health

Acronym:	NN
PI:	Sjouke MAUW

Funding:	European Space Agency
Budget:	182.900,00 €
Duration:	1 May 2021 – 31 Oct 2022
Member:	Sjouke MAUW (Principal Investigator)
Area:	Computer Science & ICT Security

Description

The objective is to harness state-of-the-art explainable AI and operating system technology to build in an additional layer of dependability, accountability and intelligence between the critical core of a CubeSat and the environment it controls. Our initial evaluation found current operating systems deployed on CubeSats, e.g., FreeRTOS, are not fit for a future in which Launching States increasingly transfer liability for collisions resulting from failures or even cyber attacks to CubeSat Operators. We propose a novel solution that is verified, hence dependable, and which builds auditable real-time anomaly detection and overall health monitoring into the critical core of a CubeSat. More precisely, this project will result in a framework with the following contributions, which required us to balance the key requirements of verifiability and adaptability: (A) Trustworthy auditing of system health for post-disaster diagnostics. We will develop a method for automated root-cause analysis for disasters (e.g., tumbling and collisions), leveraging the diverse I/O used to maintain a Cubesat. We anticipate insurers will require such an analysis to resolve liability disputes, e.g., to prove that a fault is not due to negligence during CubeSat development and operations. (B) A hardware-isolated, dependable layer for autonomous disaster recovery. Instead of a set of hard-coded rules for disaster recovery, we will develop suitable AI mechanisms for onboard data analysis that take all I/O into account (not only telemetry). The framework must also adapt to unforeseen scenarios based on new data. Such a mechanism can make swift decisions in response to unexpected failures and perceived risks. Hardwareisolation ensures that monitors cannot be tampered with even when control software is compromised.

B.13   EU - COST Action Projects

Distributed Knowledge Graphs

Acronym:	DKG
PI:	Ross James HORNE
Funding:	European Union - European Cooperation in Science & Technology Action
Duration:	23 Sep 2020 – 22 Sep 2024
Member:	Ross James HORNE (Principal Investigator)

Description

Knowledge Graphs are a flexible way to represent interlinked information about virtually anything. People from a variety of application domains including biomedical research, public and open data, linguistics, journalism, and manufacturing publish, use, and investigate knowledge graphs. As the publication is done in a decentralised fashion across the web, the knowledge graphs form a distributed system.

Due to the ever-increasing uptake of Knowledge Graph technologies in recent years, there are new challenges for research and development including dealing with the scale and the de- gree of distribution of knowledge graphs, while monitoring and maintaining data quality and privacy. Tackling these research challenges will need a stronger collaboration within the research community, and a joint effort to establish a more functional, decentralized Web of Data.

The main aim of the Action is therefore to create a research community for deployable Distributed Knowledge Graph technologies that are standards-based, and open, embrace the FAIR principles, allow for access control and privacy protection, and enable the decentralised publishing of high-quality data. To this end, the Action connects European researchers and practitioners from (1) diverse application domains and (2) the whole life cycle of Distributed Knowledge Graphs, from provisioning to finding, accessing, integrating, programming, deploying, enriching, and analytics. The Action will develop practices for scalable, privacy-respecting, high quality and decentralised Knowledge Graph publication and consumption, reach out to the European industry, and formulate a research agenda.

Results

In 2022, Dr. Ross James Horne, as the local organiser, successfully organised Workshops on Privacy Issues in Distributed Social Knowledge Graphs, 13-15 June 2022, at the University of Luxembourg.

European Network on Future Generation Optical Wireless Communication Technologies

Acronym:	NEWFOCUS
PI:	Thomas ENGEL
Funding:	European Union - European Cooperation in Science & Technology Action
Budget:	4.000.000,00 €
Duration:	1 May 2020 – 30 Apr 2024
Member:	Thomas ENGEL (Principal Investigator)
Area:	Computer Science & ICT Security

Description

The design of future wireless communication networks that cope with the ever-growing mobile data traffic as well as support varied and sophisticated services and applications in vertical sectors with a low environmental impact is recognized as a major technical challenge that European engineers face today. The COST Action NEWFOCUS will propose truly radical solutions with the potential to impact the design of future wireless networks. Particularly, NEWFOCUS aims to establish optical wireless communications (OWC) as an efficient technology that can satisfy the demanding requirements of backhaul and access network levels in beyond 5G networks. This also includes the use of hybrid links that associate OWC with radiofrequency or wired/fiber-based technologies. Towards this vision, NEW-FOCUS will carry out a comprehensive research programme under two major pillars. The first pillar is on the development of OWC-based solutions capable of delivering ubiquitous, ultra-high-speed, low-power consumption, highly secure, and low-cost wireless access in diverse application scenarios. The developed solutions will in particular support Internet-of-Things (IoT) for smart environments with applications in vertical sectors. The second pillar concerns the development of flexible and efficient backhaul/fronthaul OWC links with low latency and compatible with access traffic growth. In addition to scientific and technological advances, NEWFOCUS will serve as a global networking platform through capacity building of all relevant stakeholders including universities, research institutions, major industry players, small medium enterprises, governmental bodies and non-governmental organisations. Within this rich consortium, NEWFOCUS will train experts to accompany related European industries for the standardisation and commercialization of the OWC technology.

European Research Network on Formal Proofs

Acronym:	EuroProofNet
PI:	Matteo ACCLAVIO
Funding:	European Union - European Cooperation in Science & Technology Action
Duration:	11 Oct 2021 – 10 Oct 2025
Member:	Matteo ACCLAVIO (Principal Investigator)

Description

If testing can reveal errors in computer programs, only formal verification can guarantee their absence. The highest Evaluation Assurance Levels of the Common Criteria for Information Technology Security Evaluation require automatically checked mathematical proofs of correct- ness. Proofs are also the basis of mathematics and many sciences, and thus are very important in education and research.

In many computer technologies, developers and users rely on standard languages and protocols for exchanging data and enabling tool interoperability: TCP/IP for network communication, HTML for web pages, etc. This is however not the case for formal proofs, which is a major bot- tleneck for their adoption by the industry. The main reason is that, currently, proof systems use

14mutually incompatible logical foundations. Fortunately, only small parts of the proofs developed in a system use features that are incompatible with other systems.

Europe is a leading actor in the area of formal proofs: about 65% of the proof systems of the world are developed in Europe, including the two most used proof assistants, Coq and Isabelle. This Action aims at boosting the interoperability and usability of proof systems and making

formal proofs enter a new era. For the first time, it gathers all the developers and users of proof systems in Europe. To make the proofs exchangeable, they will express, in a common logical framework, the logical foundations of their systems and develop tools for inter-translation of the proofs developed in individual systems to and from this common logical framework.

B.14   FNR Projects

Securing Time Critical Traffic in (next gen) Automotive Networks

⎘ https://vehicularlab.uni.lu/project/setica/

Acronym:	SETICA
Reference:	R-AGR-3969-10+20
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche
Budget:	567.481,00 €
Duration:	1 Jun 2021 – 31 May 2024
Members:	• Thomas ENGEL (Principal Investigator)
	• Stefanie OESTLUND (Project Coordinator)
	• Alessio BUSCEMI (Post-Doc)
	• Mahdi FOTOUHI (PhD student)
Area:	Communicative Systems
Partner:	Honda r&d Europe GmbH

Description

Today's vehicles incorporate more and more enhanced services such as ADAS systems, smartphone integration, autonomous driving, connectivity, and entertainment for passengers. Efficient communication is the key to facilitate all these services. So far, in-vehicle communication systems have been designed to allow for very stringent end-to-end delays and deterministic communication requirements. However, they are inflexible, will hardly able to provide the bandwidth needs of future cars, and offer little security.

Contrary to conventional in-vehicle communication systems, Ethernet is flexible and offers high bandwidth. While Time Sensitive Networking (TSN) can guarantee tight end-to-end delays, and MACsec can provide security, there is no profile that consolidates these properties. Developing such an automotive TSN profile, which includes answering challenging research questions and thorough evaluation, is of the essence for future cars in terms of safety and security as well as comfort. The importance of this has been acknowledged by the IEEE which started working on such a profile (802.1DG).

The goal of SETICA is solving the research part of this endeavour as well as developing a realistic security-enabled TSN testbed, which, in turn, will allow thorough realistic evaluation. We plan to especially focus on gPTP, the timing protocol of TSN. The impact of successful attacks against gPTP is severe because many safety-critical applications depend on timing guarantees. We will also research novel approaches that go beyond 802.1DG, among them leveraging SDN for gaining even more flexibility and security.

SETICA will generate significant value, researching and developing important future technology to be used as key communication technology in vehicles to facilitate future functionalities and services, such as autonomous driving, connected cars, and ADAS functions, which will require all of high bandwidth, precise timing, and security.

Results

We built a gPTP-based physical testbed, which allowed us to complete i) Task T2.2 related to the evaluation of high-risk attacks, ii) Task T2.3 related to the evaluation of gPTP-compliant security controls, iii) Task T2.4 related to the evaluation of an intrusion detection system for gPTP. Furthermore, we initialized T3.1, related to the creation of a risk matrix for automotive TSN.

Three papers were written based on this work, i) "Assessing the Impact of Attacks on an Automotive Ethernet Synchronization Testbed", submitted to VNC 2023, ii) "An Intrusion Detection System Against Rogue Master Attacks on gPTP", submitted to VTC 2023, and iii) "Evaluation of PTP Security Controls on gPTP".

B.15   FNR - AFR Projects

Remote memory attestation and erasure through formal verification

Acronym:	ATTEST
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche
Duration:	1 Mar 2020 – 31 Jan 2024
Members:	• Sjouke MAUW (Principal Investigator) • Reynaldo GIL PONS (AFR PhD Applicant)

Description

Resource-constrained computational devices with Internet connectivity are collectively termed Internet of Things (IoT) devices, and are particularly vulnerable to attacks, as they cannot afford the implementation of proactive defences against malicious code. IoT devices not only become easy targets for hackers but also a useful weapon to launch further attacks on major services. Verifying the integrity of a remote device is essential to maintaining a secure computer network, as malicious or erroneous code could be used, for example, to compromise secrets and escalate privileges remotely. The current practice is to rely on forensic techniques such as memory attestation and erasure protocols. The former verifies the integrity of a device's memory and the latter certifies memory has been erased. Both result in devices without unexpected contents in memory. Current attestation and erasure protocols are restricted to highly controlled environments. Either the protocol needs direct access to the device's hardware, or it requires the device to be isolated from the network. Both restrictions are hard to meet in large-scale networks that exhibit a high level of heterogeneity, such as IoT networks. On the one hand, the area of Security Protocol Analysis produces protocols that resist attackers with full control over the network. On the other hand, memory erasure and attestation protocols are limited in terms of their ability to cope with network attackers, i.e. attackers able to intercept and manipulate network messages. This project will use current experience in developing security protocols and adversary models to make novel memory attestation and erasure protocols resilient against network attackers. To this end, we will identify the limits of memory erasure/attestation protocols in terms of the attacker model and security properties they can cope with, and put forward more robust, efficient and versatile protocols.

Results

In 2022, we published the following paper:

- Reynaldo Gil-Pons, Ross Horne, Sjouke Mauw, Alwen Tiu, and Rolando Trujillo-Rasua. Is Eve nearby? Analysing protocols under the distant-attacker assumption. In Proc. 35th IEEE Computer Security Foundations Symposium (CSF'22), pages 17-32, Haifa, Israel, 2022. IEEE Computer Society.

B.16   FNR - AFR PhD Projects

Investigating Graph Neural Networks for Open-Domain Question Answering

Acronym:	GNN-QA
PI:	Martin THEOBALD
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD
Budget:	190.000,00 €
Duration:	1 May 2021 – 30 Apr 2025
Member:	Martin THEOBALD (Principal Investigator)

Area: Computer Science & ICT Security

Description

We intend to investigate a novel approach to knowledge-graph based question-answering by combining the previous approaches for QA into one coherent framework. Current QA systems are either based on (i) solving complex graph algorithms, based on spanning- and/or Steiner-tree problems, or on (ii) on deep-learning approaches, which however require hundreds of thousands of manually annotated question-answer pairs for training (see e.g. the Stanford Question Answering Dataset). Our goal therefore is to combine a huge knowledge graph, consisting of automatically extracted and decomposed natural-language clauses, to automatically learn more generic graph patterns, which can then be fed into the respective question-answering algorithms and thereby drastically reduce the manual training input that is currently still needed for open-domain QA systems.

Neural Vulnerable Program Repair

Acronym: NERVE

PI: Tegawendé François d Assise BISSYANDE

Funding: Fonds National de la Recherche - Aide à la Formation Recherche PhD

Budget: 168.510,00 €

Duration: 1 Sep 2020 – 31 Aug 2024

Member: Tegawendé François d Assise BISSYANDE (Principal Investigator)

Area: Computer Science & ICT Security

Description

The use of software is booming, making it the heart of the infrastructure that powers our society. However, any software will always face various problems, and exploiting software vulnerabilities for the wrong purpose is costing the global economy millions of Euros each year. In January 2020 alone, 1,660 vulnerabilities were published the Common Vulnerability Exposure (CVE) database. Even if there is research to deal with these vulnerabilities and with different objectives such as the detection, prevention or repair of software vulnerabilities, the results remain below expectations. This PhD proposal, NERVE for Neural Vulnerable Program Repair investigate the repair of software vulnerabilities using a deep learning approach, called, sequence-tosequence (Seq2Seq) learning. NERVE aims to build on the "naturalness of code" and the naming conventions and principles in source code" in order to apply to software code, sequence-to-sequence (Seq2Seq) learning which is a modern machine learning framework used in automated translation. It consists of an automatic translation based on an encoder-decoder which maps an input of sequence to an output of sequence with a tag and attention value. Like human language translation, NERVE "translate" identified vulnerable code into safe software code. NERVE presents a new approach to manage the unlimited possibilities of tokens in the source code. This novelty concerns the taking into account of software engineering's naming conventions and principles (eg. camelCase) in the representation and building of a vocabulary.

Privacy Attacks and Protection in Machine Learning as a Service

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

Description

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

Results

The PhD candidate Hailong Hu has worked on several research tasks, including membership inference on GANs and diffusion models, and ownership protection of GANs. He has three papers under submission.

Privacy Attacks and Protection in Machine Learning as a Service

Acronym:	PriML
PI:	Jun PANG
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD

Budget:	160.000,00 €
Duration:	1 Nov 2019 – 31 Oct 2023
Member:	Jun PANG (Principal Investigator)
Area:	Computer Science & ICT Security

Description

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

The logical content of secure properties of computer systems

Acronym:	LCSPCS
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD
Budget:	175.650,00 €
Duration:	1 Apr 2021 – 14 Nov 2024
Member:	Sjouke MAUW (Principal Investigator)
Area:	Computer Science & ICT Security

Description

In this thesis we aim at studying the intersection of two research field, proof theory and security and trust. The connection between the two is not an entire novelty, although it is

still a young research topic - unlike the connection between proof theory and functional programming which has been intensively explored, the connection of proof theory and concurrency has not yet been entirely satisfactory, a part of the reason why may be that most of what has been done so far tries to recreate what has been done with functional programming in the concurrency setting - this approach, so far, did not seem to bring the best results. We therefore seek to find new approaches, new frameworks to interpret logical content into the concurrency setting. One of the novelty is using a logical system that operates on graphs rather than on formula (AHS 2020), our intuition is that these graphs can represent conflict in concurrency; our first idea was to connect it to access control models and especially with the chinese wall, since all the rules of GS delete edges then it ensures that if a graph represented a secure state of the chinese wall then any derivable graphs would preserve that secure state. Another idea is linking this graphical logic with the notion of conflict in the concurrent execution of queries. It is know that transactions can be in conflict for example running two transactions that take an amount of money from a bank account concurrently ie. at the same time may lead to an inconsistent state ie. the bank account could go in the negative, although each transaction individually was consistent. Representing the transactions as nodes and the edges as conflicts or locks, we could aim at saying that the provable graphs corresponds to finite sets of transactions that can be safely executed. Logic operating with security as shown to be fruitful, which is why I believe it is a worth pursuing research, also because there is still a lot to be done to really understood what it means to be secure for a protocol (and there are many different definition and contexts). I also believe that there must be indeed a correspondence between security and trust and discrete mathematics (and specifically proof theory), and that the formalism of mathematics - that is currently lacking - will be needed to tackle some specific problems.

B.17   FNR - AFR PhD and ILNAS Projects

Technical Standardisation for Trustworthy ICT, Aerospace and Construction

 https://ilnas-snt.uni.lu

PI:	Pascal BOUVRY
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD, Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services
Budget:	1.792.254,00 €
Duration:	1 Jan 2021 – 31 Dec 2024
Members:	• Pascal BOUVRY (Principal Investigator) • Grégoire DANOY (Collaborator) • Manuel COMBARRO SIMON (PhD student) • Hedieh HADDAD (PhD student)

- Lena Maria HARTMANN (PhD student)
- Mohammed ALSWAITTI (Research Associate)

Area: Computer science and informatics

Partners:
- ILNAS
- Jean-Philippe Humbert

Description

The second ILNAS-SnT research programme 2021-2024 is consciously sector-oriented and targets three highly relevant growth sectors for Luxembourg's economy, in conformity with the national technical standardization strategy 2020-2030, that will deepen data and AI capabilities and enable a steady potential for innovation. The three sectors are a) ICT, b) Aerospace, and c) Construction. The economic power for these three domains is strongly determined by normative values notably related to trustworthiness, security, and privacy. Consequently, policies, regulations, and standards are required to be established to enhance trust in each particular domain-specific ecosystem.

In line with the new master in Technopreneurship, the ICT sector fosters ICT driven by trustworthy AI. The research part will provide tools, techniques, and algorithms to assess, analyse, and develop privacy, trust and security aspects of AI systems. In this frame, standardization efforts strengthen the research process and outcomes to direct developers and enterprises to valorise trustworthiness in emerging products and processes.

Results

Talks

- On 29.06.2022, Prof. Pascal Bouvry, Dr. Grégoire Danoy, Dr. Mohammed Alswaitti and Ms. Maria Hartmann delivered a talk at the Space and technical standardisation workshop (ILNAS/ University of Luxembourg).
- On 14.10.2021, Dr. Grégoire Danoy, Dr. Mohammed Alswaitti, Mr. Manuel Combarro Simón, Ms. Hedieh Haddad and Ms. Maria Hartmann delivered a talk at the World Standards Day 2022 event, describing the research topics of the project.

B.18   FNR - Bridges Projects

SEcuring TIme Critical traffic in (next gen) Automotive networks

Acronym: SETICA

PI: Thomas ENGEL

Funding: Fonds National de la Recherche - Bridges

Budget: 609.127,00 €

Duration: 1 Jun 2021 – 31 May 2024

Member: Thomas ENGEL (Principal Investigator)

Area: Computer Science & ICT Security

Description

In-vehicle communication systems have been designed to allow for very stringent end-to-end delays and deterministic communication requirements. However, they are inflexible, do not provide the bandwidth needs of future cars, and offer no security. Contrary to in-vehicle communication systems, Ethernet is flexible and offers high bandwidth. While Time Sensitive Ethernet (TSN) can guarantee tight end-to-end delays, and MACsec can provide security on the link layer, there is no profile that consolidates these properties. Developing such an automotive Ethernet profile, which includes answering challenging research questions and thorough evaluation, is of the essence for future cars in terms of safety and security as well as comfort. The importance of this has been acknowledged by the IEEE which started working on such a profile (802.1DG). The goal of SETICA is solving the research part of this endeavour as well as developing a realistic security-enabled TSN testbed, which, in turn, will allow thorough realistic evaluation. We plan to especially focus on gPTP, the timing protocol of TSN. Both attacking gPTP and researching counter measures are an integral part of SETICA. The impact of successful attacks against gPTP is severe because many safety-critical applications depend on timing guarantees. SETICA will also research novel approaches that go beyond 802.1DG, among them leveraging SDN for gaining even more flexibility and security.

B.19   FNR - CORE Projects

A Concurrent Model of Computation for Trustworthy GPU Programming

Acronym: COMOC

PI: Pascal BOUVRY

Funding: Fonds National de la Recherche - CORE

Budget: 856.986,00 €

Duration: 1 Jan 2021 – 31 Dec 2023

Member: Pascal BOUVRY (Principal Investigator)

Area: Computer Science & ICT Security

Description

Nowadays, the capabilities of graphics processing units (GPUs) go beyond the scope of image processing, and their efficiency potential enhances many general-purpose applications. However, it is very hard to program on GPUs because the classic sequential model of computation does not fit multi-cores architectures. We propose the design, implementation and evaluation of a new programming language, based on lattice theory and logic programming, to leverage GPUs to new artificial intelligence applications. We focus on constraint reason-

ing which is an important area of artificial intelligence to solve combinatorial problems, that has not yet benefited from the GPU revolution. We connect GPU programming and constraint reasoning via lattices, which are structures at the core of constraint reasoning with interesting mathematical properties for their executions on multi-cores architectures. Our overarching goal is to demonstrate that the power of GPU can be leveraged to various AI applications with the right model of computation.

Automating the Design of Autonomous Robot Swarms

Acronym:	ADARS
PI:	Grégoire DANOY
Funding:	Fonds National de la Recherche - CORE
Budget:	952.990,00 €
Duration:	1 Jan 2021 – 31 Dec 2023
Member:	Grégoire DANOY (Principal Investigator)
Area:	Computer Science & ICT Security

Description

Aerospace and space systems are both experiencing a recent and rapid shift towards distributed models where several autonomous aircrafts/spacecrafts jointly achieve a common goal. These systems bring multiple economic advantages that increase the value proposition over monolithic systems from the reduction of realisation time and operational and launch cost, increased mission success rate and resilience to the increased coverage capacity and possibility to embed different payloads. These Distributed Aerospace and Space Systems (DASS) open numerous new perspectives ranging from search and rescue missions with fleets of unmanned autonomous vehicles (UAV) to asteroid observation with a constellation of probes. In turn allowing to achieve new fundamental science goals that simply would have not been deemed feasible with monolithic systems. A promising way to manage these distributed systems is by utilising swarm intelligence. Swarming is an emergent collective intelligence behaviour, where simple entities self-organise based on local rules, to achieve a mutual objective. However designing fully distributed and autonomous systems remains a challenging open problem since the global systems' performance is hardly predictable based on individual behaviours, their mutual interactions and the interactions with the environment. The problem becomes even more challenging since it is multi-objective by nature, such as maximising the swarm coverage while minimising its energy consumption. The ADARS (Automating the Design of Autonomous Robot Swarms) project aims to propose a unique solution to this problem by addressing the following question: is it possible to automatically generate efficient and reusable behaviors for distributed aerospace and space systems (DASS)? To this end, ADARS will advance the state-of-the-art in the field of swarm robotics and automated algorithm design. A novel hyper-heuristics framework relying on multi-objective machine learning will be designed to automatically generate efficient swarming heuristics to tackle two challenging DASS problems: swarm formation for a counter UAV system and swarm formation of small satellites for asteroid observation. Experimental validation will not only be conducted using specifically developed simulators but also using real field tests with swarms of multi-rotor UAVs. The developed hyper-heuristic

framework and the DASS simulation platform will be made available to the community as software libraries / plug-ins. ADARS unique automated design approach will additionally generate novel IP creation, technology transfer and business opportunities in the aerospace and space sectors, with its counter unmanned aerial vehicle (UAV) and satellite swarming for asteroid observation solutions.

Automating the Design of Autonomous Robot Swarms

  [↗ https://adars.uni.lu](https://adars.uni.lu)

Acronym:	ADARS
PI:	Grégoire DANOY
Funding:	Fonds National de la Recherche - CORE
Budget:	953.000,00 €
Duration:	1 May 2021 – 30 Apr 2024
Members:	• Grégoire DANOY (Principal Investigator)
	• Florian FELTEN (PhD student)
	• Daniel STOLFI ROSSO (Research Associate)
	• Pascal BOUVRY (Scientific Advisor)
	• Pierre-Yves HOUITTE (Research and Development Specialist)
	• Sébastien VARRETTE (Senior Researcher)

Description

The ADARS (Automating the Design of Autonomous Robot Swarms) project aims to propose a unique approach to automatically generate behaviours for distributed aerospace and space systems (DASS) thanks to a cross-fertilisation between multi-objective optimisation and machine learning techniques. ADARS will demonstrate through specifically designed software simulations and real field tests with multi-rotor drones, that state-of-the-art results can be obtained on two challenging DASS applications: swarm formation for a counter UAV system and swarm formation of small satellites for asteroid observation.

EnCaViBS

  [↗ https://encavibs.uni.lu/](https://encavibs.uni.lu/)

Acronym:	EnCaViBS
PI:	Thomas ENGEL

Funding:	Fonds National de la Recherche - CORE
Budget:	969.000,00 €
Duration:	1 Sep 2019 – 31 Aug 2022
Members:	• Thomas ENGEL (Principal Investigator) • Sandra SCHMITZ-BERNDT (Post-Doc) • Aurel MACHALEK (Research and Development Specialist)
Area:	Communicative Systems
Partners:	• Mark Cole • University of Luxembourg, Faculty of Law, Economics and Finance

Description

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

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

For more info and current affairs of the project please visit https://encavibs.uni.lu

Give control back to users: personalised privacy-preserving data aggregation from heterogeneous social graphs - resubmission

Acronym:	HETERS
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - CORE
Budget:	700.621,00 €
Duration:	1 Mar 2021 – 31 Mar 2025
Member:	Sjouke MAUW (Principal Investigator)
Area:	Computer Science & ICT Security

Description

Heterogeneous social graphs (HSG) have been widely used to analyse social network data to support decision making. Compared to simple social graphs which only model the relations between users, HSGs capture the heterogeneity nature of social networks in terms of data subjects and relations between them. The richer information encoded in HSGs leads to overwhelming better results than those on simple social graphs. In the meantime, it also imposes more risk of a privacy breach. Due to the potential economic and reputation loss, social network operators only publish a limited amount of HSG data for researchers and third-party data analysts. In this project, we address an alternative decentralised solution for data analysts to collect data of HSGs directly from volunteers while guaranteeing volunteers' privacy. Specifically, users privately calculate and share data about their local views of HSGs. Data analysts aggregate these responses into the information of interest. To the best of our knowledge, no works in the literature exist to achieve this goal. Moreover, we will take into account the fact that in real-life scenarios, users may have different privacy requirements, e.g., due to various trust to data collectors. We design methods for users to perturb their local data according to their own personalised privacy requirements. In this manner, we manage to give control back to users over their data by determining the level of privacy protection. In addition to precise privacy preservation, our methods can also ensure better utility for the aggregated data when only a small number of users require high-level protection. To achieve our purpose, we will first extend the notion of local differential privacy to quantify users' personalised privacy requirements over different types of sensitive information, i.e., vertices and edges. Once the privacy properties have been defined, we will design corresponding privacy-preserving methods for two widely studied data aggregation tasks: query answering and graph synthesis. Query answering is used to aggregate statistics of some structural properties of HSGs while graph synthesis allows data analysts to conduct flexible analysis on synthetic HSGs with similar properties to the original graphs. Last but not least, we will develop a comprehensive evaluation framework to evaluate the effectiveness of our methods and define new measures to quantitatively assess the utility of the aggregated data.

Secure, Quantum-Safe, Practical Voting Technologies

Acronym:	EquiVox
PI:	Peter Y A RYAN
Funding:	Fonds National de la Recherche - CORE
Duration:	1 Apr 2020 – 31 Mar 2023
Members:	• Peter Y A RYAN (Principal Investigator)
	• Peter ROENNE (Researcher)
	• Georgios FOTIADIS (Research Associate)
	• Johannes MUELLER (Research Associate)

Description

Digital information and communication technologies, entrenched in the fabric of modern society, enrich and facilitate our lives. Used carefully, the very same tools can also serve to

enrich and protect core mechanisms, such as elections, that are fundamental to the functioning of democratic societies. In effect, elections form the foundations of democracy and as such, ensuring their security is of the utmost importance. One of the major security challenges that ought to be dealt with is the threat posed by the emergence of quantum computers. Despite a considerable number of well-designed secure electronic voting schemes proposed over the past few decades, almost all existing schemes depend on cryptography which will be broken by quantum algorithms. Therefore, the goal of this project is to develop and prototype practical e-voting schemes that are secure against attackers capable of performing arbitrary quantum computations.

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

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

Acronym:	FinCrypt
PI:	Alexei BIRYUKOV
Funding:	Fonds National de la Recherche - CORE
Duration:	1 Aug 2018 – 31 Jul 2022
Member:	Giuseppe VITTO (PhD student)
Area:	Security, Reliability and Trust in Information Technology

Description

Blockchain technology gathered momentum with the popularity of the Bitcoin cryptocurrency. Being an interesting practical proposal which gained a large community of followers in the last 4 years Bitcoin can be seen as a testbed for ideas in the FinTech area. By now it is clear what Bitcoin ideas can be generalized and are valuable but also what are the shortcomings of the concrete Bitcoin instantiation of a distributed ledger and cryptocurrency. For example, the scalability problem has become vital, as the transaction rate growth made the designers think to increase the block size, which in turn might lead to higher network latency and vulnerability to various network attacks. Also current proof-of-work based blockchains are very energy intensive. Active research is now happening around greener alternatives for consensus protocols, such as fault-tolerant Byzantine agreement or Proof of Stake which tolerate higher transaction rate and were tested on small networks. The security of blockchain applications with an accent on the data confidentiality is an unsolved problem. So far the blockchain ledger is implicitly public, but users demand more confidentiality for their data. On the other hand governments demand access to blockchain information for AML/KYC policies and taxation. The problem of storing and processing encrypted data on the blockchain as well as privacy vs governance tradeoff remain largely unexplored. One of the most interesting blockchain applications are smart contracts. Whereas the Bitcoin ledger consists of transactions only, a smart contract ledger contains programming code of almost arbitrary complexity, so that sophisticated financial instruments, legal contracts,

and reputation systems can be encoded and executed automatically. However, the private character of contracts poses a challenge of concealing the exact functionality while, at the same time, still keeping it verifiable to the other protocol participants. Our proposal is to investigate blockchain applications from both the scalability and confidentiality point of view and to suggest new solutions in this area (Work Package 1) as well as to study the privacy and security aspects of smart contracts and to propose new efficient methods to achieve user privacy and contract confidentiality (Work Package 2).

Note: The formal part of the project ended after three years (i.e., on 31st July 2021). The fourth year was used by the Ph.D. student involved in the project to finish and defend his thesis.

teSTing sELf-LeARning systems

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

Description

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

B.20   FNR - CORE - Core International Projects

ByzRT: Intrusion resilient real-time communication and computation in autonomous systems - RESUBMISSION

Acronym:	ByzRT - Resubmission
PI:	Paulo ESTEVES-VERISSIMO
Funding:	Fonds National de la Recherche - CORE - Core International
Budget:	1.599.598,00 €
Duration:	1 Jan 2020 – 31 Dec 2022
Member:	Paulo ESTEVES-VERISSIMO (Principal Investigator)
Area:	Computer Science & ICT Security

Description

Complex autonomous real-time and embedded systems (RTES), e.g. self-driving cars, will increasingly operate unattended over extended periods of time. The limitations of continuous supervision given their real-time nature, and the threat vectors originating from combined cyber and physical attacks, make these systems vulnerable and call for improved protection, such as tolerance to intrusions, in particular in face of time-domain attacks, to achieve safety and security in such critical systems. In this project, we investigate the interplay of intrusion tolerance techniques, such as Byzantine fault-tolerant consensus (BFT), and real-time communication and processing paradigms, e.g. event- and time-triggered abstractions. To date, the examples of research in this area are confined to very specialised and constrained RTES (e.g. flight control), thus not generalizable, and providing limited safety-security balance. Hence the hardness of the problem of reconciling security paradigms, of asynchronous (non-timed) nature, with real-time paradigms, of non-secure nature, to achieve secure and timely operation and cooperation of autonomous systems, over general networks. ByzRT will bridge this gap, by investigating on two essential fronts: - devising innovative BFT algorithms exhibiting real-time capability for single- and inter-RTES operation; and - extending formal methods for proving such protocols correct, by incorporating notions of time and hybridisation. If successful, ByzRT will significantly contribute to the design of safer and more secure critical cyber-physical systems.

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

Acronym:	STV
PI:	Peter Y A RYAN
Funding:	Fonds National de la Recherche - CORE - Core International
Budget:	1.280.000,00 €

Duration:	1 Sep 2019 – 31 Aug 2022
Member:	Peter Y A RYAN (Principal Investigator)
Area:	Security, Reliability and Trust in Information Technology

B.21 FNR - CORE - Core Junior Projects

Automated Reasoning with Legal Entities (AuReLeE)

  https://aurelee.net/

Acronym:	AuReLeE
PI:	Alexander STEEN, Leon VAN DER TORRE
Funding:	Fonds National de la Recherche - CORE - Core Junior
Budget:	508.697,00 €
Duration:	1 Mar 2021 – 1 Aug 2022
Members:	• Leon VAN DER TORRE (Principal Investigator) • David FUENMAYOR PELAEZ (Research and Development Specialist)

Description

The goal of the project Automated Reasoning with Legal Entities (AuReLeE) is to provide effective and general means for the automation of normative reasoning processes based on legal knowledge bases. To this end, the project will design and implement a dedicated system that combines efficient decision procedures with a flexible approach to import and re-use existing knowledge bases for their employment as underlying contexts for the normative reasoning tasks. The results of AuReLeE hence allow the full utilization of the existing legal knowledge bases' potential for compliance checking.

Future-Proofing Privacy in Secure Electronic Voting

Acronym:	FP2
PI:	Johannes MUELLER
Funding:	Fonds National de la Recherche - CORE - Core Junior
Duration:	1 Jan 2021 – 31 Dec 2023
Member:	Johannes MUELLER (Principal Investigator)

B.22   FNR - Industrial Fellowships Projects

Application of Near Field Technology in Commercial Vehicle Tire Monitoring System

Acronym:	NFT
Reference:	R-AGR-3426-10
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - Industrial Fellowships
Budget:	51.000,00 €
Duration:	15 Sep 2018 – 15 Sep 2022
Members:	• Thomas ENGEL (Principal Investigator) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Ahmad RIDA (Doctoral Candidate)
Area:	Communicative Systems
Partner:	Goodyear S.A.

Description

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

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

Collaboration21

 http://collaboration21.uni.lu

Acronym:	C21
PI:	Christoph SCHOMMER

Funding:	Fonds National de la Recherche - Industrial Fellowships
Duration:	12 Jan 2022 – 12 Jan 2027
Member:	Christoph SCHOMMER (Principal Investigator)
Partner:	CISCO

Description

The public-private partnership COLLABORATION 21 is an interdisciplinary research program that responds to pressing 21st-century challenges such as the shortage of collaboration skills and the recent pandemic-induced "social distancing". It aims to leverage digital technologies to enhance people's experience for better collaborative learning and working.

Researchers from the University of Luxembourg team up with Cisco – the world leader in digital technologies for collaboration – and with SCRIPT – a national agency driving innovation and digitalization in Luxembourg's schools. Together they address seven research challenges at the intersection of user experience, educational sciences and digital technologies

The project outcomes of 10 PhD candidates and 2 Postdocs will yield numerous actionable insights to support education and the workforce, covering the entire spectrum from fundamental to applied research

B.23 FNR - INTER Projects

An integrated approach to study the delegation of decision-making to autonomous agents in socio-technicalsystems

Acronym:	DELICIOS
PI:	Jean BOTEV
Funding:	Fonds National de la Recherche - INTER
Budget:	867.141,00 €
Duration:	1 Nov 2019 – 31 Oct 2023
Members:	• Jean BOTEV (Principal Investigator) • Ningyuan SUN (Doctoral Candidate)
Areas:	• Computational Sciences • Security, Reliability and Trust in Information Technology
Partners:	• Ghent University • Vrije Universiteit Brussel

Description

In this age of ubiquitous digital interconnectivity, we may envisage that humans will increasingly delegate their social, economic or data-related transactions to an autonomous agent, for reasons of convenience or complexity. Although the scientific knowledge to create such systems appears to be available, this transformation does not appear to become commonplace soon, except maybe the use of basic digital assistants. We aim to explore if this is due to the lack of knowledge about human trust and acceptance of artificial autonomous delegates that make decisions in their place or even how these delegates should be designed. We study these questions using computational agents models that are validated in a series of behavioural experiments defined around the public goods game. We investigate when and how the autonomous agent may evolve from observer, over decision support to a delegate with full autonomy in decision-making. Using VR and AR technologies, we will investigate if the representation in which the agent is experienced influences trust. All the technology-oriented research is checked against socio-technology acceptance theories through an intricate collaboration with experts in social sciences. The results of this fundamental research will allow us to explore important questions related to the intelligence and interface of the envisioned agents, and lay the foundation for new types of online markets that brings autonomous agents into real-world applications.

Analysis and Protection of Lightweight Cryptographic Algorithms

⮺ https://www.fnr.lu/projects/analysis-and-protection-of-lightweight-cryptographic-algorithms/

Acronym:	APLICA
PI:	Alexei BIRYUKOV
Funding:	Fonds National de la Recherche - INTER
Duration:	1 Jan 2021 – 31 Dec 2023
Members:	• Alexei BIRYUKOV (Principal Investigator) • Johann GROSZSCHÄDL (Researcher) • Baptiste LAMBIN (Researcher) • Aleksei UDOVENKO (Researcher) • Anne OCHSENBEIN (Project Coordinator)
Areas:	• Computer Science & ICT Security • Information Security • Security, Reliability and Trust in Information Technology
Partners:	• Gregor Leander • Ruhr-Universität Bochum

Description

The Internet of Things (IoT) represents the next phase of the evolution of the Internet towards a network that integrates the physical world into the virtual world. In the near future,

the vast majority of devices connected to the Internet will not be classical computers like PCs, laptops, or smart phones, but miniature sensor nodes, actuators, and various other kinds of "smart" devices with computation and communication capabilities. This evolution will create a strong demand for lightweight cryptographic algorithms that are suitable for devices with extreme resource constraints such as RFID tags. Recently, the US National Institute of Standards and Technology (NIST) announced an initiative to standardize lightweight hash functions and authenticated encryption schemes in an open process with public evaluation. The mission of the APLICA project is to contribute to the evaluation of the more than 50 candidate algorithms submitted to the NIST by analyzing their theoretical and practical security properties. More concretely, APLICA will contribute to the development of new cryptanalytic techniques (including new software tools for cryptanalysis) that can be applied to lightweight authenticated encryption algorithms and hash functions, and to the design and implementation of new countermeasures against side-channel attacks, in particular differential power analysis, that are suitable for resource-constrained IoT devices. Both topics have the potential to create significant real-world impact since the NIST-standardized algorithms will likely get deployed in billions of devices.

Results

The APLICA project started in January 2021 as a joint research effort between the CryptoLux group of the University of Luxembourg (UL) and the Workgroup for Symmetric Cryptography of the Ruhr-University Bochum (RUB). Its main goals are (i) to evaluate the security of lightweight symmetric cryptosystems, in particular the candidate algorithms (and eventual standards) of the currently-ongoing Lightweight Cryptography (LWC) standardization project of the NIST and (ii) to support the candidates submitted by UL and RUB. The security evaluation takes into account both classical cryptanalysis (i.e., the analysis of the security of an algorithm in a mathematical sense) and their robustness against physical attacks (i.e., analysis under assumption that an attacker can observe certain implementation-related properties of a cryptographic algorithm while it is executed on a device, such as the execution time or power consumption).

In 2022, the APLICA team at UL focused on three main topics in the area of lightweight cryptosystems, namely cryptanalysis, white-box protection against physical attacks, and efficient implementation. (i) The project team improved a key-recovery framework for differential cryptanalysis, called Meet-in-the-Filter (MiF), which was initially developed in the course of the APLICA project. MiF is suitable for symmetric algorithms with a slow or incomplete diffusion layer, such as ciphers based on the Addition-Rotation-XOR (ARX) design principle. The APLICA team gained more insights into the theoretical and practical aspects of the MiF technique and simplified its application. These advances made it possible to achieve the best-to-date single-key differential attacks against the block cipher families Cham and Katan. (ii) The project team developed practical attacks against white-box implementations of ARX-based ciphers using implicit functions and quadratic-affine encodings, which were introduced at CRYPTO 2022. In the white-box model, the attacker is assumed to have direct access to (and full control over) the implementation of a cryptographic algorithm and its execution environment, which includes the ability to tamper with the implementation in any way. The APLCICA team found various attacks against the white-box techniques from CRYPTO 2022 that only use the round functions as oracles and do not rely on their description. These attacks were experimentally verified on white-box instances of the lightweight block ciphers Speck-32/64 and Speck-64/128 and led to the conclusion that a single ARX round is too weak to be used as a white-box round. (iii) The APLICA team contributed to an assessment of the efficiency (i.e., execution time and code size) of

the ten final-round NIST LWC candidates on the 32-bit RISC-V platform. Two implementation options were considered, namely pure software implementation using the RV32B ("BitManip") extension in addition to the base RV32I instruction set and hardware/software co-design where the most performance-critical operations of the underlying low-level primitive were accelerated through the integration of custom instructions. Experimental results showed that, in both implementation scenarios, the permutation-based designs ASCON, SPARKLE, TinyJAMBU, and Xoodyak are particularly efficient.

Brainsourcing for Affective Attention Estimation

Acronym:	BANANA
PI:	Luis A. LEIVA
Funding:	Fonds National de la Recherche - INTER
Budget:	800.307,00 €
Duration:	1 Feb 2022 – 31 Jan 2025
Member:	Luis A. LEIVA (Principal Investigator)

Description

Attention estimation and annotation are tasks aimed at revealing which parts of some content are likely to draw the users' interest. Previous approaches have tackled these incredibly challenging tasks using a variety of behavioral signals, from dwell-time to clickthrough data, and computational models of visual correspondence to these behavioral signals. Today, these signals are leveraged by a myriad of online services to personalize social media, search engine results, recommender systems, and even in supporting critical decision making, such as financial or medical data. However, the signals that all these services are based on are rough estimations of the real underlying attention and affective preferences of the users. Indeed, users may attend to some content simply because it is salient, but not because it is really interesting, or simply because it is outrageous. In contrast, project BANANA will use brain-computer interfaces (BCIs) to infer users' preferences and their attentional correlates towards visual content, as measured directly from the human brain. We aim for a scientific breakthrough by proposing the first-of-its-kind affective visual attention annotation via brainsourcing, i.e. crowdsourced BCI signal acquisition. First, our approach will allow accurate estimation of user preferences, attention allocation, and –critically– the affective component of attention, directly measured from the natural and implicit brain potentials evoked in response to users experiencing digital contents. Then, we will utilize the resulting data in a crowdsourcing setting to reveal how multiple users react to different stimuli and how their attention and affective responses are distributed. These collective responses will produce unified, consistent measures as a result. Our technology will be used in several downstream tasks such as segmentation of users' attention while looking at images, identification of key events, and video summarisation. We will pilot BANANA with different user groups to test and prove its effectiveness, using objective benchmarks and evaluation strategies.

Intelligent aNd orcheStrated securIty and privacy-aware slicing for 5G and beyond veHicular neTworks

Acronym:	5G-INSIGHT
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - INTER
Budget:	1.300.041,00 €
Duration:	1 Apr 2021 – 31 Mar 2024
Member:	Thomas ENGEL (Principal Investigator)
Area:	Computer Science & ICT Security

Description

Network slicing is considered as the key technology of an agile Vehicle-to-everything deployment. However, most deployments in Europe focus on evaluating the network performance and ignore the security and privacy aspects, notably in a cross-border scenario.

Building on key 5G technologies (SDN, NFV) and machine learning algorithms (federated and deep learning), 5G-INSIGHT aims at (a) proposing new techniques for road and network traffic prediction, thus allowing the early detection of intrusions and anomalies within 5G vehicular slices, (b) enforcing security-by-design and privacy-preserving slicing policies for attack mitigation and personal data anonymization, and (c) developing resource orchestration and management across multiple potential providers using federated slicing. Proposed approaches will be validated by simulations as well as by a demonstration platform (proof-of-concept) that integrates the specific characteristics of the France-Luxembourg cross-border area.

Intelligent orchestrated security and privacy-aware slicing for 5G and beyond vehicular networks

Acronym:	5G-INSIGHT
Reference:	R-AGR-3925-10
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - INTER
Budget:	1.649.301,00 €
Duration:	1 Apr 2021 – 31 Mar 2024
Members:	• Thomas ENGEL (Principal Investigator) • Stefanie OESTLUND (Project Coordinator) • Abdelwahab BOUALOUACHE (Research Associate)
Area:	Computer Science & ICT Security
Partners:	• Université Gustave Eiffel

- Université de Bourgogne
- Université de La Rochelle

Description

The tremendous technological developments in the automotive industry today are mainly fuelled by the development of vehicle-to-everything (V2X) communication capabilities and new automated driving features. Given their intrinsic requirements in terms of ultra-low latency and ultra-high reliable connectivity under high-mobility conditions, these features will only be unlocked over the long run with the large-scale adoption of 5G technologies. Among them, network slicing is considered as the key technology of an agile V2X use-case deployment, ensuring network flow isolation, resource assignment, and network scalability. However, while most deployments in Europe focus on evaluating the resulting network performance, security and privacy challenges associated with this technology have not been much investigated, notably in a cross-border scenario. Building on key 5G technologies (SDN, NFV) and machine learning algorithms (federated and deep learning), 5G-INSIGHT aims at: (a) proposing new techniques for road and network traffic prediction, thus allowing the early detection of intrusions and anomalies within 5G vehicular slices; (b) enforcing security-by design and privacy-preserving slicing policies for attack mitigation and personal data anonymization respectively; and (c) developing resource orchestration and management across multiple potential providers using federated slicing. The project will validate the proposed approaches by implementing simulations as well as a demonstration platform (Proof-of-concept) that will integrate the specific characteristics of the France-Luxembourg cross-border area.

Results

Network slicing is considered the key technology of an agile Vehicle-to-everything (V2X) use-case deployment. However, most deployments in Europe focus on evaluating the network performance and ignore the security and privacy aspects, notably in a cross-border scenario. 5G-INSIGHT (ANR-FNR project) aims to fill this gap by building novel security mechanisms ranging from attack detection to attack mitigation leveraging novel tools and paradigms such as those based on Machine-Learning (ML), particularly federated and deep learning, to Blockchains and Deception Security, all while considering the specific but very sensitive (in terms of security) case of cross-border areas (i.e., the France-Luxembourg border-crossing case). 5G-INSIGHT has started in April 2021. The SECAN-lab team is responsible to coordinate Luxembourg activities in this project.

In 2022, the SECAN-lab have contributed to successfully closing activities for Work Package (WP) 2 of this project. Specifically, our team has contributed to concluding the study on the security challenges of 5G-V2X at the cross border and has successfully led Task and deliverable 2.3 and delivered related inputs. Some results of the SECAN-lab work for WP2 have been published as a survey paper in IEEE Communications Surveys & Tutorials and a magazine paper in IEEE Internet of Things Magazine. Moreover, as a WP4 and task (T4.2) leader, the SECAN-lab has made significant progress in this WP. Specifically, SECAN-lab has developed a deep learning-based intra-slice attack detection mechanism for 5G-V2X sliced networks for T2.1. The results of this work have been published as a paper in Vehicular Technology Conference (VTC)-Spring 2022. The team has also developed a federated Learning-based Inter-slice attack detection mechanism for 5G-V2X Sliced Networks. The results of this work have been published in VTC-Fall 2022. Besides this, the SECAN-lab has

collaborated with other partners in the consortium to propose two works related to WP4 and WP6 respectively. The results of these works have been published at the 2022 IEEE Global Communications Conference (GLOBECOM).

Personalized Explainable Artificial Intelligence for decentralized agents with heterogeneous knowledge

Acronym:	EXPECTATION
PI:	Leon VAN DER TORRE
Funding:	Fonds National de la Recherche - INTER
Budget:	946.005,00 €
Duration:	1 Apr 2021 – 31 Mar 2024
Members:	• Leon VAN DER TORRE (Principal Investigator) • Joris HULSTIJN (Researcher) • Igor TCHAPPI HAMAN (Researcher)
Area:	Computer Science & ICT Security
Partners:	• Amro Najjar • LIST - Luxembourg Institute of Science & Technology • Ozyegin University • University of Applied Sciences and Arts Western Switzerland • Università di Bologna

Description

Explainable AI (XAI) has emerged in recent years as a set of techniques and methodologies aiming at explaining machine learning (ML) models, and enabling humans to understand, trust, and manipulate the outcomes produced by artificial intelligent entities effectively. Although these initiatives have advanced over the state of the art, several challenges still need to be addressed to apply XAI in real-life scenarios adequately. In particular, two key aspects that need to be addressed are the personalization of XAI and the ability to provide explanations in decentralized environments where heterogeneous knowledge is prevalent. Firstly, personalization of XAI is particularly relevant, due to the diversity of backgrounds, contexts, and abilities of the subjects receiving the explanations generated by AI-systems (e.g., patients and healthcare professionals). Henceforth, the need for personalization must be coped with the imperative need for providing trusted, transparent, interpretable, and understandable outcomes from ML processing. Secondly, the emergence of diverse AI systems collaborating on a given set of tasks relying on heterogeneous datasets opens to questioning how explanations can be combined or integrated, considering that they emerge from different knowledge assumptions and processing pipelines. In this project, we want to address those two challenges, leveraging on the multi-agent systems (MAS) paradigm, in which decentralized AI agents will extract and inject symbolic knowledge from/in ML-predictors, which, in turn, will be dynamically shared composing custom explanations. The proposed approach combines inter-agent, intra-agent, and human-agent interactions to benefit from both the specialization of ML agents and the establishment of agent collaboration mechanisms, which will integrate heterogeneous knowledge/explanations extracted

from efficient black-box AI agents. The project includes the validation of the personalization and heterogeneous knowledge integration approach through a prototype application in the domain of food and nutrition monitoring and recommendation, including the evaluation of agent-human explainability, and the performance of the employed techniques in a collaborative AI environment.

Secure, Usable and Robust Cryptographic Voting Systems

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

Description

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

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

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

Long-term security: Electronic records will be protected by cryptography, but they will be public and must remain secure into the future. A specific long-term threat against most existing voting system is quantum computers. This project will address each of these areas. We will contribute to increased confidence in our voting systems, and thereby also in the integrity of the electoral process. Our emphasis on security proofs for voting systems will improve the overall assurance of voting systems, both directly and by establishing a scientific standard in the field of voting systems.

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

Results

In 2022, we have succeeded in publishing/submitting the following papers:

- S. Baloglu, S. Bursuc, S. Mauw, J. Pang. Election Verifiability in Receipt-free Voting Proto-cols. To be presented at IEEE Computer Security Foundations Symposium – CSF 2023
- S. Baloglu, S. Bursuc, S. Mauw, J. Pang. Formal Verification, Attacks and Solutions for the Estonian Voting Protocol. Submitted to ESORICS 2023, under review.

Spin and bias in Language Analyzed in News and Text

Acronym:	SLANT
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - INTER
Budget:	815.385,00 €
Duration:	1 Mar 2020 – 28 Feb 2023
Member:	Sjouke MAUW (Principal Investigator)
Area:	Computer Science & ICT Security

Description

There is a growing concern about misinformation or biased information in public com-munication, be it in traditional media or social forums. While automating fact checking has received a lot of attention recently, the problem of fair information is much larger and much more fundamental. It includes insidious forms like biased presentation of events and discussion and their interpretation. To fully analyse and the problem, an interdisciplinary approach is called for. One needs tools and techniques from Linguistics, to study the struc-ture of texts and the relationships between words and sentences, from Game and Decision Theory, to study the strategic reasoning built into the presentation of texts and their individ-ual interpretation and also from Machine Learning and AI, to automatically detect biased text and develop algorithms to de-bias them. The SLANT project aims at characterising bias in textual data, either intended (eg. in public reporting), or unintended (eg. in writing aiming at neutrality). An abstract model of biased interpretation will be complemented and concretised using work on discourse structure, semantics and interpretation. We will find relevant lexical, syntactic, stylistic or rhetorical differences through an automated but ex-plainable comparison of texts with different biases on the same subject. This will be based on a dataset of news media coverage from a diverse set of sources. We will also explore how our results can help alter bias in texts or remove it from automated representations of texts.

Spin and bias in Language Analyzed in News and Text

Acronym:	SLANT
PI:	Sjouke MAUW

Funding:	Fonds National de la Recherche - INTER
Duration:	1 Mar 2020 – 28 Feb 2023
Members:	• Sjouke MAUW (Principal Investigator)
	• Sviatlana HOEHN (Research Associate)

Description

There is a growing concern about misinformation or biased information in public communication, be it in traditional media or social forums. While automating fact checking has received a lot of attention recently, the problem of fair information is much larger and much more fundamental. It includes insidious forms like biased presentation of events and discussion and their interpretation. To fully analyse and the problem, an interdisciplinary approach is called for. One needs tools and techniques from Linguistics, to study the structure of texts and the relationships between words and sentences, from Game and Decision Theory, to study the strategic reasoning built into the presentation of texts and their individual interpretation and also from Machine Learning and AI, to automatically detect biased text and develop algorithms to de-bias them.

The SLANT project aims at characterising bias in textual data, either intended (eg. in public reporting), or unintended (eg. in writing aiming at neutrality). An abstract model of biased interpretation will be complemented and concretised using work on discourse structure, semantics and interpretation. We will find relevant lexical, syntactic, stylistic or rhetorical differences through an automated but explainable comparison of texts with different biases on the same subject. This will be based on a dataset of news media coverage from a diverse set of sources. We will also explore how our results can help alter bias in texts or remove it from automated representations of texts.

Results

In 2022, we published the following papers in international journals/conferences:

- Sviatlana Höhn, Nicholas Asher, and Sjouke Mauw. Belelect: a new dataset for bias research from a "dark" platform. In Proc. 16th International Conference on web and social media (AAAI ICWSM'22), volume 16(1), pages 1268-1274, Atlanta, Georgia, 2022. AAAI Press.
- Sviatlana Hoehn, Barbara Lewandowska-Toszczyk, Sjouke Mauw, and Dov Gabbay. Dripping the poison: The instruments of bias – A qualitative case study of news articles in four languages over nine years. Journal of applied logics, 2023

What should we do? What can we do? What are we doing!? Studying the limits, problems, and risks associated to autonomous vehicles from an integrative approach

Acronym:	INTEGRAUTO
PI:	Leon VAN DER TORRE

Funding:	Fonds National de la Recherche - INTER
Budget:	192.050,00 €
Duration:	1 Sep 2022 – 31 Aug 2023
Members:	• Leon VAN DER TORRE (Principal Investigator) • Réka MARKOVICH (Main Researcher)
Area:	Computer Science & ICT Security
Partner:	Université du Québec à Trois-Rivières

Description

Technologies are being developed at an alarming rate and citizens are becoming more aware of the social issues related to technological developments. More recently, for example, autonomous vehicles have been under the spotlight given how rapidly these technologies came on the market and how quickly advancements are made in the area. Despite these technological achievements, unfortunate incidents have increased awareness regarding the risks and social issues associated with autonomous technologies. As we saw with Uber and Tesla, for instance, it can be difficult to establish who is responsible in the event of an incident when many parties are indirectly involved. Perspectives from human and social sciences on technological advances are deeply relevant. However, these perspectives can only have a limited impact on technological developments if these ethical and social considerations are not integrated to the practice and the industry. Beside a reflection upon sociopolitical aspects of emerging technologies (e.g., accessibility or social inequities), it is important to understand how values can be reached by specific aspects of the conception and development of technologies. Hence, although theoretical considerations regarding the principles, values and norms that should guide technological developments are important, there is a pressing need to stop reflecting upon the theory and think of feasible ways to apply this theory to concrete cases. This can be understood as a shift of perspective from normative ethics to applied ethics. Accordingly, human and social scientists should not simply tell the industry the values they should be considering, but they should also be able to understand how these values can be integrated within technological developments in order to be able to participate to the coming of an ethical fourth industrial revolution. Human and social sciences should inform technological developments, but they should also be informed by natural sciences and engineering. As such, human and social scientists need to engage in a reciprocal dialog where their concerns are informed by the practice and the industry. Scholars in human and social sciences need to understand the constraints and limitation surrounding technological developments in order to be able to integrate these concerns into their ethical and social reflections. Otherwise, human and social sciences will have a very limited impact on our technological future. The objective of this research project is to address the risks, limits and problems associated with autonomous technologies from an intersectoral approach by promoting interdisciplinary collaborations through students' co-supervision and by establishing partnerships between scholars and the industry. Specifically, our aim is to assess the risks and ethical issues surrounding autonomous technologies (e.g., ethical behavior, responsibility, sustainable development, etc.) in light of their capacities as well as their physical and technical limitations.

B.24   FNR - INTER MOBILITY Projects

Deontic logic for Artificial Intelligence

Acronym: DLAI

PI: Leon VAN DER TORRE

Funding: Fonds National de la Recherche - INTER MOBILITY

Budget: 121.528,00 €

Duration: 1 Sep 2020 – 31 Aug 2022

Member: Leon VAN DER TORRE (Principal Investigator)

Area: Computer Science & ICT Security

Description

Deontic logic is the field of logic that is concerned with obligation, permission, and related concepts. Typically, a deontic logic uses OA to mean it is obligatory that A, and PA to mean it is permitted that A. As explained in the handbook of deontic logic and normative systems, the history of deontic logic has developed from monadic obligations in Von Wright's SDL, via dyadic obligations in preference-based semantics of DSDL, and its representation by ordering-source-based Kratzer systems, to norm-based semantics. As is well known, there is a striking similarity between on the one hand ordering source-based semantics, preference-based semantics and norm-based semantics, and on the other hand the three classes of Makinson's overview of non-monotonic logic: pivot- based systems, preference-based systems, and rule-based systems.

Sabbatical at ANU

Acronym: SAB-ANU

PI: Sjouke MAUW

Funding: Fonds National de la Recherche - INTER MOBILITY

Budget: 7.450,00 €

Duration: 1 Oct 2022 – 31 Oct 2022

Member: Sjouke MAUW (Principal Investigator)

Area: Computer Science & ICT Security

Description

As part of my sabbatical leave from the University of Luxembourg, I will conduct a two months research visit at the Australian National University (ANU) in Canberra, Australia. The main goals of my research visit will be: 1) I will strengthen my research in security

protocols, especially in relation to the formulation and verification of non-standard security requirements, such as distance bounding; 2) I will draft a new textbook on the specification and verification of security protocols, based on recent advances in this field, in order to replace the current textbook that I wrote a decade ago. At ANU I will cooperate with local experts in the foundations of computer security, in particular with Prof. Alwen Tiu.

Tangible outputs: - Draft paper on distance-bounding protocols. - Draft textbook on the verification of security protocols.

B.25   FNR - JUMP Projects

A Secure Medication Dispenser (REMEDIS)

Acronym:	Remedis
PI:	Christoph SCHOMMER
Funding:	Fonds National de la Recherche - JUMP (Pathfinder)
Budget:	60.000,00 €
Duration:	1 Jan 2022 – 30 Jun 2022
Members:	• Christoph SCHOMMER (Principal Investigator) • Daniel KARPATI (Project Coordinator)

Description

Medical non-adherence (MNA) is one of the most pressing issues in health care. It claims lives, accelerates patients' health deterioration, and its economic impact is tremendous: 818 billion USD annually (WHO, 2020). In developed countries, among patients with chronic illnesses, medical non-adherence averages at 50%. The elderly are particularly vulnerable. Research showed dementia could increase MNA to 58 – 89.3%. It is particularly devastating as their health rapidly deteriorates due to not taking their pills correctly. With our ageing demographics, this problem escalates quickly, and our ecosystem cannot keep up: professional caregivers are overwhelmed, underpaid, and as a result, mistakes frequently happen also in nursing homes. In our project, we develop an automated medication dispenser, particularly for people suffering from dementia. REMEDIS sorts their medication and reminds them of each medication intake. REMEDIS automates the sorting process to the benefit of the patient and simultaneously overcomes all challenges automation presents. How to mitigate if the machine erroneously dispenses a pill? What if the device works fine but was not filled correctly in the first place? How do we make sure users do know what medications are they taking if each dose is automatically sorted for them? Until now, the industry has not come up with a solution that gives satisfying answers to these questions. REMEDIS conclusively solves all three problems and is on its way to being the first secure pill dispenser on the market. We focus on creating a reliable product for those who cannot

rely on managing their medication intake on their own. Our goal with this project is to develop a prototype and prepare for commercialisation. We are using these two years to put the most value into our product for our users.

B.26   FNR - OPEN Projects

Deontic Logic for Epistemic Rights

Acronym:	DELIGHT
PI:	Leon VAN DER TORRE
Funding:	Fonds National de la Recherche - OPEN
Budget:	840.114,00 €
Duration:	1 Sep 2021 – 1 Sep 2024
Members:	• Leon VAN DER TORRE (Principal Investigator) • Aleks KNOKS (Researcher) • Xu LI (Researcher) • Réka MARKOVICH (Main Researcher)
Partners:	• Beishui Liao • Christoph Benzmüller • Freie University Berlin • Google Research Amsterdam • Guillaume Aucher • Huimin Dong • Marc van Zee • Marija Slavkovik • Sun Yat-Sen University • University of Bergen • Université de Rennes • Zhejiang University

Description

Deontic logic is the field of logic that is concerned with obligation, permission, and related concepts. Traditionally deontic logic has been developed as a branch of philosophical logic, in particular in formal ethics, it is used to formalize the normative use of language, thus, it has also widely been used to formalize legal reasoning, and since the early nineties, it has been applied in computer science. On the one hand, DELIGHT is going to develop new formalisms to reason about epistemic rights in the different normative systems, and provides feedback about the coherence and consistency of these right concepts in existing legal and ethical theories and regulations. On the other hand, DELIGHT, applying an overarching methodology for the design of normative reasoners is going to yield a comprehensive and influential study of the extended and all-embracing use of deontic logic in computer science and, especially, in Artificial Intelligence (AI). Practical and social reasoning, that is, reasoning about agents and their actions, decisions, and relations are used in the foundations of explainable AI for the design and engineering of legal and ethical reasoners, and the

control and governance of intelligent autonomous systems. DELIGHT is a basic research project moving vast and complex knowledge from the legal domain to the computer science domain. We are going to investigate deontic logics for reasoning about special normative relations among agents and their normative positions regarding epistemic states: the right to know, the freedom of thought and the right to believe, the right to not know, the right to not be misled, or the right to truth. We develop new deontic logics providing a comprehensive formal analysis of epistemic rights and related legal and ethical concepts, and new reasoning methods to infer which duties follow from these rights, and whether concrete situations in real-life normative systems comply with these rights. Moreover, we evaluate and validate our formal framework using COVID-19 pandemic related legislation and policies in various cultures and legal traditions. Finally, we provide interactive theorem provers to experiment with these new logics, formal models of epistemic rights, and AI applications. These new logics and reasoning systems together with the applied methodology will set the stage for future knowledge representation and reasoning projects in the deontic logic community and develop key technology for AI applications using practical and social reasoning. The deontic logic community faces a great demand for ethical and legal reasoning coming from society. The new methodology with the tool support applied in DELIGHT makes it possible to work and experiment with several different logics, which possibility radically improves our efficiency as deontic logicians and means a major step forward in legal knowledge representation and computational modeling of normative systems.

B.27   FNR - PRIDE Projects

Security and Privacy for System Protection

Acronym:	PRIDE: SPsquared
Reference:	R-AGR-3125
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - PRIDE
Budget:	3.037.120,00 €
Duration:	1 Oct 2016 – 30 Jun 2023
Members:	• Sjouke MAUW (Principal Investigator)
	• Alexei BIRYUKOV (Collaborator)
	• Jean-Sébastien CORON (Collaborator)
	• Thomas ENGEL (Collaborator)
	• Jacques KLEIN (Collaborator)
	• Gabriele LENZINI (Collaborator)
	• Christian MULLER (Collaborator)
	• Jun PANG (Collaborator)
	• Peter Y A RYAN (Collaborator)
	• Radu STATE (Collaborator)
	• Olga GADYATSKAYA (Research Associate)
Areas:	• Computer Science & ICT Security
	• Security, Reliability and Trust in Information Technology

| Partners: | • David Naccache |
| | • Université de Paris - II |

Description

The proposed Doctoral Training Unit (DTU) focuses on information security and privacy, including its storage, processing and transmission. Our Security and Privacy for System Protection (SP2) research program is set up by the leading researchers of DCS research unit and the Interdisciplinary Centre SnT at the University of Luxembourg. The SP2 program is designed to provide a high-quality research environment for PhD students and to strengthen the links between fundamental and applied research. In particular, research is organized in an interdisciplinary way along five themes where the most critical and pressing research challenges will be addressed:

1. Number Theory, Cryptography and Cryptographic Protocols;

2. Implementation of Cryptography;

3. Internet Privacy;

4. System Security;

5. Socio-Technical Security.

In addition to the research program, our DTU offers a comprehensive training and career development program, with a strong quality control framework, that will not only ensure a high quality scientific output but also prepare our students for an excellent future career in academia, industry and governmental environment. We believe that our DTU's contributions will have a significant scientific, economical and societal impact and will realize strategic priorities of the involved institutions.

Results

In 2022, we published the following results in international journals/conferences:

- Z. Zhong, C. Li, J. Pang. Hierarchical message-passing graph neural networks. Data
- Mining and Knowledge Discovery 37: 381-408, 2023.
- Z. Zhong, G. Gonzalez, D. Grattarola, J. Pang. Unsupervised network embedding
- beyond homophily. Transactions on Machine Learning Research, 2022.
- Z. Zhong, S. Ivanov, Jun Pang. Simplifying node classification on heterophyllous graphs with compatible label propagation. Transactions on Machine Learning Research, 2022.
- Z. Zhong, C. Li, J. Pang. Personalised meta-path generation for heterogeneous graph neural networks. Data Mining and Knowledge Discovery, 36(6): 2299-2333, 2022.
- R. Horne, S. Mauw, S. Yurkov. Whenever a privacy property fails a formula describes an attack: A Complete and Compositional Verification Method for the Applied π- Calculus. In Theoretical Computer Science Journal, Elsevier, 2022.
- R. Horne, S. Mauw, S. Yurkov. Unlinkability of an Improved Key Agreement Protocol for EMV 2nd Gen Payments. In IEEE Computer Security Foundations Symposium 2022.

In addition, we also succeeded in making the following submission:

- S. Bursuc, R. Horne, S. Mauw, S. Yurkov. Designing an Unlinkable Smartcard-based payment protocol. Submitted to IEEE Symposium on Security and Privacy 2023.

B.28 FNR (Luxembourg)/NCBiR (Poland) Projects

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

Acronym: STV

PI: Peter Y A RYAN

Funding: FNR (Luxembourg)/NCBiR (Poland)

Duration: 1 Sep 2019 – 31 Aug 2022

Members: • Peter Y A RYAN (Principal Investigator)
                 • Wojciech JAMROGA (Research Associate)
                 • Gabriele LENZINI (Senior Researcher)

B.29 UL Projects

Decentralized global decision-making over dynamic networks of proactive engines

Acronym: Proactive PhD 4

PI: Denis ZAMPUNIERIS

Funding: University of Luxembourg

Duration: 1 Nov 2019 – 1 Nov 2022

Members: • Denis ZAMPUNIERIS (Principal Investigator)
                 • Parisa MAHYA (Doctoral Candidate)
                 • Sandro REIS (Research assistant)

Description

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

global objectives, to deal with potential conflicts between local decisions or their effects, and to pursue goals dedicated to some global optimization purposes.

Proactive computing paradigm applied to the programming of robotic systems

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

Description

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

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

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

Reconstructing gene regulatory networks with neural relational inference

Acronym:	GENERIC
Reference:	U-AGR-6052
PI:	Jun PANG, Lasse SINKKONEN
Funding:	University of Luxembourg
Budget:	399.303,00 €

Duration: 1 Jul 2022 – 30 Jun 2026

Members: • Jun PANG (Principal Investigator)
                  • Lasse SINKKONEN (Principal Investigator)
                  • Tsz Pan TONG (Doctoral Candidate)

Description

Discovering structures of gene regulatory networks (GRNs) based on large-scale high throughput data is a fundamental research challenge in systems biology. The inference of accurate GRNs from data is challenging not only because of the large number of components involved, but also their possible mutual interactions. The inferred network models can provide system-level understanding of the mechanism of cell transformations, which is crucial for the comprehension of the progression of complex diseases such as Parkinson's disease (PD), and the affected cell types.

GENERIC takes an interdisciplinary approach towards GRN inference, integrating theories, techniques and tools from biology and computer science. It aims to devise data-driven deep learning models for inferring GRNs with high accuracy from single-cell gene expression data. In particular, with this proposed project we will be the first to develop novel GRN inference methods by exploiting neural relational inference (NRI) to discover latent inter-actions directly from data. This paves a new way for accurate and efficient reconstruction of comprehensive real-life GRNs.

18Our inference methods combine an iterative graph generation process and reinforcement learning into NRI in order to increase its efficiency and accuracy, and as well to incorporate prior biological knowledge of the studied GRN and well-established GRN structural properties. The development of our methods will be driven and accompanied by application of the methods to single cell gene expression data from differentiation of human dopaminergic neurons (hDAns), a cell type with high biomedical relevance for example in PD. Moreover, the effectiveness and accuracy of the inferred GRNs will be validated in wet-lab using ChIP-seq and CRISPR-dCas9 inhibition experiments in hDAns derived from induced pluripotent stem cells (iPSCs). The newly identified networks will give rise to better control of hDAn differentiation.

Results

We have hired Tsz-Pan Tong to work on the project as a PhD candidate.

B.30   UL and Esch2022 Projects

AI & Art Pavilion

⧉ https://esch2022.uni.lu/projects/aiart/

Acronym:	AI&Art
Funding:	University of Luxembourg, Esch2022
Budget:	300.000,00 €
Duration:	1 Jun 2020 – 31 Dec 2022
Members:	• Amro NAJJAR (Researcher)
	• Daniel KARPATI (Project Coordinator)
	• Sana NOUZRI (Management Committee Member)
	• Igor TCHAPPI HAMAN (Management Committee Member)
	• Christoph SCHOMMER (Project Manager)
	• Leon VAN DER TORRE (Project Manager)

Description

Artificial intelligence (AI) is increasingly going to transform our daily life, and the resulting changes raise fundamental questions about the nature of humanity and the goals of civilisation. The AI&ART Pavilion is a multidisciplinary initiative trying to reflect this emerging future in an interactive context, a place where scientists, artists and the public can meet and exchange ideas. The AI&ART Pavilion does this by combining Belval's industrial heritage with the scientific ambitions of the university, while letting individuals find a sense of community in the face of contemporary and forthcoming challenges.

B.31   UL - University of Luxembourg - Institute for Advanced Studies (IAS) - Audacious projects Projects

Reconstructing gene regulatory networks with neural relational inference (Resubmission)

Acronym:	GENERIC
PI:	Jun PANG
Funding:	UL - University of Luxembourg - Institute for Advanced Studies (IAS) - Audacious projects
Budget:	397.017,00 €
Duration:	1 Jul 2022 – 30 Jun 2026
Member:	Jun PANG (Principal Investigator)
Areas:	• Computer Science & ICT Security
	• Health and Systems Biomedicine - Biomedicine and IT
	• Health and Systems Biomedicine - Research and Healthcare

Description

Discovering structures of gene regulatory networks (GRNs) based on large-scale high throughput data is a fundamental research challenge in systems biology. The inference of accurate GRNs from data is challenging not only because of the large number of components involved, but also their possible mutual interactions. The inferred network models can provide system-level understanding of the mechanism of cell transformations, which is crucial for the comprehension of the progression of complex diseases such as Parkinson's disease (PD), and the affected cell types. GENERIC takes an interdisciplinary approach towards GRN inference, integrating theories, techniques and tools from biology and computer science. It aims to devise data-driven deep learning models for inferring GRNs with high accuracy from single-cell gene expression data. In particular, with this proposed project we will be the first to develop novel GRN inference methods by exploiting neural relational inference (NRI) to discover latent interactions directly from data. This paves a new way for accurate and efficient reconstruction of comprehensive real-life GRNs. Our inference methods combine an iterative graph generation process and reinforcement learning into NRI in order to increase its efficiency and accuracy, and as well to incorporate prior biological knowledge of the studied GRN and well-established GRN structural properties. The development of our methods will be driven and accompanied by application of the methods to single cell gene expression data from differentiation of human dopaminergic neurons (hDAns), a cell type with high biomedical relevance for example in PD. Moreover, the effectiveness and accuracy of the inferred GRNs will be validated in wet-lab using ChIP-seq and CRISPR-dCas9 inhibition experiments in hDAns derived from induced pluripotent stem cells (iPSCs). The newly identified networks will give rise to better control of hDAn differentiation.

B.32   Other Funding Source Projects

Advanced Methods of Quantization, Compression and Learning in Artificial Intelligence

Acronym:	Com-in-AI
PI:	Vladimir DESPOTOVIC
Budget:	189.588,00 €
Duration:	1 Sep 2020 – 31 Aug 2022
Member:	Vladimir DESPOTOVIC (Principal Investigator)
Area:	Computer Science & ICT Security

Description

Decreasing computational complexity and memory resources are of particular importance for implementation of AI algorithms in portable and edge computing devices with limited memory and processing power. Related research in this area is still in early stage and deserves further investigation; therefore our project will contribute by proposing innovative methods of compression and quantization of deep neural network (DNN) parameters

(weights, biases, activations) and deep features. The goal of the project is to develop a state-of-the-art DNN model with a high performance not only on the hardware commonly used for AI applications, but also on devices with limited computational resources and thus enabling them to support energy demanding and memory constraint applications. In order to achieve these goals, the project proposes an integrated approach to quantization and compression of DNN parameters, based on statistical modeling of data per layers, as well as data subsets within layers and adaptation of the quantizers on the statistical characteristics of the input data. Moreover, from the exploration of the compression and quantization effects in DNNs with regard to their performance, the benchmark of our methodology will be defined. The researchers' interdisciplinary competences ensure successful development of innovative quantization, compression and learning methodologies that will enable reducing the complexity of AI algorithms and its much wider usage. The results obtained within this project will find a wide range of applications in both academia and industry, particularly in numerous latency-critical services.

African Cyber Security Resource Centre for Financial Inclusion

Acronym:	AfricaCSRC
PI:	Tegawendé François d Assise BISSYANDE
Budget:	5.454.545,00 €
Duration:	1 Jan 2020 – 31 Dec 2024
Member:	Tegawendé François d Assise BISSYANDE (Principal Investigator)
Area:	Computer Science & ICT Security

Description

The project will scale up our experience for financial inclusion in Africa to drastically improve cyber resilience in SSA in three years with the support of # 200 cyber security experts from Luxembourg and Africa. ⊠ Luxembourg is a large financial centre and a longstanding partner of financial inclusion. It has also built a large cyber security ecosystem with >300 cyber security companies including 68 startups. The 74 companies that have cyber security as core business are employing 1.000 experts. ⊠ The project is articulated around 3 complementary types of organization as recommended by international cyber security frameworks: - ISAC (Information Sharing and Analysis Centre), - CSIRT (Computer Security Incidents Response Teams), - C-SOC (Cyber Security Operation Centre). ⊠ The consortium deliverable will include: - Set up a continental ISAC and a scalable sub regional centres network (3 CSIRT and 3 SOC), a unique 90 experts taskforce - Build a cyber security community for financial inclusion, connected to other international, regional or local communities, ⊠ Offer expert advisory services to central banks regulating the sector, ⊠ Massive lasting capacity building and security awareness including training teachers (12 PhD) in partnership with African Universities, ⊠ Deliver key services at the highest level of international standards (open source threat intelligence and detection software, maturity assessment, security supervision, incident response, crisis management, penetration testing, governance ...), at a fraction of the cost through mutualization and capacity maintenance. ⊠ The consortium will manage the project as a multi stake holder project. International Financial Inclusion public and private partners are already involved and will be instrumental to reach

the ambitious targets. ⬜ The interconnected SOC and CSIRT network will provide Business Continuity in case of serious events, ⬜ The expertise acquired through the project for building international communities will be available to expand to other continents or develop similar programs for other critical sectors, e.g. electricity, telco, health, and governments.

Automated GDPR compliance checking of documents and processes

Acronym:	icomplai
PI:	Tomer LIBAL
Budget:	199.158,00 €
Duration:	1 May 2021 – 30 Apr 2023
Member:	Tomer LIBAL (Principal Investigator)
Area:	Computer Science & ICT Security

Description

Since the introduction of the GDPR in 2018, privacy law compliance checking has gained much importance, both financially and ethically. Despite that, a relatively small number of software exists, which can help in this process. Moreover, the current software solutions suffer from several problems, such as inexplainability and nontransparency, which restricts their usability in practice. The icomplai project utilizes technologies that are widely used in high-risk domains, such as train control, for providing an easy-to-use, fully automatic, transparent and explainable interface for privacy law compliance checking of various documents and processes

CLOUDMAP

Acronym:	CLOUDMAP
PI:	Jean-Sébastien CORON
Budget:	2.500.000,00 €
Duration:	1 Sep 2018 – 31 Aug 2023
Member:	Jean-Sébastien CORON (Principal Investigator)
Areas:	• Computational Sciences
	• Security, Reliability and Trust in Information Technology

Description

Homomorphic cryptography offers the tantalizing goal of being able to process sensitive information in encrypted form, without needing to compromise on the privacy and se-

curity of the citizens and organizations that provide the input data. And more recently, cryptographic multilinear maps have revolutionized cryptography with the emergence of indistinguishability obfuscation, which has been used to realize numerous advanced cryptographic tasks that previously seemed beyond reach. The goal of the proposal is to improve the efficiency of existing homomorphic encryption and multi- linear map schemes and possibly design new ones, in order to bridge the gap between the theoretical constructions and the concrete applications.

CMSB 2023

Acronym:	CMSB 2023
PI:	Jun PANG
Budget:	23.000,00 €
Duration:	1 Nov 2022 – 14 Dec 2023
Member:	Jun PANG (Principal Investigator)
Area:	Computer Science & ICT Security

Co-creating resIlient and susTaInable food systEms towardS FOOD2030

Acronym:	CITIES2030
PI:	Thomas ENGEL
Duration:	1 Oct 2020 – 30 Sep 2024
Member:	Thomas ENGEL (Principal Investigator)
Area:	Computer Science & ICT Security

Description

Urban food systems and ecosystems (UFSE) demand immediate action. CITIES2030 innovative approach have a great opportunity to attract the best researchers, entrepreneurs, civil society leaders, cities and all agents of the UFSE as well. The main goal of CITIES2030 is to create a future proof and effective UFSE via a connected structure centered in the citizen, built on trust, with partners encompassing the entire UFSE. CITIES2030 commit to work towards the transformation and restructuring of the way systems produce, transport and supply, recycle and reuse food in the 21st century. CITIES2030 vision is to connect short food supply chains, gathering cities and regions, consumers, strategic and complement industry partners, the civil society, promising start-ups and enterprises, innovators and visionary thinkers, leading universities and research across the vast diversity of disciplines addressing UFSE, including food science, social science and big data. CITIES2030 actively encourage the participation of citizens by delivering a trusted UFSE, moving consumers from being passive recipients to active engagement and motivated change agents. This objective is achieved via multiple tools delivered by CITIES2030 such as the CRFS Alliance,

a community of practice supported by a digital platform, reaching all over Europe and beyond. This approach will enable innovation actions and enhancements on a pan-European scope with a global reach. Cities and regions will improve resilience and sustainability, and their leadership will create short food supply chain and ecosystems enabling local investments, trans-borders and transnational deployment. A blockchain-based data-driven UFSE management platform will secure intelligence and coordination actions by delivering an accurate, almost real-time digital twin of the whole supply chain, e.g. from production to waste management, but also on key enablers of resilience and sustainability.

Cyber Security Network of Competence Centres for Europe

Acronym: CyberSec4Europe

PI: Paulo ESTEVES-VERISSIMO

Budget: 15.999.981,00 €

Duration: 1 Jan 2019 – 30 Jun 2022

Member: Paulo ESTEVES-VERISSIMO (Principal Investigator)

Area: Computer Science & ICT Security

Description

CyberSec4Europe is a research-based consortium with 44 participants covering 21 EU Member States and Associated Countries. It has received more than 40 support letters and promises of cooperation from public administrations, international organisations, and key associations worldwide including Europe (such as ECSO), Asia, and North America. As pilot for a Cybersecurity Competence Network, it will test and demonstrate potential governance structures for the network of competence centres using the best practices examples from the expertise and experience of the participants, including concepts like CERN. CyberSec4Europe will support addressing key EU Directives and Regulations, such as GDPR, PSD2, eIDAS, and ePrivacy, and help to implement the EU Cybersecurity Act including, but not limited to supporting the development of the European skills-base, the certification framework and ENISA's role. The 26 ECSO participants in CyberSec4Europe are active in all 6 ECSO Working Groups, including chairing many subgroups in cybersecurity certification, vertical sectors, and international cooperation, as well as having representatives on the ECSO Board of Directors and the Cybersecurity Public-Private Partnership Board. CyberSec4Europe participants address 14 key cybersecurity domain areas, 11 technology/applications elements and nine crucial vertical sectors. With over 100 cybersecurity projects, CyberSec4Europe participants have been addressing a comprehensive set of issues across the cybersecurity domain. The project demonstration cases will address cybersecurity challenges within the vertical sectors of digital infrastructure, finance, government and smart cities, health and medicine and transportation. In addition to the demonstration of the governance structure and the operation of the network, CyberSec4Europe will develop a roadmap and recommendations for the implementation of the Network of Competence Centres using the practical experience gained in the project.

Digitalisation, Law and Innovation

⤢ https://wwwfr.uni.lu/recherche/fdef/dl/dillan

Acronym:	DILLAN
Duration:	14 Apr 2020 – 31 Dec 2025
Members:	• Vincent DE WIT (Doctoral Candidate) • Réka MARKOVICH (Co-Supervisor) • Leon VAN DER TORRE (Co-Supervisor)
Partner:	University of Luxembourg, Faculty of Law, Economics and Finance

Description

DILLAN brings together researchers from various fields of law with those having a background in artificial intelligence and computer science, in order to allow for a common effort to study possibilities and regulatory needs for adapting our European multi-level legal system to the opportunities and challenges of the ongoing digital revolution. It will contribute to the design of research-informed pathways in order to ensure that digitalization will not only enhance efficiency in problem solving, but also protect the rule of law, democracy, transparency and the protection of fundamental individual rights.

Elements of AI 2022 and 2023

Acronym:	Elements of AI 2022 and 2023
PI:	Christoph SCHOMMER, Leon VAN DER TORRE
Budget:	25.000,00 €
Duration:	1 Dec 2022 – 30 Nov 2024
Members:	• Christoph SCHOMMER (Principal Investigator) • Leon VAN DER TORRE (Principal Investigator) • Salima LAMSIYAH (Researcher) • Sana NOUZRI (Main Researcher)
Area:	Computer Science & ICT Security

Future Network Academy

Acronym:	FNA
PI:	Thomas ENGEL
Budget:	400.000,00 €

Duration:	1 Sep 2022 – 31 Aug 2025
Member:	Thomas ENGEL (Principal Investigator)
Areas:	• Computer Science & ICT Security
	• Education

Description

5G will serve as a backbone of the numerical revolution. Massive data transfers need not only high broadband but also low latency for real-time applications which are essential for the industry. 5G is next generation wireless network technology that's expected to change the way people live and work. It will be faster and able to handle more connected devices than the existing 4G LTE network, improvements that will enable a wave of new kinds of tech products. While applications of fasted connected devices could improve a lot of areas (environment, agriculture, workspace, management of pollution, medicine, etc.), the Huawei controversy in 2018 has risen the policy maker and wider public's attention on the sovereignty issue underlying 5G development. While market players are largely responsible for the secure rollout of 5G, and EU Member States are responsible for national security, 5G network security is an issue of strategic importance for the entire Single Market and the EU's technological sovereignty. Awareness about this issue is indispensable to ensure EU businesses and citizens can make full use of all the benefits of the new technology in a secure way. There is a critical and urgent education and training need to enable innovation and support the digital transformation. The objective of 5G Academy is to provide educational resources at different level (undergraduates and in-service training) and to different audience (scientific students, entrepreneurs students, policy makers) beyond the natural audience of network specialists. Margrethe VESTAGER, Commissioner for Competition and chair of the Commission's group "Europe Fit for the Digital Age": "We can do great things with 5G. The technology supports personalised medicines, precision agriculture and energy grids that can integrate all kinds of renewable energy. This will make a positive difference. But only if we can make our networks secure. Only then will the digital changes benefit all citizens."

Hinting at Malicious Code in Android Apps Identifying Malicious Payloads in Malware at Market Scale with Graph and Data Clustering Techniques

Acronym:	HitDroid
Reference:	R-AGR-3219-00
PI:	Jacques KLEIN
Budget:	263.753,00 €
Duration:	15 Feb 2019 – 30 Sep 2022
Members:	• Jacques KLEIN (Principal Investigator)
	• Jacques KLEIN (Supervisor / Scientific Advisor)
	• Tegawendé François d Assise BISSYANDE (Research Associate)
Area:	Security, Reliability and Trust in Information Technology

Description

In HitDroid, we aim at proposing a new malware detection approach in mobile ecosystems. It builds on our previous work investigating millions Android apps to reveal how malware is mostly built via repackaging popular apps. Although the community is slowly focusing on repackaged app detection, the existing approaches remain impractical because they require pairwise comparison of apps.

We propose an original detection approach that analyses each app alone, making the approach practical, leveraging graph mining techniques to identify alien code grafted to an "original" code graph.

The project cost will be 140945 €, out of which 131345 € staff costs.

Luxembourg/West Africa Lab for Higher Education Capacity Building in Cyber Security and Emerging Topics in ICT4Dev

Acronym:	LuxWAys
PI:	Tegawendé François d Assise BISSYANDE
Budget:	3.555.797,00 €
Duration:	1 Jun 2020 – 31 May 2026
Member:	Tegawendé François d Assise BISSYANDE (Principal Investigator)
Area:	Computer Science & ICT Security

Description

Le projet LuxWAyS est un projet ambitieux qui s'inscrit dans le cadre de la coopération universitaire entre le Luxembourg et les pays de la Coopération luxembourgeoise. LuxWAyS a pour objectif de former des compétences en cyber-sécurité dans la sous-région Afrique de l'Ouest. Cette initiative est originale car elle croise plusieurs priorités : - Permettre l'établissement d'une coopération Sud-Sud qui sera initiée, appuyée et encouragée par le Luxembourg à travers la création d'un cadre de collaboration scientifique universitaire. - Mettre en avant les expertises de l'écosystème luxembourgeois sur une thématique de pointe embrassée par les acteurs luxembourgeois, notamment la digitalisation et la cyber-sécurité. - Contribuer à l'employabilité des jeunes à travers la mise en place d'un tremplin pour la création de cursus pour lesquels les besoins sont immenses sur le marché. - Pérenniser l'investissement de la Coopération luxembourgeoise dans le « digital » au sein des pays de la Coopération (ex., Burkina Faso, Sénégal) grâce à une mise à disposition de compétences en mesure de s'assurer de leur fonctionnement sécurisé. - Contribuer à la maîtrise de l'immigration intellectuelle par l'appui à la formation des formateurs locaux de haut niveau en mesure de fournir la même qualité d'enseignement. - Promouvoir et prendre compte la dimension genre dans le recrutement et la formation des futurs enseignants-chercheurs et experts dans le domaine de la cyber-sécurité. Le projet, porté par le centre interdisciplinaire SnT de l'Université du Luxembourg, cadre parfaitement avec les principes et les recommandations énoncés dans le rapport1 « New Africa-Europe Digital Economy – Accelerating the Achievement of the Sustainable Development Goals » de la Commission

Européenne. Parmi les principes énumérés par La DETF (EU-AU Digital Economy Task Force) pour permettre la prioritisation des actions de coopération, le projet LuxWAyS respecte de manière intrinsèque les suivants : - « African leadership » (le projet est avant tout le fruit de l'expression d'un besoin des universités partenaires en Afrique avec lesquelles l'Université du Luxembourg a déjà entrepris des collaborations). - « Human-centered » (le projet est focalisé sur la construction du capital humain) - « Mutually beneficial for African and Europe » (le projet permettra la création de compétences pour les partenaires, tout en pourvoyant des ressources humaines pour l'avancée de recherche technologique à Luxembourg) Finalement, LuxWAyS répond à l'une des cinq précieuses recommandations de la commission européenne : donner la priorité à la création de compétences (voir extrait du rapport ci-dessous)

NIR Watchdog PoC

Acronym:	NIRW PoC
PI:	Radu STATE
Budget:	375.000,00 €
Duration:	15 Jan 2021 – 14 Jan 2023
Member:	Radu STATE (Principal Investigator)
Area:	Computer Science & ICT Security

Description

NIR Watchdog unifies Near-infrared spectroscopy (NIRS), is a type of electromagnetic spectroscopy used to measure the molecular composition of materials. This project aims to rapidly identify counterfeit products amounting to the loss of €60bn/year.

PIDSKG

Acronym:	PIDSKG
PI:	Sjouke MAUW
Budget:	3.500,00 €
Duration:	15 Mar 2022 – 14 Dec 2022
Member:	Sjouke MAUW (Principal Investigator)
Area:	Computer Science & ICT Security

Description

PIDSKG

REMEDIS - A secure medication dispenser

Acronym: REMEDIS

PI: Christoph SCHOMMER

Budget: 364.683,00 €

Duration: 1 Jan 2022 – 30 Apr 2024

Member: Christoph SCHOMMER (Principal Investigator)

Area: Computer Science & ICT Security

Description

Medical non-adherence (MNA) is identified in the literature as one of the most pressing issues in health care. It claims lives, accelerates patients' health deterioration, and its economic impact is tremendous: 818 billion USD annually (WHO, 2020). In developed countries, among patients with chronic illnesses, medical non-adherence averages at 50%. The elderly are particularly vulnerable. Dementia could increase MNA to 58 – 89.3%, studies have shown. The more complex their medication regimen is, the more likely they tend to be on the higher end of the spectrum. It is particularly devastating as their health rapidly deteriorates due to MNA. With our ageing demographics, this problem escalates quickly, and our ecosystem cannot keep up: professional caregivers are overwhelmed, underpaid, and nursing homes can not provide solutions alone. The literature estimates mistakes in administering medications in nursing homes are between 16-42%. REMEDIS is an automated medication dispenser. It is being developed to see through patients struggling with dementia. It sorts their medication and reminds them of each medication intake. REMEDIS automates the sorting process to the benefit of the patient and simultaneously overcomes all challenges automation presents. How to mitigate if the machine erroneously dispenses a pill? What if the device works fine but was not filled correctly in the first place? How do we make sure users do know what medications are they taking? Until now, the industry has not come up with a solution that gives satisfying answers to these questions. REMEDIS conclusively solves all three problems and is on its way to being the first secure pill dispenser on the market. Our technology and system design has multiple checkpoints and can be deployed anywhere to assist medication intake. After the automated sorting process, our software verifies every pill before dispensation. Then the user can identify at a glance which pills they have in their hands independently from our verification process. We focus on creating a reliable product for those who cannot rely on managing their medication intake on their own. Our goal with this project is to develop a prototype and prepare for commercialisation. We are going to use these two years to put the most value into our future spinoff.

Security as a Box

Acronym: SecuBox

PI: Jacques KLEIN

Budget: 353.934,00 €

Duration: 1 Jan 2022 – 30 Jun 2023

Member: Jacques KLEIN (Principal Investigator)

Area: Computer Science & ICT Security

Description

Security by design is now commonly accepted by practitioners and software engineers to design products that are foundationally secure. However, most of the companies do not have the money, nor the expertise, nor the time to invest in software cybersecurity testing. Furthermore, reviewing source code during continuous development is also essential, yet humans cannot realistically review thousands of lines of code, nor artificially propagate data across tens or even hundreds of function calls. Consequently, if small companies do not include security processes for their digital assets, it can be devastating for their business. Recently, our research group proposed several approaches that cope with most of the afore-mentioned limitations for companies. Indeed, as a software engineering research group, we propose automated solutions to detect and fix program properties that allow companies to save money, time, and human expertise. Besides, due to the automated nature of our prototypes, the problem of scaling to large codebases is mitigated. We propose SecuBox, an affordable automated software security testing system-as-a-service that embeds both existing work and numerous of our own research prototypes. Our solution SecuBox can be relied upon during the development process, and post-production. SecuBox will allow: (1) development companies to deliver secure code to clients; (2) companies that receive code from providers to ensure code liability; (3) companies to regularly perform security tests on their systems; and (4) pentesters to accelerate manual code reviews.

Service Contract Matchory

Acronym: Service Contract Matchory

PI: Martin THEOBALD

Budget: 7.200,00 €

Duration: 1 Jun 2022 – 31 Aug 2022

Member: Martin THEOBALD (Principal Investigator)

Area: Computer Science & ICT Security

Sponsored PhD TEGGS

Acronym: TEGGS

PI: Leon VAN DER TORRE

Budget: 33.333,00 €

Duration: 1 Sep 2019 – 31 Aug 2023

Member: Leon VAN DER TORRE (Principal Investigator)

Area: Computer Science & ICT Security

Representational Activities

C.1 Conference Committee Memberships

11th European Congress Embedded Real Time Systems (ERTS 2022)

 ⧉ https://www.erts2022.org/

Location: Toulouse, France, 1 Jun 2022 – 2 Jun 2022.

Description: The ERTS Congress is a unique International cross sector event on Embedded Software and Systems, the "place to be" for actors from universities, research centers and industries :

- **Unique** : no other event have this particular mix of scientist and industrial representatives, acting in several domains, that we have in ERTS !
- **International** : half of our 60 program committee members come from outside of France
- **Cross sector** : all the domains where embedded systems are central, including, but not limited to :

- transportation : aeronautics, automotive, railway, subway and marine
- satellite and space exploration
- e-healthcare
- smart agriculture
- industry
- defence energy
- telecom domains

Completed by a specialized exhibition : a selection of tools providers, SMEs specialized in embedded systems development and integration dedicated to your exact needs.

And it's in Toulouse, **a unique blend of south art of living and high technology**, famous for its aeronautical and space industry, but also for its automotive activity !

The 2020 edition has gathered more than 100 talks, 400 participants and 50 exhibitors, with more than 2000 B2B meetings.

In 2022, we'll do even better; with a special emphasis on embedded computing platforms and networked systems, processes, methods and tools, resilience, human systems, associated and connected systems.

Participating Members:

• Nicolas NAVET (Program Committee Member)

11th International Conference on Complex Networks and their Applications

⤤ https://2022.complexnetworks.org/

Location: Palermo, Italy, 8 Nov 2022 – 10 Nov 2022.

Participating Members:

• Xihui CHEN (Program Committee Member)
• Andrzej MIZERA (Program Committee Member)

12th IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)

Location: Salerno, Italy, 6 Jun 2022 – 10 Jun 2022.

Participating Members:

• Jean BOTEV (Keynote speaker)

12th IEEE Workshop Parallel / Distributed Combinatorics and Optimization (PDCO 2022)

⤤ https://pdco2022.sciencesconf.org

Location: Lyon, France, 30 May 2022 – 3 Jun 2022.

Description: IEEE PDCO 2022, Lyon France will be the 12th edition of our Workshop. It will be held in conjunction with the 36th IEEE International Parallel and Distributed Processing Symposium. The Workshop PDCO comes from the merging of Workshop Parallel Computing and Optimization (PCO) and Workshop Nature Inspired Distributed Computing (NIDISC).

The IEEE Workshop on Parallel / Distributed Combinatorics and Optimization aims at providing a forum for scientific researchers and engineers on recent advances in the field of parallel or distributed computing for difficult combinatorial optimization problems, like 0-1 multidimensional knapsack problems, cutting stock problems, scheduling problems, large scale linear programming problems, nonlinear optimization problems and global optimization problems. Emphasis is placed on new techniques for the solution of these difficult problems like cooperative methods for integer programming problems. Techniques based on metaheuristics and nature-inspired paradigms are considered. Aspects related to Combinatorial Scientific Computing (CSC) are considered.

Participating Members:

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

12th International Workshop on Enterprise Modeling and Information Systems Architectures (EMISA 2022)

Location: Luxembourg, Luxembourg, 2 Jun 2022 – 3 Jun 2022.

Participating Members:

- Qin MA (Program Committee Member)

13th International Conference on Social Informatics (SocInfo)

 ⬀ https://www.dcs.gla.ac.uk/socinfo2022/

Location: Glasgow, United Kingdom, 19 Oct 2022 – 21 Oct 2022.

Participating Members:

- Ninghan CHEN (Program Committee Member)

14th International Conference on Computational Collective Intelligence (ICCCI 2022)

 ⬀ https://iccci.pwr.edu.pl/2022/

Location: Hammamet, Tunisia, 28 Sep 2022 – 30 Sep 2022.

Description: Track chair (SUAV 2022: Special Session on Swarms of UAVs)

Participating Members:

- Grégoire DANOY (Track / Working Group Chair)

14th International Conference on Quality of Multimedia Experience (QoMEX 2022)

Location: Lippstadt, Germany, 5 Sep 2022 – 7 Sep 2022.

Participating Members:

- Jean BOTEV (Program Committee Member)

14th International Symposium on Foundations & Practice of Security (FPS)

 https://www.dcs.gla.ac.uk/socinfo2022/index.html

Location: Ottawa, United Kingdom, 12 Dec 2022 – 14 Oct 2022.

Participating Members:

• Jun PANG (Program Committee Member)

14th International Workshop on Immersive Mixed and Virtual Environment Systems (MMVE 2022)

Location: Athlone, Ireland, 14 Jun 2022 – 17 Jun 2022.

Participating Members:

• Jean BOTEV (Steering Committee Member, Program Committee Member)

14th Metaheuristics International Conference (MIC 2022)

 https://www.ants-lab.it/mic2022/

Location: Ortigia-Syracuse, Italy, 11 Jul 2022 – 14 Jul 2022.

Participating Members:

• Grégoire DANOY (Program Committee Member)

15th IEEE International Conference on Software Testing (ICST'22)

 https://icst2022.vrain.upv.es/

Location: Online, 4 Apr 2022 – 13 Apr 2022.

Participating Members:

• Mike PAPADAKIS (Track / Working Group Chair, Steering Committee Member)
• Yves LE TRAON (Program Committee Member)

15th International Conference on Security for Information Technology and Communications (SECITC 2022)

Location: Bucharest, Romania, 8 Dec 2022 – 9 Dec 2022.

Participating Members:

• Johann GROSZSCHÄDL (Program Committee Member)

16th International Symposium on Theoretical Aspects of Software Engi- neering (TASE)

 https://www.cs.ubbcluj.ro/tase2022/

Location: Cluj, Romania, 25 Aug 2022 – 27 Aug 2022.

Participating Members:

• Jun PANG (Program Committee Member)

16th International Working Conference on Variability Modelling of Software-Intensive Systems

Location: Florence, Italy, 24 Feb 2022 – 25 Feb 2022.

Participating Members:

• Maxime CORDY (Program Committee Member)

17th ACM Asia Conference on Computer and Communications Security (ASIACCS 2022)

Location: Nagasaki, Japan, 30 May 2022 – 2 Jun 2022.

Participating Members:

• Alexei BIRYUKOV (Program Committee Member)

18th IEEE International Workshop on Factory Communication Systems (WFCS'2022)

 https://wfcs22.unipv.it/

Location: Pavia, Italy, 27 Apr 2022 – 29 Apr 2022.

Description: The conference, supported by IEEE and IES and led by the Technical Committee on Factory Automation, will be virtually hosted by the University of Pavia in collaboration with the Institute Industrial IT (inIT) of the Technische Hochschule OWL in Lemgo, Germany: due to the current COVID-19 pandemic, **the event will be completely online**.

WFCS is the largest IEEE conference especially dedicated to communications for (industrial) automation systems. Its main aim is to provide a forum for researchers, developers and practitioners to review and discuss most recent trends in the area and share innovative research directions.

Participating Members:

- Nicolas NAVET (Program Committee Member)
- Tingting HU (Reviewer)

18th International Workshop on Security and Trust Management (STM)

https://sptage.compute.dtu.dk/STM2022/

Location: Copenhagen, Denmark, 26 Sep 2022 – 30 Sep 2022.

Participating Members:

- Sjouke MAUW (Program Committee Member)

19th International Conference on Mining Software Repositories (MSR'22)

https://conf.researchr.org/home/msr-2022

Location: Pittsburgh, United States of America, 23 May 2022 – 24 May 2022.

Participating Members:

- Yves LE TRAON (Program Committee Member)

2022 ACM Conference on Conversational User Interfaces (CUI)

Location: Glasgow, United Kingdom, 26 Jul 2022 – 28 Jul 2022.

Participating Members:

- Mateusz DUBIEL (PC Member)

2022 ACM Conference on Human Factors in Computing Systems

Location: New Orleans, United States of America, 29 Apr 2022 – 5 May 2022.

Participating Members:

- Luis A. LEIVA (PC Member)
- Bereket Abera YILMA (Reviewer)
- Luis A. LEIVA (Associate Chair)

2022 ACM Conference on Intelligent User Interfaces (IUI)

Location: Helsinki, Finland, 22 Mar 2022 – 25 Mar 2022.

Participating Members:

- Luis A. LEIVA (SPC member, Associate Chair)

2022 ACM International Conference on Multimodal Interaction (ICMI)

Location: Bangalore, India, 7 Nov 2022 – 11 Nov 2022.

Participating Members:

- Luis A. LEIVA (PC Member)

2022 ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR)

Location: Madrid, Spain, 11 Jul 2022 – 15 Jul 2022.

Participating Members:

- Luis A. LEIVA (PC Member)
- Bereket Abera YILMA (Reviewer)

2022 Black in AI Workshop (BAI)

Location: New Orleans, United States of America, 15 Dec 2022 – 16 Dec 2022.

Participating Members:

- Bereket Abera YILMA (PC Member)

2022 European Conference on Object-Oriented Programming

 https://2022.ecoop.org/

Location: Berlin, Germany, 6 Jun 2022 – 10 Jun 2022.

Participating Members:

- Matthieu JIMENEZ (Technical Program Committee Member)

2022 Hybrid Human Artificial Intelligence (HHAI)

Location: Amsterdam, Netherlands, 13 Jun 2022 – 17 Jun 2022.

Participating Members:

- Luis A. LEIVA (PC Member)
- Bereket Abera YILMA (PC Member)

2022 IEEE Congress on Evolutionary Computation (CEC 2022)

☐ https://wcci2022.org

Location: Padova, Italy, 18 Jul 2022 – 23 Jul 2022.

Participating Members:

- Grégoire DANOY (Program Committee Member)

2022 Mensch und Computer (MuC)

Location: Darmstadt, Germany, 4 Sep 2022 – 7 Sep 2022.

Participating Members:

- Luis A. LEIVA (PC Member, Associate Chair)

2022 Workshop on Privacy in the Electronic Society (WPES)

☐ https://arc.encs.concordia.ca/wpes22/cfp.html

Location: Los Angeles, United States of America, 7 Nov 2022.

Participating Members:

- Sjouke MAUW (Program Committee Member)

20th Conference on Computational Methodsi n Systems Biology (CMSB)

☐ https://fmi.unibuc.ro/en/cmsb-2022/

Location: Bucharest, Romania, 14 Sep 2022 – 16 Sep 2022.

Participating Members:

• Jun PANG (Program Committee Member)

20th IEEE International Conference on Pervasive Intelligence and Computing (PiCOM 2022)

[⧉ http://cyber-science.org/2022/picom/](http://cyber-science.org/2022/picom/)

Location: Calabria, Italy, 12 Sep 2022 – 15 Sep 2022.

Participating Members:

• Grégoire DANOY (Program Committee Member)

21st IEEE International Conference on Trust Security and Privacy in Computing and Communications (TrustCom)

[⧉ http://www.ieee-hust-ncc.org/2022/TrustCom/](http://www.ieee-hust-ncc.org/2022/TrustCom/)

Location: Wuhan, China, 28 Oct 2022 – 30 Oct 2022.

Participating Members:

• Sjouke MAUW (Program Committee Member)

22nd IEEE International Working Conference on Source Code Analysis and Manipulation (SCAM 22)

[⧉ https://www.ieee-scam.org/2022/](https://www.ieee-scam.org/2022/)

Location: Limassol, Cyprus, 3 Oct 2022 – 4 Oct 2022.

Participating Members:

• Mike PAPADAKIS (Track / Working Group Chair)

23rd International Conference on Formal Engineering Methods (ICFEM)

 ⧉ http://maude.ucm.es/ICFEM22/

Location: Beijing, China, 24 Oct 2022 – 27 Oct 2022.

Participating Members:

• Jun PANG (Program Committee Member)

25th International Symposium On Real-Time Distributed Computing (ISORC 2022)

 ⧉ https://isorc2022.github.io/

Location: Västerås, Sweden, 17 May 2022 – 19 May 2022.

Description: **IEEE ISORC** was founded in 1998 (with its first meeting in Kyoto, Japan) to address research into the application of real-time object-oriented distributed technology. Since then, ISORC has continually evolved to meet the latest challenges faced by researchers and practitioners in the real-time domain, with an emphasis on object-, component- and service-oriented systems and solutions.

ISORC is a **single-track conference,** with a lively community. We have hosted a number of associated workshops, and are proud of our spirit of openness. We seek to encourage diverse views and new approaches to all Real-Time Issues and Challenges for novel applications and systems in RT computing issues.

Participating Members:

• Nicolas NAVET (Program Committee Member)

26th International Conference on Availability Reliablility and Security (ICECSS)

 ⧉ http://iceccs2022.xsrv.jp/

Location: Hiroshima, Japan, 26 Mar 2022 – 30 Mar 2022.

Participating Members:

• Jun PANG (Program Committee Member)

26th International Conference on Reliable Software Technologies (AEiC 2022)

⤤ https://www.ada-europe.org/conference2022/

Location: Ghent, Belgium, 14 Jun 2022 – 17 Jun 2022.

Description: The conference is an established international forum for providers, practitioners and researchers in reliable software technologies. The conference presentations will illustrate current work in the theory and practice of developing, running and maintaining challenging long-lived, high-quality software systems for a variety of application domains including manufacturing, robotics, avionics, space, health care, transportation, Cloud environments, smart energy, serious games. The program will allow ample time for keynotes, Q&A sessions and discussions, and social events. Participants include practitioners and researchers from industry, academia and government organizations active in the promotion and development of reliable software technologies.

The topics of interest for the conference include but are not limited to:

- *Real-Time and Safety-Critical Systems*
  – Design, implementation and verification challenges
  – Novel approaches, e.g., Mixed-Criticality Systems, novel scheduling algorithms, novel design and analysis methods
- *High-Integrity Systems and Reliability*
  – Theory and practice of High-Integrity Systems
  – Languages vulnerabilities and countermeasures
  – Architecture-centred development methods and tools
- *Reliability-oriented Programming Languages (not limited to Ada)*
  – Compilation and runtime challenges, language profiles
  – Use cases and experience reports
  – Language education and training initiatives
- *Experience Reports*
  – Case studies, lessons learned, and comparative assessments

Following the journal-first model inaugurated in 2019, the conference includes a journal-track that seeks original and high-quality submissions that describe mature research work in the scope of the conference.

Participating Members:

- Nicolas NAVET (Program Committee Member)

27th European Symposium on Research in Computer Security (ESORICS)

⤤ https://esorics2022.compute.dtu.dk/index.html#intro

Location: Copenhagen, Denmark, 26 Sep 2022 – 30 Sep 2022.

Participating Members:

• Sjouke MAUW (Program Committee Member)

27th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'2022)

⧉ https://2022.ieee-etfa.org/

Location: Stuttgart, Germany, 6 Sep 2022 – 9 Sep 2022.

Description: ETFA 2022 is the 27th Annual Conference of the IEEE Industrial Electronics Society (IES) focusing on the latest developments and new technologies in the field of industrial and factory automation. The conference aims to disseminate novel ideas and emerging trends, research results and practical achievements. ETFA 2022 will be held on September 6-9, 2022

ETFA 2022 is a unique opportunity to network, build up partnerships and exchange ideas with both industry leaders and a variety of experienced researchers, developers and practitioners from several industries, research institutes, and academia. Join the exciting ETFA 2022 technical and social activities. The ETFA 2022 Organizing Committee looks forward to welcoming you to this event.

Participating Members:

• Nicolas NAVET (Program Committee Member)

27th International Conference on Exploring Modeling Methods for Systems Analysis and Development (EMMSAD 2022)

⧉ https://www.emmsad.org/archive/2022

Location: Online, 6 Jun 2022 – 7 Jun 2022.

Description: The objective of the EMMSAD conference series is to provide a forum for researchers and practitioners interested in modelling methods for Systems Analysis and Development (SA&D) to meet and exchange research ideas and results. To this end, the focus is on both insights in modelling for SA&D in general, and the fostering of cross-pollination of insights between different specific modelling approaches (such as business process modelling, enterprise modelling, value modelling, capability modeling, etc.).

Participating Members:

• Qin MA (Program Committee Member)

28th International Workshop on Fast Software Encryption (FSE 2022)

Location: Athens, Greece, 25 Mar 2022 – 30 Mar 2022.

Participating Members:

- Aleksei UDOVENKO (Program Committee Member)
- Qingju WANG (Program Committee Member)

30th International Conference on Real-Time and Network Systems (RTNS'2022)

[⧉ https://rtns2022.inria.fr/](https://rtns2022.inria.fr/)

Location: Paris, France, 7 Jun 2022 – 8 Jun 2022.

Description: RTNS covers a wide-spectrum of topics in real-time and embedded systems, including, but not limited to:

- Real-time applications design and evaluation: automotive, avionics, space, railways, telecommunications, process control, multimedia.
- Real-time aspects of emerging smart systems: cyber-physical systems and emerging applications, real-time big data, real-time edge/fog and cloud computing, smart grid.
- Real-time system design and analysis: real-time tasks modeling, task/message scheduling, evaluation, mixed-criticality systems, Worst-Case Execution Time (WCET) analysis, quality of service, security.
- Software technologies for real-time systems: model-driven engineering, programming languages, compilers, WCET-aware compilation and parallelization strategies, middleware, Real-Time Operating Systems, virtualization, hypervisors.
- Formal specification and verification: application of formal models, such as model checking, satisfiability modulo theories or constraint programming, to solve real-time problems.
- Real-time distributed systems: fault tolerance, time synchronization, task/messages allocation, adaptability and reconfiguration, publisher/subscriber protocols, distributed real-time database.
- Real-time networks: Networks on Chip (NoC), wired and wireless sensor and actuator networks, Time-Sensitive Networks (TSN), industrial IoT, SDN, 5G, end-to-end latency analysis.
- Hardware support for real-time systems: hardware/software co-design, power/temperature-aware techniques, design of predictable hardware, multi-core and many-core platforms, hardware accelerators, cache related issues, interconnect and memory.

Participating Members:

- Nicolas NAVET (Program Committee Member)
- Tingting HU (Reviewer)

31st International Joint Conference on Artificial Intelligence (IJCAI 22)

[⧉ https://ijcai-22.org/](https://ijcai-22.org/)

Location: Vienna, Austria, 23 Jul 2022 – 29 Jul 2022.

Participating Members:

• Maxime CORDY (Program Committee Member)

33rd IEEE International Symposium on Software Reliability Engineering (ISSRE22)

 https://issre2022.github.io/

Location: Charlotte, United States of America, 31 Oct 2022 – 3 Nov 2022.

Participating Members:

• Mike PAPADAKIS (Program Committee Member)

34th IFIP International Conference on Testing Software and Systems (ICTSS 22)

Location: Almeria, Spain, 27 Sep 2022 – 29 Sep 2022.

Participating Members:

• Mike PAPADAKIS (Program Committee Member)

34th International Conference on Advanced Information Systems Engineering

Location: Leuven, Belgium, 6 Jun 2022 – 10 Jun 2022.

Participating Members:

• Maxime CORDY (PC Member)

35th IEEE Computer Security Foundations Symposium (CSF)

 https://www.ieee-security.org/TC/CSF2022/

Location: Haifa, Israel, 7 Aug 2022 – 10 Aug 2022.

Participating Members:

• Sjouke MAUW (Program Committee Member)

36th AAAI conference on Artificial Intelligence

  https://aaai.org/Conferences/AAAI-22/

Location: Online, 22 Feb 2022 – 1 Mar 2022.

Participating Members:

- Maxime CORDY (Program Committee Member)
- Yves LE TRAON (Program Committee Member)

36th AAAI Conference on Artificial Intelligence

  https://aaai.org/conference/aaai/aaai-22/

Location: Vancouver, Canada, 22 Feb 2022 – 1 Mar 2022.

Participating Members:

- Jun PANG (Program Committee Member)

36th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec)

  http://cs.iit.edu/~dbsec2022/

Location: Newark, NJ, United States of America, 18 Jul 2022 – 20 Jul 2022.

Participating Members:

- Sjouke MAUW (Program Committee Member)

36th IEEE International Parallel and Distributed Processing Symposium: IPDPS 2022 Workshop

  https://www.ipdps.org/ipdps2022/

Location: Lyon, Online, France, 30 May 2022 – 3 Jun 2022.

Participating Members:

• Daniel STOLFI ROSSO (Program Committee Member)

37th IEEE/ACM International Conference on Automated Software Engineering (ASE22)

⌐ https://conf.researchr.org/home/ase-2022

Location: Ann Arbor, United States of America, 10 Oct 2022 – 14 Oct 2022.

Participating Members:

• Yves LE TRAON (Program Committee Member)
• Mike PAPADAKIS (Program Committee Member)

38th IEEE International Conference on Software Maintenance and Evolution (ICSME 22)

⌐ https://cyprusconferences.org/icsme2022/

Location: Limassol, Cyprus, 3 Oct 2022 – 7 Oct 2022.

Participating Members:

• Mike PAPADAKIS (Track / Working Group Chair, Steering Committee Member, Program Committee Member)

3rd ACM/IEEE International Conference on Automation of Software Test (AST 22)

⌐ https://conf.researchr.org/home/ast-2022

Location: Online, 17 May 2022 – 18 May 2022.

Participating Members:

• Yves LE TRAON (Program Committee Member)

3rd IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS 2022)

Location: Los Angeles, CA, United States of America, 19 Sep 2022 – 23 Sep 2022.

Participating Members:

• Jean BOTEV (Steering Committee Member, Program Committee Member)

3rd Workshop on Secure Cryptographic Implementation (SCI 2022)

Location: Rome, Italy, 23 Jun 2022.

Participating Members:

• Johann GROSZSCHÄDL (Program Committee Member)

41st Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2022)

Location: Olso, Norway, 30 May 2022 – 3 Jun 2022.

Participating Members:

• Alexei BIRYUKOV (Program Committee Member)

43rd ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2022)

 https://pldi22.sigplan.org/

Location: San Diego, United States of America, 13 Jun 2022 – 17 Jun 2022.

Participating Members:

• Maxime CORDY (Artefact track Porgram Committee member)

43rd IEEE Real-Time Systems Symposium (RTSS 2022)

 http://2022.rtss.org/

Location: Houston, United States of America, 5 Dec 2022 – 8 Dec 2022.

Description:

RTSS 2022

The IEEE Real-Time Systems Symposium (RTSS) is the premier conference in the field of real-time systems and is a venue for researchers and practitioners to showcase innovations covering all aspects of real-time systems, including theory, design, analysis, implementation, evaluation, and experience. RTSS '22, celebrating the 43rd anniversary of the event,

continues the trend of making RTSS an expansive and inclusive event, striving to embrace new and emerging areas of real-time systems research.

Participating Members:

• Tingting HU (Program Committee Member)

44th International Conference in Software Engineering (ICSE 22)

 https://conf.researchr.org/home/icse-2022

Location: Pittsburgh, United States of America, 22 May 2022 – 27 May 2022.

Participating Members:

• Yves LE TRAON (Program Committee Member)

4th Workshop on Artificial Intelligence and Model-driven Engineering (MDE Intelligence)

Location: Montreal, Canada, 23 Oct 2022.

Participating Members:

• Benoit RIES (Program Committee Member)

5th IEEE Conference on Dependable and Secure Computing (IEEE DSC)

 https://attend.ieee.org/dsc-2022/

Location: Edinburgh, United Kingdom, 22 Jun 2022 – 24 Jun 2022.

Participating Members:

• Sjouke MAUW (Program Committee Member)

6th International Symposium on Cyber Security Cryptology and Machine Learning (CSCML 2022)

Location: Be'er Sheva, Israel, 30 Jun 2022 – 2 Jul 2022.

Participating Members:

• Alexei BIRYUKOV (Program Committee Member)

6th International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2022)

Location: Copenhagen, Denmark, 29 Sep 2022 – 30 Sep 2022.

Participating Members:

• Alexei BIRYUKOV (Program Committee Member)

7th Workshop on "Critical Automotive applications: Robustness & Safety" (CARS)

https://conf.laas.fr/cars/cars2022.html

Location: Zaragoza, Spain, 15 Sep 2022.

Description: The CARS workshop is a forum focusing on architecture, methods and development techniques for safety-related automotive embedded systems and applications. The 7th edition of CARS is collocated with the 18th European Dependable Computing Conference.

Participating Members:

• Nicolas NAVET (Program Committee Member)

8th IEEE Latin American Conference on Computational Intelligence: IEEE LA-CCI 2022

https://la-cci.org/

Location: Montevideo, Uruguay, 23 Nov 2022 – 25 Nov 2022.

Description: The IEEE Latin American Conference on Computational Intelligence 2022 aims to (1) bring together the Soft Computing community to present the latest achievements and innovations in the multiple areas of Computational Intelligence; (2) to encourage participation by young researchers and, according to the LA-CCI Manifesto, (3) to provide a high-level international forum for scientists, researchers, engineers, professionals and educators to disseminate their research results and exchange views of the future directions for the area of Computational Intelligence

Participating Members:

• Daniel STOLFI ROSSO (Program Committee Member)

8th International Symposium on Dependable Software Engineering Theories and Tools and Applications (SETTA)

⧉ http://lcs.ios.ac.cn/setta2022/index.html

Location: Madrid, Spain, 27 Oct 2022 – 29 Oct 2022.

Participating Members:

• Jun PANG (Program Committee Member)

9th International Conference on Future Internet of Things and Cloud (FiCloud 2022)

⧉ http://www.ficloud.org/2022/

Location: Rome, Italy, 22 Aug 2022 – 24 Aug 2022.

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

Participating Members:

• Qin MA (Program Committee Member)

AAMAS: International Conference on Autonomous Agents and Multiagent Systems

Location: Auckland, 9 May 2022 – 13 May 2022.

Participating Members:

• Leon VAN DER TORRE (PC Member)

ACM Conference on Computer and Communication Security,ACM CCS 2022

⧉ https://www.sigsac.org/ccs/CCS2022/

Location: Los Angeles, United States of America, 7 Nov 2022 – 11 Nov 2022.

Description: The ACM Conference on Computer and Communications Security (CCS) is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM). The conference brings together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results.

Participating Members:

• Andy RUPP (Technical Program Committee Member)

ACM / ESSE 2022: 2022 The 3rd European Symposium on Software Engineering

Location: Rome, Italy, 27 Oct 2022 – 29 Oct 2022.

Participating Members:

• Nicolas GUELFI (Program Committee Member)

AICOL 2022: XIV Workshop on Artificial Intelligence and the Complexity of Legal Systems

Location: Saarbrücken, 14 Dec 2022.

Participating Members:

• Réka MARKOVICH (PC Member)

AIFA 2022 - Artificial Intelligence and the Future of Art

  https://aifa.uni.lu

Location: Belval & Online, Luxembourg, 28 Nov 2022 – 30 Mar 2022.

Participating Members:

• Sana NOUZRI (Organising Committee)
• Leon VAN DER TORRE (General Chair)
• Christian FRANCK (Reviewer)

ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES

Location: Online, United States of America, 4 Jan 2022 – 7 Jan 2022.

Participating Members:

• Benoit RIES (Reviewer)

ArgMining 2022: 9th Workshop on Argument Mining

 https://argmining-org.github.io/2022/

Location: Gyeongju & Online, South Korea, 17 Oct 2022.

Participating Members:

• Davide LIGA (Program Committee Member)

BNAIC/BeNeLearn 2022: Joint International Scientific Conferences on AI and Machine Learning

Location: Lamot Mechelen, 7 Nov 2022 – 9 Nov 2022.

Participating Members:

• Leon VAN DER TORRE (PC Member)

BNAIC/BeNeLearn 2022: Joint International Scientific Conferences on AI and Machine Learning

 https://bnaic2022.uantwerpen.be

Location: Lamot Mechelen, Belgium, 7 Nov 2022 – 9 Nov 2022.

Participating Members:

• Grégoire DANOY (Program Committee Member)

CAST IT-Security Award 2022

 https://cast-forum.de/en/award/award.html?ts=1679924652141

Location: Wiesbaden, Germany, 11 Oct 2022.

Description:

CAST Förderpreis IT-Sicherheit 2022 verliehen

Darmstadt 11.10.2022

Gestern wurde in Wiesbaden zum 22. Mal der CAST-Förderpreis IT-Sicherheit verliehen.

Gutachter:innen des CAST e.V. hatten im Vorfeld alle Einreichungen gesichtet und deren Qualität bewertet. Auf dieser Basis wurden insgesamt 6 Autor:innen für den Finalisten-Workshop nominiert, der dieses Jahr im Rahmen des Cybersicherheitsgipfel Hessen stattfand. Herr Malte Kuckel vom Hessischen Ministerium des Innern und für Sport hielt die diesjährige Laudatio für die Preisträger:innen.

Die Finalist:innen waren geladen (hier das Programm), die Ergebnisse ihrer Arbeit der interessierten Öffentlichkeit vorzustellen. Teilnehmer:innen erhielten hier Gelegenheit die Innovation der einzelnen Arbeiten zu hinterfragen und sich von der Qualität der Beiträge zu überzeugen. Im Anschluss hat eine Jury aus Vertretern der Wirtschaft und Forschung die Preisträger:innen ermittelt.

In der Kategorie Masterarbeiten setzte sich Herr **Simon Nachtigall** von der Universität Paderborn mit seiner Arbeit *Evaluation of TLS session tickets* durch.

Unter den Bachelorarbeiten gewann Herr **Nico Heitmann** (ebenfalls Universität Paderborn) mit seiner Arbeit *Security Analysis of the Web Conferencing System BigBlueButton*.

Alle Finalist:innen gewinnen die kostenlose Teilnahme an den CAST-Workshops 2023. Darüber hinaus sind mit dem CAST-Förderpreis Preisgelder in Höhe von insgesamt 3.600,- verbunden.

Die Preisträger:innen in der Übersicht.

Kategorie **Masterarbeiten**

1. Platz: Simon Nachtigall (Universität Paderborn): *Evaluation of TLS session tickets*

2. Platz: Johanna Henrich (Hochschule Darmstadt): *Performanz Evaluation von PQC in TLS 1.3 unter variierenden Netzwerkcharakteristiken*

3. Platz: Felix Clemens Gail (TU Darmstadt / Fraunhofer SIT): *Intrusion Detection for SOME/IP through Machine Learning and Rule Generation*

Kategorie **Bachelorarbeiten**

1. Platz: Nico Heitmann (Universität Paderborn): *Security Analysis of the Web Conferencing System BigBlueButton*

2. Platz: Lorenz Hetterich (Universität des Saarlandes / Helmholtz Center for Information Security (CISPA)): *Exploiting Spectre on iOS*

3. Platz: Leon Michael Trampert (Universität des Saarlandes / Helmholtz Center for Information Security (CISPA)): *Browser-based CPU Fingerprinting*

Participating Members:

• Andy RUPP (Jury Member)

COMMA 2022: 9th International Conference on Computational Models of Argument

[QR] https://comma22.cs.cf.ac.uk

Location: Cardiff, United Kingdom, 14 Sep 2022 – 16 Sep 2022.

Participating Members:

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

EUMAS 2022: The 19th European Conference on Multi-Agent Systems

Location: Düsseldorf, 14 Sep 2022 – 16 Sep 2022.

Participating Members:

- Leon VAN DER TORRE (PC Member)

European Conference on Computer Vision (ECCV22)

[QR] https://eccv2022.ecva.net/

Location: Tel Aviv, Israel, 23 Oct 2022 – 27 Oct 2022.

Participating Members:

- Maxime CORDY (Program Committee Member)

European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE22)

[QR] https://2022.esec-fse.org/

Location: Singapore, Singapore, 14 Nov 2022 – 18 Nov 2022.

Participating Members:

- Maxime CORDY (Program Committee Member)
- Mike PAPADAKIS (Program Committee Member)

EuroSys 2022

☑ https://2022.eurosys.org/

Location: Rennes, France, 5 Apr 2022 – 8 Apr 2022.

Participating Members:

• Yves LE TRAON (Program Committee Member)

EXTRAAMAS 2022: EXplainable and TRAnsparent AI and Multi-Agent Systems

Location: Online, 9 May 2022 – 10 May 2023.

Participating Members:

• Réka MARKOVICH (Track Chair)

FNR Researchers Days 2022

☑ https://researchersdays.science.lu/en

Location: Belval, Luxembourg, 25 Nov 2022 – 26 Nov 2022.

Description: Organisation of a Science Workshop entitled "INTELLIGENT ROBOTS ON A MISSION!" as part of the FNR Researchers' Days 2022.

Participating Members:

• Grégoire DANOY (Exhibitor)
• Pierre-Yves HOUITTE (Exhibitor)
• Daniel STOLFI ROSSO (Exhibitor)

Global Communications Conference 2022

☑ https://www.comsoc.org/conferences-events/ieee-global-communicatio
ns-conference-2022

Location: Rio de Janeiro-RJ, Brazil, 4 Dec 2022 – 8 Dec 2022.

Description: IEEE GLOBECOM 2022 - IEEE Global Communications Conference (GLOBECOM) is one of the IEEE Communications Society's two flagship conferences dedicated to driving innovation in nearly every aspect of communications.

Participating Members:

• Abdelwahab BOUALOUACHE (Technical Program Committee Member)

IEEE Future Networks World Forum

 https://www.computer.org/cfp/fnwf-2022

Location: Montreal, Canada, 12 Oct 2022 – 14 Oct 2022.

Description: The 2022 IEEE 5th Future Networks World Forum (FNWF'22) — formerly the 5G World Forum — seeks contributions on how to nurture and cultivate future network technologies and applications through 5G and beyond for the betterment of society.

This will be an in-person event in Montreal, Canada, but authors of accepted conference papers may opt to present remotely.

5G systems have started to deliver a novel mobile network architecture that not only improves physical data rate, but also creates a new ecosystem allowing the deployment of novel services and applications. A key target for future networks will be to improve support not only for classical mobile broadband applications and services but also for vertical industry (e.g. Intelligent Transport, Industrial IoTs, eHealth, etc.) and other mobility-based services.

This conference, called the 5G World Forum in its first four years, aims to bring experts from industry, academia and research to exchange their visions as well as their achieved advances in 5G and towards 6G, and encourage innovative cross-domain studies, research, early deployment and large-scale pilot showcases that address the challenges of 5G while identifying and investigating the possibilities of future networks.

Participating Members:

• Abdelwahab BOUALOUACHE (Technical Program Committee Member)

IEEE International Conference on Software Security and Reliability (QRS22)

 https://qrs22.techconf.org/

Location: Guangzhou, China, 5 Dec 2022 – 9 Dec 2022.

Participating Members:

• Mike PAPADAKIS (Program Committee Member)

IEE International Mediterranean Conference 2022

⌕ https://meditcom2022.ieee-meditcom.org/

Location: Athens, Greece, 5 Sep 2022 – 8 Sep 2022.

Description: IEEE MeditCom will bring together visionaries in academia, research labs and industry from all over the world to the shores of the Mediterranean Sea, with programming that will address many of the outstanding challenges that exist in the areas of communications and networking. The conference will solicit research papers on a wide range of research topics, spanning both theoretical and systems research along with vertical technologies. Known as the "cradle of Western civilization", IEEE MeditCom participants will also have an opportunity to explore this exciting and dynamic region with its rich history and beauty.

IEEE Communications Society aims at engaging local IEEE Sections, ComSoc Chapters, and possibly Sister Societies, from all Mediterranean region, including Spain, France, Monaco, Italy, Slovenia, Croatia, Bosnia and Herzegovina, Montenegro, Albania, Greece, Turkey, Syria, Lebanon, Israel, Egypt, Libya, Tunisia, Algeria, Morocco, Malta, and Cyprus.

Participating Members:

• Abdelwahab BOUALOUACHE (Technical Program Committee Member)

IHAD2022 - I HAVE A DREAM CONFERENCE 2022

⌕ https://aifa.uni.lu/ihad/

Location: Belval & Online, Luxembourg, 1 Dec 2022 – 2 Dec 2022.

Participating Members:

• Igor TCHAPPI HAMAN (Programme Chair)

International Conference on AI Engineering – Software Engineering for AI (CAIN 22)

Location: Online, 16 May 2022 – 17 May 2022.

Participating Members:

• Mike PAPADAKIS (Program Committee Member)

International Conference on Communications 2022

 ☐ https://icc2022.ieee-icc.org/

Location: Seoul, South Korea, 12 May 2022 – 20 May 2022.

Description: We are very happy to welcome you all in Seoul, Korea and are confident that the situation is improving regarding the on-going COVID-19 pandemic. From July 1, 2021, people vaccinated abroad will no longer be required to lock themselves up for two full weeks. Nevertheless, in view of the possible travel restrictions, the conference will be in the form of a hybrid conference with as many authors and

Participating Members:

• Abdelwahab BOUALOUACHE (Technical Program Committee Member)

International Conference on the Applications of Evolutionary Computation (EvoApps 2022)

 ☐ https://www.evostar.org/2022/evoapps/

Location: Madrid, Spain, 20 Apr 2022 – 22 Apr 2022.

Participating Members:

• Grégoire DANOY (Program Committee Member)

JURIX 2022

 ☐ https://jurix2022.rechtsinformatik.saarland/

Location: Saarbrücken, Germany, 14 Dec 2022 – 16 Dec 2022.

Participating Members:

• Réka MARKOVICH (Program Committee Member)
• Leon VAN DER TORRE (PC Member)

KR 2022: 19th International Conference on Principles of Knowledge Representation and Reasoning

Location: Haifa, 31 Jul 2022 – 5 Aug 2022.

Participating Members:

• Leon VAN DER TORRE (PC Member)

LateRAISSe 2022: 1st Workshop on Language Technology and Resources for a Fair Inclusive and Safe Society

Location: Marseille, France, 5 Jun 2022.

Participating Members:

• Réka MARKOVICH (PC Member)

Lifelike Computing Systems Workshop (LIFELIKE 2022)

Location: Trento, Italy, 19 Jul 2022 – 23 Jul 2022.

Participating Members:

• Jean BOTEV (Co-Chair)

LNGAI 2022: Second International Workshop on Logics for New-Generation Artificial Intelligence

Location: Zhuhai, China, 10 Jun 2022 – 12 Jun 2022.

Participating Members:

• Réka MARKOVICH (PC Chair)
• Leon VAN DER TORRE (PC Member)

Mutation 2022

 https://icst2022.vrain.upv.es/home/mutation-2022

Location: Online, 4 Apr 2022 – 8 Apr 2022.

Description: Colocated with ICST

Participating Members:

• Mike PAPADAKIS (Program Committee Member)

NMR 2022: 20th International Workshop on Non-Monotonic Reasoning

 https://sites.google.com/view/nmr2022/

Location: Haifa, Israel, 7 Aug 2022 – 9 Aug 2022.

Participating Members:

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

PRIMA22: The 24th International Conference on Principles and Practice of Multi-Agent Systems

Location: Valencia, 16 Nov 2022 – 18 Nov 2022.

Participating Members:

- Leon VAN DER TORRE (PC Member)

Privacy Enhancing Technologies,PETS 2022

 https://petsymposium.org/2022/

Location: Sydney, Australia, 11 Jul 2022 – 15 Jul 2022.

Description:

PETS 2022

The 22nd Privacy Enhancing Technologies Symposium
July 11–15, 2022
Sydney, Australia and Online

The annual Privacy Enhancing Technologies Symposium (PETS) brings together privacy experts from around the world to discuss recent advances and new perspectives on research in privacy technologies. PETS addresses the design and realization of privacy services for the Internet and other digital systems and communication networks.

Participating Members:

- Andy RUPP (Program Committee Member)

SEENG 2022 - the 4th International Workshop on Software Engineering Education for the Next Generation - Track @ ACM IEEE ICSE

Location: Pittsburg, United States of America, 22 May 2022 – 27 May 2022.

Participating Members:

- Nicolas GUELFI (Program Committee Member)

SEET 2022 - Software Engineering Education and Training - Track @ ACM IEEE ICSE - 44th International Conference on Software Engineering

Location: Pittsburg, United States of America, 22 May 2022 – 27 May 2022.

Participating Members:

• Nicolas GUELFI (Program Committee Member)

Symposium on Search-Based Software Engineering (SSBSE 22)

 https://conf.researchr.org/home/ssbse-2022

Location: Singapore, Singapore, 17 Nov 2022 – 18 Nov 2022.

Participating Members:

• Mike PAPADAKIS (Track / Working Group Chair, Steering Committee Member, Program Committee Member)

THE 26TH PACIFIC-ASIA CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING

 http://www.pakdd.net

Location: Chengdu (Hybrid Event), China, 16 May 2022 – 19 May 2022.

Participating Members:

• Alessandro TEMPERONI (Paper presentation)

The 37th ACM/SIGAPP Symposium On Applied Computing (SAC 2022)

Location: Online, 25 Apr 2022 – 29 Apr 2022.

Participating Members:

• Mike PAPADAKIS (Program Committee Member)

The Genetic and Evolutionary Computation Conference (GECCO 2022)

 https://gecco-2022.sigevo.org/

Location: Boston, United States of America, 9 Jul 2022 – 13 Jul 2022.

Description: The Genetic and Evolutionary Computation Conference (GECCO) presents the latest high-quality results in genetic and evolutionary computation since 1999. Topics include: genetic algorithms, genetic programming, ant colony optimization and swarm intelligence, complex systems (artificial life, robotics, evolvable hardware, generative and developmental systems, artificial immune systems), digital entertainment technologies and arts, evolutionary combinatorial optimization and metaheuristics, evolutionary machine learning, evolutionary multiobjective optimization, evolutionary numerical optimization, real world applications, search-based software engineering, theory and more.

Participating Members:

- Grégoire DANOY (Program Committee Member)
- Daniel STOLFI ROSSO (Program Committee Member)

The WebConf

https://www2022.thewebconf.org/

Location: Lyon, France, 25 Apr 2022 – 29 Apr 2022.

Participating Members:

- Jun PANG (Program Committee Member)

Thirty-sixth Conference on Neural Information Processing Systems (NEURIPS22)

https://neurips.cc/

Location: New Orleans, United States of America, 28 Nov 2022 – 1 Dec 2022.

Participating Members:

- Maxime CORDY (Program Committee Member)
- Yves LE TRAON (Area chair)

V Ibero-American Congress of Smart Cities - ICSC-CITIES 2022

http://2022.icsc-cities.com/index.html

Location: Cuenca, Ecuador, 28 Nov 2022 – 30 Nov 2022.

Participating Members:

• Daniel STOLFI ROSSO (Program Committee Member)

WOA 2022: The 23rd Workshop 'From Objects to Agents'

Location: Genova, 1 Sep 2022 – 3 Sep 2022.

Participating Members:

• Leon VAN DER TORRE (PC Member)

WOLLIC 2022: 28th Workshop on Logic Language and Computation

Location: Iasi, Romania, 20 Sep 2022 – 23 Sep 2022.

Participating Members:

• Leon VAN DER TORRE (PC Member)

C.2 Doctoral Thesis Defense Committee Memberships

Ilaria Angela Amatea, Università di Bologna

Date: 16 Jun 2022
Location: Blogna, Italy

PhD Defense Jury Members:

• Sjouke MAUW (Member)

Jim Barthel, University of Luxembourg

Date: 2 Sep 2022
Location: Belval, Luxembourg

PhD Defense Jury Members:

• Franck LEPREVOST (Chairman)

PhD Defense Jury External Partners:

• Wouter Castryck (Examiner)
• Nico Döttling (Examiner)

Paul-Lou Benedick, University of Luxembourg

Date: 27 Apr 2022
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

• Nicolas NAVET (Chairman)

Luan Cardoso dos Santos, University of Luxembourg

Date: 24 Jun 2022
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

• Jean-Sébastien CORON (Chairman)
• Volker MÜLLER (Vice-chairman)
• Alexei BIRYUKOV (Supervisor)

PhD Defense Jury External Partners:

• Maria Eichlseder (Member)
• Diego F. Aranha (Member)

Christian Cintrano López, University of Malaga

Date: 27 May 2022
Location: Malaga, Spain

PhD Defense Jury Members:

• Grégoire DANOY (Examiner)

PhD Defense Jury External Partners:

• Michael Affenzeller (External Reviewer)
• Enrique Alba (Supervisor)
• José-Francisco Chicano Garcia (Co-supervisor)
• Gabriel Luque (Chairman)
• Andrea VILLAGRA (External Reviewer)

Christof Ferreira Torres, University of Luxembourg

Date: 6 May 2022
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

• Sjouke MAUW (Chairman)

Salah Ghamizi, University of Luxembourg

Date: 7 Sep 2022
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

• Mike PAPADAKIS (Chairman)
• Maxime CORDY (Vice-chairman)
• Yves LE TRAON (Supervisor)

PhD Defense Jury External Partners:

- Jean-Philippe Thiran (Examiner)
- Jingfeng Zhang (Examiner)

Shohreh Haddadan, University of Luxembourg

Date: 4 Apr 2022
Location: Belval, Luxembourg

PhD Defense Jury Members:

- Leon VAN DER TORRE (Supervisor)

Benjamin Jahic, University of Luxembourg

Date: 5 Apr 2022
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Benoit RIES (Vice-chairman)
- Nicolas GUELFI (Supervisor)

PhD Defense Jury External Partners:

- Leonardo da Silva Sousa (Member)
- Giovanna Di Marzo (Member)

Roy Jamil, École Nationale Supérieure de Mécanique et d'Aérotechnique (ENSMA)

Date: 4 Mar 2022
Location: Poitiers, France

PhD Defense Jury Members:

- Nicolas NAVET (Chairman)

Davide Liga, University of Bologna

Date: 16 Jun 2022
Location: Bologna, Italy

PhD Defense Jury Members:

- Leon VAN DER TORRE (Supervisor)

Philippe Ludivig, University of Luxembourg

Date: 14 Mar 2022
Location: Belval, Luxembourg

PhD Defense Jury Members:

• Leon VAN DER TORRE (Vice-chairman)

Tieu Long MAI, University of Luxembourg

Date: 23 Feb 2022
Location: Belva, Luxembourg

PhD Defense Jury Members:

• Tingting HU (Member)

Alfonso Mascarenas Gonzalez, l'Institut Supérieur de l'Aéronautique et de l'Espace (ISAE)

Date: 21 Dec 2022
Location: Toulouse, France

PhD Defense Jury Members:

• Nicolas NAVET (Examiner)

Victor-Bogdan Popescu, University of Turku

Date: 3 Jun 2022
Location: Turku, Finland

PhD Defense Jury Members:

• Jun PANG (External Reviewer)

Abiodun Abdullahi Solanke, Università di Bologna

Date: 17 Jun 2022
Location: Blogna, Italy

PhD Defense Jury Members:

• Sjouke MAUW (Member)

Giuseppe Vitto, University of Luxembourg

Date: 26 Jan 2022
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

• Jean-Sébastien CORON (Chairman)
• Volker MÜLLER (Vice-chairman)
• Alexei BIRYUKOV (Supervisor)

PhD Defense Jury External Partners:

• Nadia Heninger (Member)
• Frederik Vercauteren (Member)

Aoran Wang, University of Luxembourg

Date: 12 Oct 2022
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

• Pierre KELSEN (Member)

Zhiqiang Zhong, University of Luxembourg

Date: 4 Apr 2022
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

• Sjouke MAUW (Chairman)
• Martin THEOBALD (Vice-chairman)
• Jun PANG (Supervisor)

PhD Defense Jury External Partners:

• Cheng-Te LI (Member)
• Davide MOTTIN (Member)

C.3   Awards

Best Dissertation Award Runner Up from iSchools 2022, 28 Feb 2022
Recipient: Mateusz DUBIEL

Best Paper Honorable Mention Award at EICS'22, 21 Jun 2022
Recipient: Luis A. LEIVA
Klen Čopič Pucihar, Nuwan T. Attygalle, Matjaz Kljun, Christian Sandor, Luis A. Leiva. Solids on Soli: Millimetre-Wave Radar Sensing through Materials. In Proc. ACM SIGCHI Symposium on Engineering Interactive Computing Systems (EICS).

Excellent Doctoral Thesis Award 2022, 28 Oct 2022
Recipient: Giuseppe VITTO

Excellent Thesis Award 2022, 28 Nov 2022
Recipient: Salah GHAMIZI
Excellent thesis award from the University of Luxembourg

Honorary "Bao Yugang Chair Professor" at Zhejiang University, 22 Apr 2022
Recipient: Leon VAN DER TORRE

Reviewer Recognition at ICMI'22, 7 Nov 2022
Recipient: Luis A. LEIVA

Reviewer Recognition at IUI'22, 21 Mar 2022
Recipient: Luis A. LEIVA

Teaching Award 2022, 12 Oct 2022
Recipient: Volker MÜLLER

C.4 Media Appearances

Your Mouse Reveals your Gender and Age (dataskeptic.com)

https://dataskeptic.com/blog/episodes/2022/your-mouse-reveals-your-gender-and-age

Interview (Radio), 28 Nov 2022
Members: Luis A. LEIVA
Luis Leiva is a Professor of Computer Science at the University of Luxembourg. His research lies in an intersection of human computer interaction and machine learning. Today, he talks to us about his recent work on behavioural profiling via mouse tracking.

Researchers' Days 2022 (SnT News)

https://wwwen.uni.lu/snt/news_events/researchers_days_2022

News (Internet), 24 Nov 2022
Members: Grégoire DANOY, Pierre-Yves HOUITTE, Daniel STOLFI ROSSO
[Extract]

Now a key event for research in Luxembourg, Researchers' Days offers scientists a unique platform to present their work to a wide audience. Visitors can get hands-on, experiment, ask questions and get a very concrete and personal insight into the world of research.
A day dedicated exclusively to high schools.
Researchers' Days arouse great interest and enthusiasm among children and young people - the scientists of tomorrow! That is why the first day is reserved exclusively for secondary school students. This gives them a direct insight into research in Luxembourg, introduces

them to the various research institutes, and allows them to ask scientists questions about their work and their daily professional lives.

See below what SnT has in store for you at the event.

Intelligent Robots in mission!

Would you be able to accomplish a mission with intelligent robots in three minutes? Take control of the robots and see how they 'react' as a group. They are autonomous, perceive their environment thanks to different motion captures, and take their own decisions to lead their mission. Join Grégoire Danoy in this experience!

EU debuts on Mastodon, Twitter exodus fits policy goals (Luxtimes)

https://www.luxtimes.lu/en/european-union/eu-debuts-on-mastodon-twitter-exodus-fits-policy-goals-6374b5e6de135b92369e39b5

Interview (Newspaper), 22 Nov 2022
Members: Luis A. LEIVA

Retour sur la Journée Mondiale de la Normalisation 2022 au Grand-Duché de Luxembourg (ILNAS)

https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2022/journee-mondiale-normalisation-2022-grand-duche-luxembourg.html

Article (Internet), 17 Oct 2022
Members: Manuel COMBARRO SIMON, Grégoire DANOY, Hedieh HADDAD

Die KI-Aktivistin (Revue)

Interview (Magazine), 28 Sep 2022 , p. 46-47
Members: Sahar NIKNAM

EIC Pathfinder grant for research in AI-driven data visualisation (uni.lu)

https://wwwen.uni.lu/university/news/latest_news/eic_pathfinder_grant_for_research_in_ai_driven_data_visualisation

Blog (Internet), 21 Sep 2022
Members: Luis A. LEIVA
A team of researchers from the University of Luxembourg, AEGIS IT Research GmbH (Germany), Université catholique de Louvain (Belgium), and Telefónica I+D (Spain) has received

an EIC Pathfinder Challenge grant of 4 million euros for their research in AI-driven data visualisation systems. This is the first EIC Pathfinder grant that is coordinated by the University of Luxembourg.

Spresso: Historical newspaper photography goes supercomputing (uni.lu)

[☍ https://wwwen.uni.lu/universite/actualites/diaporama/spresso_les_phot os_de_presse_historiques_passent_au_supercalculateur](https://wwwen.uni.lu/universite/actualites/diaporama/spresso_les_photos_de_presse_historiques_passent_au_supercalculateur)

Blog (Internet), 12 Sep 2022
Members: Luis A. LEIVA
While supercomputers are traditionally being used in physics, material science and advanced chemistry, the Spresso project entails the very first formal cooperation between the Luxembourgish supercomputer MeluXina, the Bibliothèque nationale du Luxembourg and an interdisciplinary team of researchers of the Centre for Contemporary and Digital History (C^{2}DH) and the Department of Computer Science of the University of Luxembourg, to explore the automatic enhancement of 20th century historical newspaper photography at a large scale through deep learning algorithms.

De belles perspectives pour l'équipe du programme de recherche « Technical Standardisation for Trustworthy ICT, Aerospace, and Construction » (2021-2024) (ILNAS Website)

[☍ https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2022/ belles-perspectives-pour-equipe-programme-recherche-technical-standard isation-for-trustworthy-ict-aerospace-construction-2021-](https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2022/belles-perspectives-pour-equipe-programme-recherche-technical-standardisation-for-trustworthy-ict-aerospace-construction-2021-)

Article (Internet), 5 Jul 2022
Members: Pascal BOUVRY, Manuel COMBARRO SIMON, Grégoire DANOY, Hedieh HADDAD

3Mol1Fro (about AI & Arts exposition at UL) (RTL Radio)

Interview (Radio), 23 Jun 2022
Members: Christian FRANCK

ILNAS – Université du Luxembourg/SnT | Workshop "Space & Technical Standardization" (ILNAS)

[☍ https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2022/ invitation-ilnas-universite-luxembourg-snt-workshop-space-and-technical- standardization.html](https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2022/invitation-ilnas-universite-luxembourg-snt-workshop-space-and-technical-standardization.html)

Article (Internet), 20 May 2022
Members: Pascal BOUVRY, Grégoire DANOY

SnT Researchers Participate in the 2022 Chercheurs à l'École Series (SnT Website)

⌖ https://wwwen.uni.lu/snt/news_events/snt_researchers_participate_in_
the_2022_chercheurs_a_l_ecole_series

News (Internet), 22 Apr 2022
Members: Grégoire DANOY
Each year, researchers from across Luxembourg venture back into the classroom to inspire a new generation of future scientists. Chercheurs à l'École, an initiative that was started by the Fonds National de Recherche 12 years ago in 2010, took place during the 14 – 18 March this year, and saw many researchers discuss their work with teenagers from schools across Luxembourg. From the University of Luxembourg's Interdisciplinary Centre for Security, Reliability and Trust, Dr. Grégoire Danoy visited the Lycée Nic-Biever in Dudelange to speak to over 100 teenagers between the age of 15 and 18.

Mausbewegungen verroden Äert Verhalen (radio 100,7)

Interview (Radio), 1 Mar 2022
Members: Luis A. LEIVA

8 chercheurs pleins d'avenir (Paperjam)

Interview (Magazine), 7 Feb 2022 , p. 95-96
Members: Jim Jean-Pierre BARTHEL

Was Mausbewegungen über den Anwender verraten und wie man das verhindern kann (science.lu)

⌖ https://www.science.lu/de/computersicherheit/was-mausbewegungen-
ueber-den-anwender-verraten-und-wie-man-das-verhindern-kann

Interview (Internet), 22 Jan 2022
Members: Luis A. LEIVA
Nicht nur die im Netz angeklickten Inhalte lassen Rückschlüsse auf den Nutzer zu, sondern bereits die Bewegungen der Computermaus. Das ist datenschutzrechtlich kritisch, lässt sich aber auch umgehen.

Luis Leiva veranschaulicht es an einem ganz einfachen Beispiel: "Nehmen wir an, wir suchen bei Google nach dem Alter eines Schauspielers und bekommen dann die Trefferseite

mit den entsprechenden Links angezeigt. Wenn wir dann keinen dieser Links anklicken, so kann das z.B. bedeuten, dass wir kein Interesse mehr an einer weiteren Recherche haben, oder aber auch, dass wir bereits auf der Seite mit den angezeigten Suchergebnissen die notwendige Information gefunden haben."

Der Betreiber der Suchmaschine wüsste in diesem Fall also nicht, warum die Seite verlassen wird – könnte man meinen, wäre da nicht noch die Sache mit der Maus. Denn deren Bewegung gibt mitunter mehr über uns Nutzer preis als wir wissen und als uns vielleicht auch recht ist.

C.5   Guest Researchers

The following guest researchers were invited to the DCS:

Nuwan T. Attygalle
Period: 11 Apr 2022 – 29 Apr 2022
Hosted by: Kayhan LATIFZADEH, Luis A. LEIVA

Dr Dina Babushkina (University of Twente)
Period: 5 Dec 2022 – 6 Dec 2022
Hosted by: Aleks KNOKS
Reason: Research exchange, seminar talk.

Lydia Blümel (FernUniversität Hagen)
Period: 7 Nov 2022 – 9 Nov 2022
Hosted by: Aleks KNOKS
Reason: Research exchange, seminar talk.

Skandylas Charilaos (Linnaeus University, Sweden)
Period: 1 Apr 2022 – 30 Jun 2022
Hosted by: Mike PAPADAKIS

Prof. Moisés Diaz (ULPGC - Universidad de Las Palmas de Gran Canaria, Spain)
Period: 21 Mar 2022 – 1 Apr 2022
Hosted by: Luis A. LEIVA

Dragan Doder (Utrecht University)
Period: 7 May 2022 – 9 May 2022
Hosted by: Réka MARKOVICH, Leon VAN DER TORRE
Reason: Working on DELIGHT

Yue Jiang
Period: 17 Mar 2022 – 18 Mar 2022
Hosted by: Mateusz DUBIEL, Kayhan LATIFZADEH, Luis A. LEIVA, Bereket Abera YILMA

Prof. Kittichai Lavangnananda (KMUTT, Bangkok, Thailand)

Period: 1 Dec 2022 – 20 Dec 2022
Hosted by: Pascal BOUVRY

Prof. Jedrzej Musial (Poznan University of Technology)

Period: 10 Dec 2022 – 17 Dec 2022
Hosted by: Pascal BOUVRY

Dr. Joan Puigcerver (Google Brain)

Period: 21 May 2022 – 24 May 2022
Hosted by: Luis A. LEIVA, Bereket Abera YILMA

Prof. Dr. Andrei Tchernykh (CICESE research center, Ensenada, Mexico)

Period: 1 Aug 2022 – 30 Sep 2022
Hosted by: Pascal BOUVRY

Prof. Dr. Je Sen Teh (Universiti Sains Malaysia)

Period: 15 Nov 2021 – 14 May 2022
Hosted by: Alexei BIRYUKOV

Marc van Zee (Google)

Period: 7 May 2022 – 9 May 2022
Hosted by: Réka MARKOVICH, Leon VAN DER TORRE
Reason: Working on DELIGHT

Dr Athanasios Votsis (University of Twente)

Period: 5 Dec 2022 – 6 Dec 2022
Hosted by: Aleks KNOKS

C.6   Visits

The following visits by DCS members to external organisations took place:

Jean BOTEV

Institution: Collegium Da Vinci
Location: Poznań, Poland
Period: 15 Jul 2022 – 15 Aug 2022.

Abdelwahab BOUALOUACHE

Institution: Université Gustave Eiffel
Location: Paris, France
Period: 7 Oct 2022 – 8 Oct 2022.

Mateusz DUBIEL

Institution: Harvard University
Location: Boston, United States of America
Period: 1 Oct 2022 – 30 Nov 2022.
Reason: Research stay to collaborate with the Intelligent Interactive Systems Group, led by Prof. Krzysztof Gajos.

Reynaldo GIL PONS

Institution: Universitat Rovirai Virgili
Location: Tarragona, Spain
Period: 24 Oct 2022 – 5 Nov 2022.
Reason: Collaborat with Rolando Trujillo-Rasua

Nicolas GUELFI

Institution: Universitè de Genève
Location: Genève, Switzerland
Period: 15 Feb 2022 – 15 Aug 2022.
Reason: The sabbatical took place from February 15 to August 15, 2022 at the Center Universitaire Informatique of the University of Geneva. The main collaborations took place with the professors Didier Buchs and Giovanna di Marzo as well as the members of their teams. During the period of the sabbatical leave, the activities and the results can be summarized in four points:

- Contribution to local education. The teams I have been collaborating with were in charge of several bachelor and master courses. I have been integrated in the teaching team that allowed me to observe and partly contribute to the concerned courses. I also had the opportunity to be part of the mid-term PhD thesis jury of the PhD students which are under the supervision of Professor Didier Buchs.

- Contribution to Requirements Engineering Methodologies. I have been working on a journal paper on MESSIR which is a Flexible Scientific Approach to Requirements Engineering.

- Software Engineering for Deep Learning exploration. I have explored the state of the art on deep learning systems engineering both on the scientific aspect and on the technical one.

- Tasks for University of Luxembourg. I spent one third of my sabbatical on tasks that concerned the courses I am in charge of at University of Luxembourg that I treated remotely.

Aleks KNOKS
Institution: Stanford University
Location: Palo Alto, United States of America
Period: 23 Sep 2022 – 16 Nov 2022.
Reason: Research exchange.

Réka MARKOVICH
Institution: University of Bergen
Location: Bergen, Norway
Period: 5 Aug 2022 – 31 Aug 2022.
Reason: Working with Prof. Marija Slavkovik

Réka MARKOVICH
Institution: University of Bayreuth
Location: Bayreuth, Germany
Period: 20 Oct 2022 – 21 Oct 2022.
Reason: Giving a talk at the Explainable AI and Society series and working with Prof. Olivier Roy.

Igor TCHAPPI HAMAN
Institution: Cheikh Anta Diop University of Dakar
Location: Dakar, Senegal
Period: 8 Oct 2022 – 22 Oct 2022.
Reason: Start to setup collaboration with University of Cheik Anta Diop about research, student and staff exchange.

Leon VAN DER TORRE
Institution: University of Vienna
Location: Vienna, Austria
Period: 3 Mar 2022 – 10 Mar 2022.

Leon VAN DER TORRE
Institution: University of Vienna
Location: Vienna, Austria
Period: 30 Jun 2022 – 28 Aug 2022.

Leon VAN DER TORRE
Institution: Cheikh Anta Diop University of Dakar
Location: Dakar, Senegal
Period: 15 Oct 2022 – 23 Oct 2022.

Leon VAN DER TORRE
Institution: University of Toulouse
Location: Toulouse, France
Period: 28 Nov 2022 – 23 Dec 2022.

Software

Accord

[] https://accord.uni.lux

License: Internal use only

Members: Christian GLODT (Analyst, Architect, Designer, Developer, Tester)

Description: Accord is a the successor to the CSC Information System and is intended to provide services to all FSTM research units. It manages research information and allows the automatic generation of reports and websites.

Changes: Small improvements and bug fixes have been applied to Accord in 2022.

ADTool

[] http://satoss.uni.lu/software/adtool

License: free use

Members: Sjouke MAUW (Analyst)

Description: The attack–defense tree language formalizes and extends the attack tree formalism. It is a methodology to graphically analyze security aspects of scenarios. With the help of attributes on attack–defense trees, also quantitative analysis can be performed. As attack–defense tree models grow, they soon become intractable to be analyzed by hand. Hence computer support is desirable. Software toll, called the ADTool, has been implemented as a part of the ATREES project to support the attack–defense tree methodology for security modeling. The main features of the ADTool are easy creation, efficient editing, and quantitative analysis of attack–defense trees. The tool is available at http://satoss.uni.lu/software/adtool. The tool was realized by Piotr Kordy and its manual was written by Patrick Schweitzer.

Algorithms for Probabilistic Argumentation

License: Creative Common

Members: Leon VAN DER TORRE (Architect)

Description: We developed efficient algorithms for computing probabilistic argumentation. These algorithms were implemented in Java, and tested on a machine with an Intel CPU running at 2.26 GHz and 2.00 GB RAM. Please refer to the following paper in details.

1. Beishui Liao, Kang Xu, Huaxin Huang. Formulating Semantics of Probabilistic Argumentation by Characterizing Subgraphs: Theory and Empirical Results, Jurnal of Logic and Computation, to appear. http://arxiv.org/abs/1608.00302

AMT: Assessment Management Tool

License: to be defined

Members: Alfredo CAPOZUCCA (Analyst), Nicolas GUELFI (Analyst), Thibault Jean Angel SIMONETTO (Developer)

Description: AMT: Assessment Management Tool is a software to assess an observed element (e.g. course, student) according to an evaluation model. Each evaluation model uses one or multiple scale(s) to evaluate the observed element. The development of this tool was initiated in the context of a Bachelor in Informatics (BINFO)'s thesis and it's still under construction. Currently, there exists only a beta version available to internal members of the group.

ASSA-PBN

http://satoss.uni.lu/software/ASSA-PBN/

License: free use

Members: Andrzej MIZERA (Designer), 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/.

at-decorator

License: GNU General Public License v3.0

Members: Sjouke MAUW (Designer)

Description: **at-decorator** is a tool designed to compute values for an attack tree (fully decorate an attack tree) given some available data points and predicates on data values (relationships between attack tree node values). In contrast to the standard bottom-up approach, our tool does not require to have all leaf node values available to fully decorate a tree.

The tool is available as open source, and it utilizes Constraint Programming and the Z3 theorem prover. The tool is available here https://github.com/vilena/at-decorator/tree/master/CSP_decorator

Automated UPPAAL Model Reduction Tool in Java

License: N.A

Members: Ross James HORNE (Supervisor)

Description: This program takes an UPPAAL Model file along with a relevant strategy encoded in an ADTool XML file as inputs, and produces a valid reduced UPPAAL model. Proper application of this tool can greatly increase UPPAAL's verification performance.

We also aim to synthesis attack-defence trees by discovering strategies that avoid vulnerabilities. This tool was developed by bachelor student Filip Jamproga during his BSP under Dr. Ross James Horne, and can be found in his github repository: https://github.com/Jonson26/Cypis

AVXECC

License: GPLv3

Members: Hao CHENG (Developer), Johann GROSZSCHÄDL (Developer)

Description: High-throughput elliptic curve cryptography software using Advanced Vector Extensions.

BEACON Q

License: N/A

Members: Aryobarzan ATASHPENDAR (Architect, Developer), Steffen ROTHKUGEL (Architect)

Description: BEACON Q is a digital quiz application for mobile devices (iOS/Android) supporting students through various scheduled activities with dynamically adapted difficulty, following along with the lecture's topics.

Changes: Launch
v1.0 | 2022-09-14

BiCS Management Tool (BMT)

[➚ https://messir.uni.lu/bmt/login](https://messir.uni.lu/bmt/login)

License: to be defined

Members: Nicolas GUELFI (Analyst), Benoit RIES (Analyst)

Description: Development of the BiCS Management Tool, a web application for managing the BiCS Semester Projects.

Changes: Due to budgetary constraint, the BiCS Management Tool (BMT) had to be redesigned into a lighter version easier and less costly to maintain. The main constraint for this new design is that the maintenance should be manageable by one student/summer job because the main senior developper contract was not renewed.

The new version of the BMT tool, named BMT-Light, is now up and running. It is composed of Google Slides, Google Sheets and automated Microsoft workflows.

BiCS Website

License: to be defined

Members: Nicolas GUELFI (Analyst), Benoit RIES (Analyst)

Description: The modern website should be a first entrance door for the new Bachelor. People from outside should get all information around the Bachelor and the projects done within the BiCSLab. One the one hand, our goal is to make the Bachelor visible to the World and attract people to enrol inside the Bachelor. On the other hand, we would like to make our projects visible to the outside, to attract industrial partners for proposing projects within the BiCS and the BiCSLab. Student's can work on these projects within their BiCS Semester Project course in cooperation with the industrial partners.

CABEAN

License: Apache License

Members: Jun PANG (Designer)

Description: CABEAN is a software tool for the control of asynchronous Boolean networks, which are often used to model gene regulatory networks. CABEAN is freely available. The newest version of CABEAN is 2.0.0, updated on October 26, 2020.

CABEAN provides the following methods to solve the six source-target control problems: the minimal one-step instantaneous source-target control (OI); the minimal one-step temporary source-target control (OT); the minimal one-step permanent source-target control (OP); attractor-based sequential instantaneous source-target control (ASI); attractor-based sequential temporary source-target control (AST); attractor-based sequential permanent source-target control (ASP). CABEAN provides the following target control methods: instantaneous target control (ITC); temporary target control (TTC); permanent target control (PTC).

CheckMasks: formal verification of side-channel countermeasures for cryptographic implementations

 ⧉ https://github.com/coron/checkmasks

License: GPL v2

Members: Jean-Sébastien CORON (Designer)

Description: This is an implementation in Common Lisp of the techniques described in the paper:

[Cor17b] Jean-Sebastien Coron. Formal Verification of Side-Channel Countermeasures via Elementary Circuit Transformations. IACR eprint archive. https://eprint.iacr.org/2017/879.pdf

Generic verification of security properties:

- Generic verification of the t-SNI of multiplication-based refreshing
- Generic verification of the t-SNI of multiplication
- Generic verification of some properties of RefreshMasks: lemmas 5, 6, 7, 8 of [Cor17a], and Lemma 3 from [CRZ18].
- Generic verification of the t-SNI property of the Boolean to arithmetic conversion algorithm from [Cor17a].

Polynomial-time verification fo security properties:

- Poly-time verification of the t-SNI of multiplication-based refreshing [Cor17b, Lemma 3]
- Poly-time verification of some properties of RefreshMasks: [Cor17b, Lemma 4] corresponding to [Cor17a, Lemma6], and [Cor17b, Lemma 5] corresponding to [Cor17a, Lemma 5]
- Poly-time verification of the t-SNI of multiplication [Cor17b, Lemma 6]

Automatic generation of security proof:

- Automatic poly-time verification of t-SNI of multiplication-based refreshing, and of the two previous properties of RefreshMasks.

References:

[Cor17a] Jean-Sebastien Coron. High-order conversion from boolean to arithmetic masking. Proceedings of CHES 2017.

[CRZ18] Jean-Sébastien Coron, Franck Rondepierre, Rina Zeitoun. High Order Masking of Look-up Tables with Common Shares. To appear at TCHES 2018. IACR Cryptology ePrint Archive 2017: 271 (2017)

Coco Müller

License: Proprietary

Members: Sviatlana HOEHN (Supervisor)

Description: Practicing foreign language conversation with a machine may have multiple advantages: a machine does not judge, a machine is always available and accessible from everywhere. In this project we focus on language understanding and generation for German as a communication language for non-native speakers.

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.

CrazyRL

 https://github.com/ffelten/CrazyRL

License: MIT

Members: Grégoire DANOY (Supervisor), Florian FELTEN (Developer)

DBVerify

 ⧉ http://satoss.uni.lu/software/DBVerify/

License: Open source

Members: Sjouke MAUW (Designer)

Description: DBVerify is a set of Tamarin implementation of several state-of-the-art distance-bounding protocols as well as their MSC representation. It intends to show the usage of the causality-based verication methodology proposed in our paper "Distance-Bounding Protocols: Verication without Time and Location" (published at IEEE S&P'18). It was developed by Zach Smith (ZS) and Jorge Toro-Pozo (JT).

E4L: Energy for Life

License: to be defined

Members: Alfredo CAPOZUCCA (Architect), Phillip DALE (Developer), Michele MEL-CHIORRE (Developer)

Description: E4L: Energy for Life is a web application aimed at helping people to calculate their daily energy consumption, and allow them to compare between days, and between people. In this manner, users input information using pictures that best fit their daily experience, and then the tool compares the persons data, to Luxembourg, European, and World averages. Thus, the tool is supposed to help people understand better energy or how much they use. The development of this web application forms the core of a larger educational and research concept. This work is done in collaboration with the Laboratory for Energy Materials (LEM).

ELRA Language Corpus

License: LC/ELDA/DISTR-S/2014-11/001-UNILU

Members: Sviatlana HOEHN (Architect), Christoph SCHOMMER (Designer)

Description: The *deL1L2IM* corpus, created between May and August 2012 and last updated in August 2014, has been collected within the framework of a PhD project (Mrs. Sviatlana Höhn, geb. Danilava) on the development of a learning method implying conversations with an artificial companion. This PhD work is presented as a qualitative investigation of instant messaging dialogues on a long-term basis (four months) between advanced learners of German and German native speakers, chatting about whatever topic they wish.

The dataset is composed of 72 dialogues, each of them having a duration of 20 to 45 minutes. The whole corpus contains ca. 52,000 words and 4,800 messages and has a file size of 0,5 Mb. Nine pairs of participants – i.e. nine learners and four native speakers – were required, with 8 dialogues per pair.

The interactions have undergone linguistic analysis whereby the annotation will be performed only on repair/correction sequences (incomplete learner error annotation). The goal of the project was to create an application for language modelling and to improve learner language applications, tutoring softwares and dialogue systems.

The corpus is delivered in one written text file (in XML format, customized under TEI P5).

ePassport Vulnerability Demonstration

[☑ https://github.com/bboyifeel/passport_relay_guide](https://github.com/bboyifeel/passport_relay_guide)

License: Apache License

Members: Ross James HORNE (Architect), Sjouke MAUW (Architect)

Description: We have a repository containing code to demonstrate vulnerabilities discovered in ePassports. Two modified readers are used for such demonstrations. One acts as a fake reader who relays information to a fake ePassport in another location. Both can be installed on an Android phone with RFC capabilities. The attack has been disclosed responsibly.

E-Puck2 ARGoS plug-in

[☑ https://gitlab.uni.lu/adars/e-puck2](https://gitlab.uni.lu/adars/e-puck2)

License: MIT License

Members: Daniel STOLFI ROSSO (Developer)

Description: E-Puck2 robot plug-in for the ARGoS simulator.

Excalibur

[☑ https://messir.uni.lu/confluence/display/EXCALIBUR/Excalibur](https://messir.uni.lu/confluence/display/EXCALIBUR/Excalibur)

License: Eclipse Public License 1.0

Members: Alfredo CAPOZUCCA (Developer), Nicolas GUELFI (Developer), Benoit RIES (Developer)

Description: Excalibur is a tool supporting the Messir methodology, a Scientific Method for the Software Engineering Master, used in Software Engineering Lectures at bachelor and master levels.

Excalibur tool covers the phase of Requirements Analysis and its main features are requirements analysis specification (its own DSL), requirements report generation (latex/pdf) and requirements simulation (prolog). It relies on Eclipse technologies as XText for textual specification and Sirius for graphical views of the textual specifications.

It is available here: http://messir.uni.lu

FELICS

https://github.com/cryptolu/FELICS

License: GNU General Public License Version 3

Members: Luan CARDOSO DOS SANTOS (Developer), Johann GROSZSCHÄDL (Developer)

Description: FELICS is an open-source framework for the fair and consistent evaluation of lightweight cryptographic primitives on 8-bit AVR, 16-bit MSP430, and 32-bit ARM Cortex-M microcontrollers. Further information about FELICS can be found on the CryptoLux Wiki at https://www.cryptolux.org/index.php/FELICS.

Findel

https://github.com/cryptolu/findel

License: GNU General Public License Version 3

Members: Alexei BIRYUKOV (Designer)

Description: Findel (Financial Derivatives Language) is a domain-specific language that implements the composable approach to modeling financial derivatives on the Ethereum platform. Most of the software was developed by Sergei Tikhomirov. More information on Findel can be found in the paper "Findel: Secure Derivative Contracts for Ethereum".

Fudomo

 ⧉ https://fudomo.uni.lu/

License: MIT

Members: Christian GLODT (Designer, Developer, Tester), Pierre KELSEN (Tester, Supervisor)

Description: Implementation of a model transformation approach based on functional decomposition, including a web-based modeling environment as well as command-line tools and libraries. The web-based modeling environment is available at https://lassy-fmde. github.io/try-fudomo/.

Gustav

 ⧉ https://gitlab.uni.lu/coin/gustav/

License: MIT

Members: Kayhan LATIFZADEH (Developer), Luis A. LEIVA (Supervisor)

Description: Gustav does offline temporal synchronization of behavioral and physiological signals collected through different devices and different computers, ensuring that all signals coincide exactly with the duration of each experiment condition, with millisecond precision.

Changes: First release

J-NERD/J-REED

 ⧉ https://people.mpi-inf.mpg.de/~datnb/

License: BSD

Members: Martin THEOBALD (Architect)

Description: Open-source information extraction libraries

LegendrePRF

 ⏿ http://github.com/cryptolu/LegendrePRF

License: MIT

Members: Aleksei UDOVENKO (Developer)

Description: This repository contains an implementation of the attack from the paper Cryptanalysis of the Legendre PRF and Generalizations by *Ward Beullens, Tim Beyne, Aleksei Udovenko, and Giuseppe Vitto.* The code can be used to break **Challenge 2** of the Legendre PRF Bounties in under 1500 CPU-hours. For more details, please refer to the paper.

Légionnaires Rallye

 ⏿ https://www.legionnaires.lu/

License: N/A

Members: Jean BOTEV (Designer), Claude Marc OHLHOFF (Developer)

Description: The Légionnaires Rallye is a mobile game engaging players in a digital treasure hunt around Luxembourg City. It was developed in collaboration with the Luxembourg Centre for Contemporary and Digital History (C^{2}DH), to promote the Légionnaires exhibition (June 30, 2021 - February 28, 2022) at the Musée Dräi Eechelen. The game extends the exhibition outside the museum walls, allowing players to learn about the history of the Luxembourgish légionnaires while solving riddles and walking around the city.

MiCS Management System

 ⏿ http://demos.uni.lux/mics

License: non-redistributable, for internal use only

Members: Christian FRANCK (Analyst, Architect), Christian GLODT (Designer, Developer, Tester)

Description: An internal web-based tool developed for the management of modules, courses and profiles of the Master in Information and Computer Sciences. Developed by Christian Glodt.

MiF-Cham-Katan

License: GPLv3

Members: Alexei BIRYUKOV (Supervisor), Luan CARDOSO DOS SANTOS (Developer), Je Sen TEH (Developer), Aleksei UDOVENKO (Developer)

Description: An experimental implementation of the Meet-in-the-Filter (MiF) technique for cryptanalysis of the lightweight cryptosystems Cham and Katan. The related research paper is entitled "Advancing the Meet-in-the-Filter Technique: Applications to CHAM and KATAN" and was published in the proceedings of SAC 2022.

MiF-Speck

License: GPLv3

Members: Alexei BIRYUKOV (Supervisor), Luan CARDOSO DOS SANTOS (Developer), Je Sen TEH (Developer), Aleksei UDOVENKO (Developer)

Description: A demonstration of the Meet-in-the-Filter (MiF) technique for cryptanalysis of the lightweight block cipher Speck. The related research paper is entitled "Meet-in-the-Filter and Dynamic Counting with Applications to Speck" and was published in the proceedings of ACNS 2023.

Minett Stories Rallye

License: N/A

Members: Jean BOTEV (Architect), Claude Marc OHLHOFF (Developer)

Description: The Minett Stories Rallye is a mobile game developed in collaboration with the Luxembourg Centre for Contemporary and Digital History (C^2DH) to promote the Esch2022 exhibition "Remixing Industrial Pasts – Constructing the Identity of the Minett" (February 27, 2022 - May 15, 2022) at the Massenoire in Esch Belval. The game allows discovering on-site various places related to the history of the area's industrial past.

Changes: Mobile web application.

MinUS

License: free use

Members: Jun PANG (Analyst)

Description: This tool, MinUS, integrates the technologies of trajectory pattern mining with the state-of-the art research on discovering user similarity with trajectory patterns. Specifically, with MinUS, we provide a platform to manage movement datasets, and construct and compare users trajectory patterns. Tool users can compare results given by a series of user similarity metrics, which allows them to learn the importance and limitations of different similarity metrics and promotes studies in related areas, e.g., location privacy. Additionally, MinUS can also be used by researchers as a tool for preliminary process of movement data and parameter tuning in trajectory pattern mining. The tool is available at http://satoss.uni.lu/software/MinUS.

Model Decomposer

License: free to use, binary redistribution permitted

Members: Christian GLODT (Architect, Developer), Qin MA (Analyst)

Description: An Eclipse plugin that implements a generic model decomposition technique which is applicable to Ecore instances and EP models, and is described in a paper published in the proceedings of the FASE 2011 conference.

MO-Gymnasium

License: MIT

Members: Grégoire DANOY (Supervisor), Florian FELTEN (Developer)

Description: MO-Gymnasium: a unified API for multi-objective reinforcement learning (MORL) benchmark environments. Allowing to test on various problems without changing the algorithm (goes in the sense of hyper-heuristics in the sense of genericity). MO-Gym was accepted and presented at BNAIC 2022 [10993/52836] and officially integrated to Farama foundation.

MORL-Baselines

License: MIT

Members: Grégoire DANOY (Supervisor), Florian FELTEN (Developer)

MouseFaker

License: MIT

Members: Luis A. LEIVA (Developer)

Description: A web browser extension that anonymizes your mouse movements to prevent user profiling.

MsATL (MonoSat for Alternating-time Temporal Logic)

License: MIT License

Members: Wojciech JAMROGA (Designer)

Description: MsATL is a prototype tool for deciding the satisfiability of Alternating-time Temporal Logic (ATL) with imperfect information. MsATL combines SAT Modulo Monotonic Theories solvers with existing ATL model checkers: MCMAS and STV. The tool can deal with various semantics of ATL, including perfect and imperfect information, and can handle additional practical requirements. MsATL can be applied for synthesis of games that conform to a given specification, with the synthesized game often being minimal.

MSP430 code analysis tool

License: (c) University of Luxembourg

Members: Christian FRANCK (Developer)

Description: Tool that simulates step by step the execution of an assembler program on the MSP430. While doing so, it collects statistical data about various aspects of the code

execution, such as how often specific instructions and addressing modes are used, how often memory is accessed to read instructions and how often to read data, the stack depth that is used, how many times a user defined macro is executed, and so on. The tool can be used to evaluate implementations of cryptographic functions on the MSP430, assess for instance the efficiency of rotations, linear and non-linear operations and so on.

Primes-Backdoor

 ☞ https://github.com/cryptolu/primes-backdoor

License: GPLv3

Members: Giuseppe VITTO (Developer)

Description: The Primes-Backdoor repository contains a SageMath implementation of the prime generation procedure and factorization attack detailed in the paper "Factoring Primes to Factor Moduli: Backdooring and Distributed Generation of Semiprimes".

Protocol implementation of Dining Cryptographers Networks (DC-nets)

 ☞ https://gitlab.uni.lu/cfranck/dcnets

License: (C) University of Luxembourg

Members: Christian FRANCK (Developer)

Description: This project is about a practical implementation of Dining Cryptographers Networks based on the research that can be found on our project homepage (https://dcnets.readthedocs.io).

The protocol relies on the following techniques:

- Zero-knowledge ciphertext verification based on Pedersen commitments. (https://arxiv.org/abs/1402.2269)
- SICTA-based collision resolution with a throughput of 0.924 packets. (https://arxiv.org/abs/1402.1732)

ReCon

☑ https://github.com/cryptolu/ReCon

License: GNU General Public License Version 3

Members: Alexei BIRYUKOV (Designer)

Description: ReCon is a Universal Reputation Module for Distributed Consensus Protocols. This software provides the simulation of the protocol written in Python 2.7 based on the paper "Guru: Universal Reputation Module for Distributed Consensus Protocols". Most of the software was written by Daniel Feher.

RuleML_to_TPTP_conversion

License: (c) University of Luxembourg

Members: Christian FRANCK (Developer)

Selene Cryptographic Library in Python

License: Internal use only

Members: Peter Y A RYAN (Supervisor)

Selene User Interface

License: Internal use only

Members: Marie-Laure ZOLLINGER (Developer)

SemiPrimes

☑ https://github.com/cryptolu/semiprimes

License: GPLv3

Members: Giuseppe VITTO (Developer)

Description: The SemiPrimes repository contains a SageMath and MP-SPDZ implementation of the distributed semiprime generation protocol detailed in the paper "Factoring Primes to Factor Moduli: Backdooring and Distributed Generation of Semiprimes".

SHA512 optimized for MSP430

 ⧉ https://gitlab.uni.lu/cfranck/sha512_for_msp430

License: (C) University of Luxembourg

Members: Christian FRANCK (Developer), Johann GROSZSCHÄDL (Developer)

Description: Optimized Implementation of SHA-512 for MSP430 Microcontrollers. Details are described in the paper referenced on https://orbilu.uni.lu/handle/10993/49799.

Sketchnoting

License: N/A

Members: Aryobarzan ATASHPENDAR (Developer), Christian GREVISSE (Architect)

Description: Enhanced sketchnoting (iOS app) for the retrieval and integration of learning material.

Features handwriting recognition and semantic annotation for retrieving resources relevant to the concepts mentioned in the handwritten notes from existing Knowledge Graphs. Drawing recognition enables visual queries, allowing for enhanced search capabilities.

SPARKLE

 ⧉ https://github.com/cryptolu/sparkle

License: GNU General Public License Version 3

Members: Luan CARDOSO DOS SANTOS (Developer), Johann GROSZSCHÄDL (Developer), Aleksei UDOVENKO (Developer)

Description: SPARKLE is an ARX-based cryptographic permutation suitable for software implementation on 8/16/32-bit microcontrollers. SCHWAEMM and ESCH are an authenticated encryption algorithm and a hash function, respectively, which use the SPARKLE permutation in a sponge construction. This repository contains (i) reference and optimized C implementations of SCHWAEMM and ESCH, (ii) supporting software for the security analysis of SPARKLE, SCHWAEMM, and ESCH, (iii) documentation, (iv) the submission packages for the NIST Lightweight Cryptography competition, and (v) benchmarking results.

STV (STrategic Verifier)

License: MIT License

Members: Wojciech JAMROGA (Supervisor)

Description: STV is a prototype tool aimed at verification of strategic abilities in multi-agent systems, and synthesis of strategies that guarantee a given temporal goal. We have significantly extended the tool with support for model reductions. Two methods are used: (i) checking for equivalence of models according to a handcrafted relation of alternating bisimulation, and (ii) fully automated partial order reduction (POR). We also added a simple model specification language that allows the user to define their own inputs for verification, which was not available in the previous version.

The purpose of the extension is twofold. First, it should facilitate practical verification of MAS, as the theoretical and experimental results for POR and bisimulation-based reduction suggest. No less importantly, it serves a pedagogical objective. Actual reduction schemes are often difficult to understand. We put emphasis on visualisation of the reductions, so that the tool can be also used in the classroom to show how the reduction works. Finally, checking strategic bisimulation by hand is difficult and prone to errors; here, the user can both see the idea of the bisimulation, and automatically check if it is indeed correct.

TeachDCS: Teaching Load Monitoring System

License: Copyright University of Luxembourg (Default)

Members: Christian FRANCK (Developer)

Description: DCS Teaching Monitoring System (for internal use)

TESMA

License: Eclipse Public License 1.0

Members: Nicolas GUELFI (Analyst), Benjamin JAHIC (Developer), Sandro REIS (Developer), Benoit RIES (Analyst)

Description: Tool for the Specification, Management and Assessment of Teaching Programs.

Nicolas Guelfi, Benjamin Jahic and Benoît Ries, TESMA: Towards the Development of a Tool for Specification, Management and Assessment of Teaching Programs, published in the Proceedings of the 2nd International Conference on Applications in Information Technology (ICAIT-2016)

http://orbilu.uni.lu/handle/10993/28607

TriAD

 ⧉ https://people.mpi-inf.mpg.de/~gurajada/

License: BSD

Members: Martin THEOBALD (Architect)

Description: Open-source, distributed graph database

Whitebox

 ⧉ https://github.com/cryptolu/whitebox

License: GNU General Public License Version 3

Members: Alexei BIRYUKOV (Designer), Aleksei UDOVENKO (Developer)

Description: This repository contains white-box analysis and implementation tools, in particular proof-of-concept code for the paper "Attacks and Countermeasures for White-box Designs" by Alex Biryukov and Aleksei Udovenko (ASIACRYPT 2018).

The code is split into three parts:

1. Implementation: Proof-of-concept implementation of AES using the new nonlinear masking scheme.

2. Verification: Code for verifying algebraic security of gadgets.

3. Attacks: Several attacks from the paper.

X64ECC: Elliptic Curve Cryptography for Dining Cryptographers Networks

 ⧉ https://gitlab.uni.lu/cfranck/dcnets

License: (C) University of Luxembourg

Members: Christian FRANCK (Developer), Johann GROSZSCHÄDL (Developer)

Description: Optimized cryptographic library using the techniques described in "Fast and Flexible Elliptic Curve Cryptography for Dining Cryptographers Networks" (https://orbilu.uni.lu/handle/10993/46390).

XDEM (eXtended Discrete Element Method)

 http://luxdem.uni.lu/

License: Internal use only

Members: Bernhard PETERS (Developer), Sébastien VARRETTE (Developer)

Description: The eXtended Discrete Element Method (XDEM), formerly Discrete Particle Method (DPM), is an advanced numerical simulation tool which deals with both motion and chemical conversion of particulate material such as coal or biomass in furnaces. However, predictions of solely motion or conversion in a de-coupled mode are also applicable. The Discrete Particle Method uses object oriented techniques that support objects representing three-dimensional particles of various shapes such as cylinders, discs or tetrahedrons for example, size and material properties. This makes it a highly versatile tool dealing with a large variety of different industrial applications of granular matter. A user interface allows easily extending the software further by adding user-defined models or material properties to an already available selection of materials, properties and reaction systems describing conversion. Thus, the user is relieved of underlying mathematics or software design, and therefore, is able to direct his focus entirely on the application. The Discrete Particle Method is organised in a hierarchical structure of C++ classes and works both in Linux and XP environments also on multi-processor machines. This software is developed by the XDEM research team, led by Prof. Bernhard Peters from the Research Unit in Engineering Science (RUES) in collaboration with the Department of Computer Science.

Yactul

License: N/A

Members: Steffen ROTHKUGEL (Architect)

Description: Yactul is a game-based student response framework for interactive education.

ZettaStreams

 https://gitlab.uni.lu/omarcu/zettastreams

License: Apache2

Members: Ovidiu-Cristian MARCU (Developer)

Description: The ZettaStreams prototype is a unified storage and processing architecture for handling key-value and streaming storage and real-time processing. ZettaStreams develops on top of RAMCloud, KerA, DFI, Apache Arrow, Apache Flink.

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	45.85
Postdoctoral Researcher	33.44
Student / Intern	27.97
Professor	21.61
Research Scientist	17.11
Specialist	5.59
Scientific / Technical Support Staff	4.99
Research Associate	4.66
Administrative Staff	3.76
Research Facilitator	1.21
Technology Transfer Officer	1
International Relations Officer	0.49
Total	*167.68*

Table E.1: Number of Staff by Category

E.2   Distribution of Staff by Category
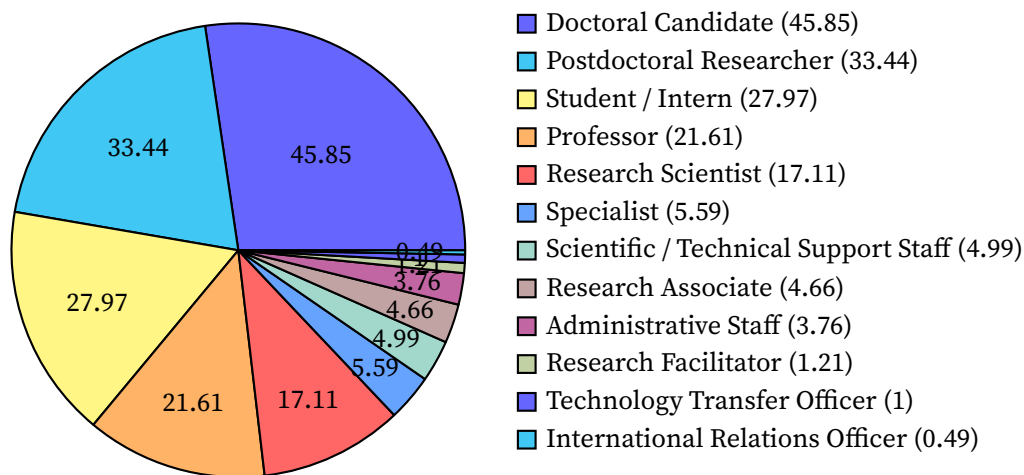
Figure E.1: Staff Distribution

E.3   List of Members by Category

Note: In the following list, staff members without an explicitly shown FTE number implicitly have an FTE number of 1.0.

Category	Last Name	First Name
Professor	BIRYUKOV	Alexei
	BOUVRY	Pascal (0.87 FTE)
	CORON	Jean-Sébastien
	ENGEL	Thomas
	GUELFI	Nicolas
	KELSEN	Pierre
	LE TRAON	Yves
	LEIVA	Luis A.
	LEPREVOST	Franck
	MAUW	Sjouke
	MÜLLER	Volker
	NAVET	Nicolas
	PAPADAKIS	Mike
	ROTHKUGEL	Steffen
	RYAN	Peter Y A (0.99 FTE)
	SACHAU	Juergen (0.78 FTE)
	SCHOMMER	Christoph
	SORGER	Ulrich
	STEENIS	Bernard
	THEOBALD	Martin
	VAN DER TORRE	Leon
	ZAMPUNIERIS	Denis

Category	Last Name	First Name
Research Scientist	BOTEV	Jean
	CAPOZUCCA	Alfredo
	CORDY	Maxime
	DANOY	Grégoire
	FRANCK	Christian
	HU	Tingting
	JAMROGA	Wojciech
	KIEFFER	Emmanuel
	KUBLER	Sylvain (0.80 FTE)
	MA	Qin (0.77 FTE)
	MARKOVICH	Réka (0.13 FTE)
	MUELLER	Johannes
	PANG	Jun
	RIES	Benoit
	RUPP	Andy
	SCHLEICH	Julien (0.75 FTE)
	SKROBOT	Marjan
	VARRETTE	Sébastien (0.66 FTE)
	WEYDERT	Emil
Postdoctoral Researcher	ACCLAVIO	Matteo (0.41 FTE)
	ALEKSANDROVA	Marharyta (0.70 FTE)
	BIRYUKOV	Maria
	BOUALOUACHE	Abdelwahab
	BURSUC	Sergiu (0.99 FTE)
	BUSCEMI	Alessio (0.67 FTE)
	CARNEIRO PESSOA	Tiago (0.70 FTE)
	CHEN	Xihui
	CORTES MENDOZA	Jorge Mario (0.29 FTE)
	DAMODARAN	Aditya Shyam Shankar (0.16 FTE)
	DELERUE ARRIAGA	Afonso
	DUBIEL	Mateusz
	EBRAHIMI	Ehsan (0.99 FTE)
	GHAMIZI	Salah (0.29 FTE)
	HOEHN	Sviatlana (0.95 FTE)
	HORNE	Ross James
	HULSTIJN	Joris (0.33 FTE)
	JIMENEZ	Matthieu
	KNOKS	Aleks
	KONG	Pingfan (0.28 FTE)
	KOUTSANTONIS	Loizos (0.08 FTE)
	KRISHNASAMY	Ezhilmathi (0.33 FTE)
	LAMBIN	Baptiste (0.75 FTE)
	LAMSIYAH	Salima (0.50 FTE)
	LIBAL	Tomer
	LIGA	Davide (0.33 FTE)
	LOMBARD-PLATET	Marius
	MA	Wei (0.33 FTE)
	MARCU	Ovidiu-Cristian

Category	Last Name	First Name
	MARKOVICH	Réka (0.87 FTE)
	MIZERA	Andrzej
	NAJJAR	Amro (0.12 FTE)
	NOUZRI	Sana (0.91 FTE)
	PARDO VENTURA	Pere (0.96 FTE)
	ROY	Arijit (0.33 FTE)
	SALA	Petra (0.24 FTE)
	SALEME RUIZ	Katerine
	SIRAJZADE	Joshgun
	SOROUSH	Najmeh (0.49 FTE)
	STOLFI ROSSO	Daniel
	TCHAPPI HAMAN	Igor (0.88 FTE)
	TEH	Je Sen (0.37 FTE)
	TOPAL	Ali Osman
	UDOVENKO	Aleksei
	WANG	Qingju
	YILMA	Bereket Abera (0.88 FTE)
	ZOLLINGER	Marie-Laure (0.29 FTE)
Research Associate	FOTIADIS	Georgios
	KRISHNASAMY	Ezhilmathi (0.66 FTE)
	MESTEL	David
	TABATABAEI	Masoud
	TALBOT	Pierre
International Relations Officer	LIAKIDOU	Eleni (0.49 FTE)
Technology Transfer Officer	WASIM	Muhammad Umer
Research Facilitator	OCHSENBEIN	Anne (0.50 FTE)
	OESTLUND	Stefanie (0.71 FTE)
Specialist	BAKHNO	Iryna (0.04 FTE)
	FUENMAYOR PELAEZ	David (0.58 FTE)
	GLODT	Christian
	GROSZSCHÄDL	Johann
	HOUITTE	Pierre-Yves
	LADID	Latif (0.97 FTE)
	MACHALEK	Aurel
Scientific / Technical Support Staff	CARTIAUX	Hyacinthe
	OLLOH	Abatcha
	REIS	Sandro
	STEMPER	André
	VALETTE	Teddy
Doctoral Candidate	ADAVOUDI JOLFAEI	Amirhossein
	ALCARAZ	Benoît (0.88 FTE)
	ATASHPENDAR	Aryobarzan
	BALOGLU	Sevdenur
	BARTHEL	Jim Jean-Pierre (0.66 FTE)

Category	Last Name	First Name
	BUSCEMI	Alessio (0.32 FTE)
	CARDOSO DOS SANTOS	Luan (0.49 FTE)
	CHARLÈS	Alex (0.29 FTE)
	CHAYCHI	Samira
	CHEN	Ninghan
	CHENG	Hao
	CHITIC	Ioana Raluca (0.66 FTE)
	COMBARRO SIMON	Manuel
	DALLE LUCCA TOSI	Mauro
	DAMODARAN	Aditya Shyam Shankar (0.83 FTE)
	DE JESUS SOUSA	Tiago Alexandre (0.25 FTE)
	DE WIT	Vincent (0.75 FTE)
	DOS SANTOS LOUREIRO	Mike (0.29 FTE)
	DUFLO	Gabriel
	EL ORCHE	Fatima Ezzahra (0.66 FTE)
	ESTAJI	Ehsan
	FOTOUHI	Mahdi
	GARG	Aayush
	GHAMIZI	Salah (0.70 FTE)
	GIL PONS	Reynaldo
	HADDAD	Hedieh (0.96 FTE)
	HOSSEINI KIVANANI	Nina
	HU	Hailong
	JAHIC	Benjamin (0.36 FTE)
	KALISKI	Adam
	KAMLOVSKAYA	Ekaterina (0.08 FTE)
	KARPATI	Daniel
	KELLER	Patrick
	KIM	Yan
	LATIFZADEH	Kayhan (0.91 FTE)
	LI	Xu
	LIU	Chao (0.04 FTE)
	MA	Wei (0.41 FTE)
	MAI	TIEU LONG (0.04 FTE)
	MAKKI	Ayman
	MANCELLARI	Enea (0.13 FTE)
	NIKNAM	Sahar (0.75 FTE)
	NOURBAKHSH	Aria (0.42 FTE)
	PICARD	Stéven
	RIDA	Ahmad (0.70 FTE)
	SHEYKHMOHAMMADI	Nazanin (0.50 FTE)
	SOROUSH	Najmeh (0.08 FTE)
	SOUANI	Badr
	STREIT	David D
	SUN	Ningyuan
	TAWAKULI	Amal (0.24 FTE)
	TEMPERONI	Alessandro
	THANAPOL	Panissara
	TONG	Tsz Pan (0.25 FTE)

Category	Last Name	First Name
	VAN WIER	Jeroen
	VITTO	Giuseppe (0.08 FTE)
	WANG	Aoran
	XU	Jingjing
	YU	Liuwen
	YURKOV	Semen
	ZAHORANSKY	Valeria (0.83 FTE)
	ZHONG	Zhiqiang (0.28 FTE)
Administrative Staff	LIAKIDOU	Eleni (0.46 FTE)
	PECERO SANCHEZ	Johnatan Eliabeth
	PUECH	Andrea (0.80 FTE)
	SCHMITZ	Fabienne
	SCHROEDER	Isabelle (0.50 FTE)
Student / Intern	AGIUS	André (0.11 FTE)
	AKINYEMI	Opeyemi Priscilla (0.49 FTE)
	ALMOHAMAD	Abdulsalam (0.33 FTE)
	ALSAHLI	Malik Ruzayq M (0.50 FTE)
	ANTROPOVA	Daria
	AVDUSINOVIC	Elmir (0.25 FTE)
	BARGHOUTI	Yasmine (0.58 FTE)
	BAUM	Pit (0.19 FTE)
	BEGUM	Rubaiya (0.16 FTE)
	BLIZNIUKOV	Vladimir (0.17 FTE)
	BONTE	Eliott Cyril Michel (0.59 FTE)
	BOURSCHEID	Thiago Jorge (0.58 FTE)
	BĂDEU	Andreea (0.25 FTE)
	CAO	Rui (0.66 FTE)
	CAPITANESCU	Stefan Vladimir (0.08 FTE)
	DE JESUS MATIAS	Flavio (0.22 FTE)
	DE JESUS SOUSA	Tiago Alexandre (0.49 FTE)
	DE PLAEN	Celine (0.03 FTE)
	DECKENBRUNNEN	Tom (0.22 FTE)
	DERIDDER	Nathan Lennart Vicky (0.16 FTE)
	DI BIASE	Fabio (0.09 FTE)
	DOVUTBEKOV	Hamza (0.11 FTE)
	DUARTE TOJAL	Daniel (0.16 FTE)
	FATHI	Fatima Zahra (0.66 FTE)
	FERNANDEZ SABOGAL	Karolina (0.41 FTE)
	FERSTLER	Yves Claude (0.11 FTE)
	FIGUEIREDO CARVALHO FERNANDES OLIVEIRA	João Maria (0.15 FTE)
	GAREEV	Daniel (0.91 FTE)
	GHARBIN	Prince Yaw (0.91 FTE)
	GIESTA GONCALVES	Rui Filipe (0.10 FTE)
	GILLET	Thomas (0.25 FTE)

Category	Last Name	First Name
	GOLDBERG	Alexander Linnevers (0.51 FTE)
	GOMES DOS SANTOS	Astley (0.20 FTE)
	GOZALPOUR	Nima (0.28 FTE)
	GUERIN	Titouan François Lukas (0.41 FTE)
	HANG	Kevin (0.03 FTE)
	HOUSSEL	Paul Robert Balthazar (0.19 FTE)
	HRYHAROVICH	Daniil (0.21 FTE)
	IGHANIAN	Paria (0.50 FTE)
	ISLAM	Md Shahidul (0.91 FTE)
	JASAROVIC	Alisa (0.08 FTE)
	JOMAA	Issam (0.05 FTE)
	KALINICHENKO	Yelyzaveta (0.21 FTE)
	KHATIB	Maha (0.20 FTE)
	KHAZAEI	Somayeh (0.25 FTE)
	KILINÇ	Sena (0.30 FTE)
	KOKMEL	Meliane Angele (0.14 FTE)
	KYRIAZIS	Christos (0.33 FTE)
	LOVATO	Ivan (0.54 FTE)
	MAESTRI	Federica (0.08 FTE)
	MARTINA	Antoine Joseph Dominique (0.33 FTE)
	MAUSSION	Nino (0.19 FTE)
	MILCZAREK	Zofia (0.22 FTE)
	MOREAU	Vidiam (0.56 FTE)
	MOURDI	Elias (0.38 FTE)
	MURUGARAJ	Keerthana (0.61 FTE)
	OLIVIERI	Giovanna Buischi Antunes (0.19 FTE)
	PAIS DA SILVA	Dany Manuel (0.27 FTE)
	PEREHUDA	Yevhen (0.49 FTE)
	POLDRUGO	Alex (0.08 FTE)
	PONAKA	Manasvi (0.50 FTE)
	POST	Micah (0.12 FTE)
	PRAKASH	Harisha (0.34 FTE)
	RADWAN	Ahmed (0.24 FTE)
	RAKOTONDRASOA	Rafidison Santatra (0.21 FTE)
	RONDINELLI	Valentina (0.32 FTE)
	SANYAL	Srinjoy (0.10 FTE)
	SATHEESH	Akhil (0.22 FTE)
	SCHROEDER	Quentin (0.35 FTE)
	SEH NLATE	Daniel (0.38 FTE)
	SHOJAEE	Nooshin (0.99 FTE)
	SPADONI	Gabriel Sergio Jalmar (0.41 FTE)
	SYRUS	Abir (0.03 FTE)

Category	Last Name	First Name
	TAJIK	Mohammad Ebrahim (0.66 FTE)
	THEBAULT	Antoine (0.32 FTE)
	TON	Eugène (0.05 FTE)
	UCAK	Umut (0.47 FTE)
	VAFAEI	Navid (0.60 FTE)
	VARADHARAJAN	Vanitha (0.41 FTE)
	VATANPOUR	Mansour (0.71 FTE)
	VATAVU	Sara-Elena (0.07 FTE)
	ZHAKUDAYEVA	Arnagul (0.62 FTE)
	ŁYSAK	Filip Tomasz (0.16 FTE)

A P P E N D I X F

List of Acronyms

ComSys: Communicative Systems Laboratory
DCS: Department of Computer Science
FNR: Fonds National de la Recherche Luxembourg
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

https://dcs.uni.lu

Department of Computer Science (DCS)
University of Luxembourg
Faculty of Science, Technology and Medecine
6, avenue de la Fonte
L-4364 Esch-sur-Alzette
Luxembourg

Administrative Contact:

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