ESORICS 2019

WORKSHOPS

Welcome Message from the Chairs

On behalf of the Organizing Committee, we would like to welcome you to the collocated workshops of the 24th European Symposium on Research in Computer Security (ESORICS 2019). The organization of the workshops would not have been possible without the dedicated efforts of many individuals and organizations. To name them all in this short message is not possible. However, we would like to thank everyone who has given her or his time, energy and ideas to make this event possible. This includes the organizers of every individual workshop; the authors for providing the content of their respective programs; the PC members and external reviewers, who worked in reviewing papers and providing feedback to the authors; and all the external and local volunteers who selflessly assisted the organizers. We would like to thank as well, all our distinguished invited speakers, who agreed to provide the keynotes of the different workshop sessions.

We are delighted to have you here and we hope you find the program to be a rewarding learning and partnership experience. We also hope that you will get a chance to enjoy your visit to Luxembourg.

Joaquin Garcia-Alfaro
Workshop Chair for ESORICS 2019

Peter Y A Ryan
General Chair for ESORICS 2019

Peter B Roenne
Organisation Chair for ESORICS 2019

Program at a glance

Thursday, September 26, 2019

Workshop	CBT	CyberICPS+SPOSE+SECPRE	DPM	FINSEC+IOSEC+MSTEC	STAST	SIoT+ADIoT	STM
08:00 - 08:30	Registration	Registration	Registration	Registration	Registration	Registration	Registration
08:30 - 08:45	Registration	Registration	Registration	Registration	Registration	Registration	Registration
08:45 - 9:00	Welcome & Keynote Room Schengen II	Welcome & Keynote Room Hollenfels	Welcome & Keynote Room Schengen II	Welcome & Keynote Room Diekirch	Welcome & Keynote Room Vianden	Welcome & Session 1 Room Fischbach	Welcome & Keynote 1 Room Schengen II
09:00 - 10:00							
10:00 - 10:30	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break
10:30 - 11:00	Session 1 Room Schengen II	Session 1 Room Hollenfels	Session 1 Room Schengen I	Session 1 Room Diekirch	Session 1 Room Vianden	Session 2 Room Fischbach	Session 1 Room Wiltz
11:00 - 11:30							
11:30 - 12:00							
12:00 - 13:00	Lunch Break	Lunch Break	Lunch Break	Lunch Break	Lunch Break	Lunch Break	Lunch Break
13:00 - 13:30							
13:30 - 14:00	Session 2 Room Schengen II	Session 2 Room Hollenfels	Session 2 Room Schengen I	Session 2 Room Diekirch	Session 2 Room Vianden	Session 3 Room Fischbach	Session 2 Room Wiltz
14:00 - 14:30							
14:30 - 15:00							
15:00 - 15:30	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break
15:30 - 16:00	Session 3+Keynote Room Schengen II	Session 3 Room Hollenfels	Session 3 Room Schengen I	Session 3 Room Diekirch	Session 3 Room Vianden	Session 4 Room Fischbach	Session 3+ERCIM STM PhD Award Talk Room Wiltz
16:00 - 16:30							
16:30 - 17:00							
17:30 - 18:30	Social Activity	Social Activity	Social Activity	Social Activity	Social Activity	Social Activity	Social Activity
18:30 - 19:30							
19:30 - 20:30							
20:30 - 21:00	Gala Dinner	Gala Dinner	Gala Dinner	Gala Dinner	Gala Dinner	Gala Dinner	Gala Dinner
21:00 - 22:00							

Friday, September 27, 2019

Workshop	CBT	CyberICPS+SPOSE+SECPRE	FINSEC+IOSEC+MSTEC	ETAA	STM
08:45 - 09:00	Registration	Registration	Registration	Registration	Registration
09:00 - 09:30	Keynote Room Schengen II	Session 4 Room Hollenfels	Keynote 2 Room Diekirch	Welcome & Keynote Room Vianden	Keynote 2 Room Wiltz
09:30 - 10:00					
10:00 - 10:30	Coffee Break		Coffee Break	Coffee Break	
10:30 - 11:00	Session 4 Room Schengen II	Coffee Break		Session 1 Room Vianden	Coffee Break
11:00 - 11:30		Session 5 Room Hollenfels	Session 4 Room Diekirch		Session 4 Room Wiltz
11:30 - 12:15					
12:15 - 12:30					
12:30 - 13:00		Lunch Break	Lunch Break	Lunch Break	Farewell Lunch
13:00 - 13:30	Farewell Lunch				
13:30 - 14:00				Session 2 Room Vianden	
14:00 - 14:30		Session 6 Room Hollenfels	Session 5 Room Diekirch		
14:30 - 15:00					
15:00 - 15:30					
15:30 - 16:00			Coffee Break	Coffee Break	
16:00 - 16:30		Farewell Coffee	Session 6 & Farewell Room Diekirch	Session 3 & Farewell Room Vianden	
16:30 - 17:00					
17:30 - 18:00					

Keynote Speakers

Arthur Gervais

Imperial College London
South Kensington, London SW7 2AZ, UK

Title: Off Blockchain Protocols
Date: Thursday, September 26, 2019
Hour: 09:00
Room: Schengen II
Workshops: CBT, DPM, STM

Abstract

A plethora of recent research works have demonstrated different mechanisms on how to perform blockchain transactions without writing every single interaction to the underlying ledger. Instead, these protocols utilize the expensive and low-rate blockchain only as a recourse for disputes. Off-chain protocols promise to complete transactions in sub-seconds rather than minutes or hours while retaining asset security, reducing fees and allowing blockchains to scale. This talk will explore the various lines of research covering off-chain transactions. We will discuss their security and privacy provisions and identify unsolved challenges, indicating promising avenues of future work.

Short Biography

Arthur Gervais is a Lecturer (equivalent Assistant Professor) of Computer Science at Imperial College London. Gervais's research focuses on applied cryptography, network and distributed ledger security, privacy as well as their scalability properties. He was the first to objectively compare the security properties of different proof of work blockchains, and further outlining the tensions between scalability and security. With "Do you need a Blockchain?", he built a widely adopted framework to understand objectively if a blockchain is indeed the appropriate technical solution to a problem. Gervais co-founded two startups in the blockchain space. *Liquidity.Network*, where he acts as CEO, develops a second layer scaling solution to enable higher transaction throughputs on existing blockchains. For *ChainSecurity*, Gervais helped to design the first automated formal smart contract security verification tool Securify.ch. Gervais served on many program committees including top-tier academic security conferences such as ACM CCS. Gervais co-organized the inaugural *CryptoValley Conference in Zug* and he advises the blockchain observatory forum of the European Union.

Keynote Speakers (cont.)

Rainer Böhme

University of Innsbruck

Innsbruck, Austria

Title: Finality from Proof-of-Work Quorums
Date: Friday, September 27, 2019
Hour: 09:00
Room: Schengen II
Workshop: CBT

Abstract

We challenge the widely held belief that proof-of-work enables truly permissionless decentralized systems, but the price to pay is that state updates are never final. We propose HotPoW, a scalable permissionless distributed log protocol, as a positive example to support our claim that it is possible to build permissionless consensus protocols ***with*** finality based on proof-of-work. HotPoW adapts the three-phase commit pipeline recently presented in HotStuff (PODC 2019; used in LibraBFT) by relying on the stochastic uniqueness of proof-of-work quorums, a new theoretical concept for protocol design. We position HotPoW in the design space of consensus protocols and evaluate it with nodes that implement adversarial modifications. The protocol can tolerate network latency, churn, and targeted attacks on consistency and liveness at small overhead compared to Nakamoto consensus. We invite the community to prove our claim wrong, and provide running code to facilitate this task.

Short Biography

Rainer Böhme is professor of Computer Science at the University of Innsbruck and head of the Security and Privacy Laboratory. He is a pioneer of interdisciplinary cryptocurrency research and co-founder of one of the leading academic venues in Bitcoin and blockchain research. He served as spokesperson of the German BITCRIME research project (2014-2017) and is principal investigator in the European Commission's Horizon 2020 project TITANIUM (2017-2020) as well as in the VIRTCRIME research project (2018-2019) funded by the Austrian government.

Keynote Speakers (cont.)

Joseph Bonneau
New York University, USA

Title: Compact Blockchains & Proofs-of-Necessary Work
Date: Thursday, September 26, 2019
Hour: 15:45
Room: Schengen II
Workshop: CBT

Abstract

Incrementally verifiable computation can produce a short proof that an *entire* blockchain history is correct. This enables even light clients to track the blockchain efficiently with minimal trust assumptions. The main challenge is to incentivize creating these proofs. This talk will overview the challenges and possible solutions for solving this incentive problem in a proof-of-work setting by having proof creation double as a proof-of-work puzzle.

Short Biography

Joseph holds a Bachelor of Science and Master of Science from Stanford University. In 2012 he received a Doctor of Philosophy in Computer science from University of Cambridge. He started his career in 2007 as a Cryptographic Scientist at Cryptography Research, Inc. From 2012 to 2014 he worked as a Software Engineer at Google. From 2015 to 2017 he was a Technology Fellow at Electronic Frontier Foundation. Since 2017 Joseph has been an Assistant Professor at New York University.

Keynote Speakers (cont.)

Felix Günther

UC San Diego

Title: A Cryptographic Perspective on TLS 1.3: Modeling Advanced Protocol Security
Date: Thursday, September 26, 2019
Hour: 15:45
Room: Wiltz
Workshop: STM (PhD award talk)

Abstract

Secure communication links are at the heart of today's Internet infrastructure, and cryptographic protocols form their security core. Increasing demands for highest efficiency and stronger security have over the past years led to the standardization of novel and revised protocol designs, prominently Google's QUIC protocol and the new TLS 1.3 standard. In this talk, I will discuss the road to TLS 1.3 from a cryptographic perspective and show how advanced cryptographic modeling can contribute to security standardization.

Short Biography

Felix Günther is a postdoctoral researcher in the Security and Cryptography group at UC San Diego, working with Mihir Bellare. He obtained his Ph.D. from TU Darmstadt in 2018. His research interests are in applied cryptography enabling computer security, with a particular focus on provable security. His work aims to narrow the gap between the theoretical understanding and practical security of real-world cryptographic systems.

Keynote Speakers (cont.)

Joshua Guttman

Worcester Polytechnic Institute,
Massachusetts, USA

Title: A Cut Principle for Information Flow
Date: Friday, September 27, 2019
Hour: 09:00
Room: Wiltz
Workshop: STM

Abstract

We view a distributed system as a graph of active locations with unidirectional channels between them, through which they pass messages. In this context, the graph structure of a system constrains the propagation of information through it.

Suppose a set of channels is a cut set between an information source and a potential sink. We prove that, if there is no disclosure from the source to the cut set, then there can be no disclosure to the sink. We introduce a new formalization of partial disclosure, called *blur operators*, and show that the same cut property is preserved for disclosure to within a blur operator. A related compositional principle ensures limited disclosure for a class of systems that differ only beyond the cut.

Short Biography

Dr. Joshua Guttman is a Senior Principal Scientist at the MITRE Corporation, and Research Professor at Worcester Polytechnic Institute. He has focused on security foundations and applications, including cryptographic protocol analysis and design, network security, operating systems security, and information flow. Dr. Guttman has written extensively, with about 75 academic publications, and regularly serves on program committees and proposal evaluations. He was educated at Princeton and the University of Chicago.

Keynote Speakers (cont.)

Sascha Fahl
Leibniz University
Hannover, Germany

Title: A Holistic Approach to Secure Programming and Usable Security Research
Date: Thursday, September 26, 2019
Hour: 09:00
Room: Vianden
Workshop: STAST

Abstract

In the age of digitalization, we see a persistent gap between the theoretical security of e.g., cryptographic algorithms and real-world vulnerabilities, data breaches, and possible attacks. As a result, secure programming and usable security challenges impact all actors involved in the creation and use of technology, ranging from system designers across administrators and developers to end-users. To successfully prevent involuntary loss of control over data and empower end-users to retain power over their security, we must take all involved actors into account. It is crucial to find the weak points and empowering all actors to strengthen the overall security. For end-users, this means e.g., working with warning messages, security indicators, and authentication mechanisms; for developers, improving APIs, documentation and developer tools; for system administrators, improving configuration languages and tools. In this talk, I demonstrate how a holistic approach to usability and secure programming helps close the gap between theoretical security and real-world deployments.

Short Biography

Professor for Usable Security and Privacy at Leibniz University Hannover in Germany. Previously, he was Professor at Ruhr University Bochum, Germany, held the chair for Information Security at Leibniz University Hannover and was an independent research group leader at CISPA, Saarland University. Prof. Fahl studied Computer Science at Philipps University Marburg and received a Ph.D. in Computer Science. He worked with the Chrome Security team and was a researcher at Fraunhofer FKIE in Bonn. His research won the NSA's best Scientific Cybersecurity Paper Competition, he received a Google Faculty Research Award and is a recipient of the Heinz Maier-Leibnitz Prize 2018.

Keynote Speakers (cont.)

Katharina Krombholz

CISPA, Helmholtz Center for Information Security
Saarbrücken, Germany

Title: A User-Centric Approach to Secure the Internet Ecosystem
Date: Thursday, September 26, 2019
Hour: 09:00
Room: Hollenfels
Workshop: CyberICPS-SECPRE-**SPOSE**

Abstract

Fortunately, cryptographic protocols have become more pervasive in today's Internet ecosystem. However, a significant number of websites and IoT devices are still not sufficiently secured as even knowledgeable experts struggle with making informed security decisions. In the course of my group's interdisciplinary research agenda, we study mental models of cryptographic tools and protocols and build more user-friendly interaction mechanisms that help to construct meaningful mental models of the underlying. Our recent study on mental models of HTTPS has shown that even knowledgeable users have sparse (and sometimes even wrong) mental models of the protocol that are mostly protocol-based instead of conceptional. These results suggest that ultimately poor protocol and API design contributes to such a lack of understanding which results in vulnerable configurations and code, posing millions of Internet users at risk. To what extend should administrators and developers be required understand the cryptographic fundamentals? Who is ultimately responsible for these vulnerabilities? And what can we do to make sure that the security technology we design is used in the most secure manner?

Short Biography

Katharina Krombholz is faculty at the CISPA Helmholtz Center for Information Security in Saarbrücken, Germany where she leads the Usable Security Research Group. Before that, she was senior researcher at SBA Research in Vienna, Austria and lecturer at various institutions in Vienna, Austria. Her research interests are human-centric aspects of IT security ranging from studies on how different types of users interact with security technology to designing user-friendly security and privacy technology.

Keynote Speakers (cont.)

Vasilis Prevelakis

AEGIS IT RESEARCH UG, Germany

Title: Friend or Foe? Incident Characterization Techniques
Date: Thursday, September 26, 2019
Hour: 09:00
Room: Diekirch
Workshop: IOSEC-MSTEC-FINSEC

Abstract

In 2006 a number of undelivered SMSs initiated a routine troubleshooting investigation which led to the discovery of a large scale compromise in Vodafone/Greece's mobile network. Clearly this off-nominal event was mischaracterized as routine, delaying the response to the infiltration by several months. It is thus understandable why off-nominal events are always a source of concern. In complex environments, however, it may be very difficult to determine the exact cause of a disturbance and determine whether the cause was due to bugs, inappropriate configuration, human error, unforeseen circumstances, or an attack. The effort involved in dealing with an attack is usually significant and while rapid reaction usually prevents the attack from spreading, mobilizing the appropriate assets when in fact there is no attack can become very expensive, while blunting the readiness of the defense team. Hence the need for quick and reliable event characterization.

In this talk we look at how visualization tools can help in characterizing events by providing information in the correct context and in a way that can be quickly and correctly processed by the security analysts. The discussion applies equally to live and after-the-fact forensic analysis.

Short Biography

Dr. Vassilis Prevelakis is professor of Embedded Computer Security at the Technical University, Braunschweig, in Germany. He is also Director of Research at AEGIS IT SECURITY UG a research and development company headquartered in Germany. He has worked in various areas of security in Systems and Networks both in his current academic capacity and as a freelance consultant. Prevelakis current research involves issues related to vehicular security, embedded systems security, automation network security, secure software design, auto-configuration issues in secure VPNs, etc. He has published numerous papers in these areas and is actively involved in standards bodies such as the IETF. He has received research funding from the European Union, the German DFG and US funding agencies such as DARPA and NSF. He was awarded the CAREER award from NSF and recently received the "Test of Time" award at CCS'13 for his work on Instruction Set Randomization.

Prevelakis received his Ph.D. from the University of Geneva in Switzerland and his M.Sc. and B.Sc. from the University of Kent in the U.K..

Keynote Speakers (cont.)

Rocco Mammoliti
Poste Italiane, Italy

Title: Cybersecurity for the Protection of Critical Infrastructures
Date: Friday, September 27, 2019
Hour: 09:00
Room: Diekirch
Workshop: IOSEC-MSTEC-**FINSEC**

Abstract

In recent years, the number of cyber-attacks on public and private institutions has increased considerably, with serious consequences for businesses and customers who are victims of such attacks. Cyber incidents, in fact, in addition to affecting a company's ability to generate profits, can lead to severe legal and reputational damages. The change in digital threats, the diversification of attack techniques and the extension of violations to an increasing number of organizations, therefore pushes them to defend themselves against the real risk of being a victim of cyber-attacks. In particular, for Financial Critical Infrastructures it is of primary importance to constantly assess the degree of exposure to cyber threats of its technological infrastructures through which they manage data/information, support critical business processes and provide services and products to its customers. Until today the traditional Risk Analysis methodologies have not taken into consideration the results coming from the technical security checks through which it is possible to identify technological vulnerabilities that can be exploited by cyber criminals to perpetrate cyber-attacks. The amount of information available from these security technical activities, allows to calculate in a more objective and measurable way over time the level of cyber risk to which a company is exposed. In this talk, we will report work and experience carried out at Poste Italiane to define a methodology for evaluating Cyber Risk.

Short Biography

Rocco Mammoliti holds more than 25 years of experience in Information Security, Risk Management & Cybersecurity fields. Currently he's Poste Italiane Group Chief Information Security Manager. He's founder of PI-CERT (Poste Italiane Computer Emergency Response Team) and of Cybersecurity Technological District; he was responsible of EECTF (European Electronic Cybercrime Task Force) and General Director of GCSEC (Global Cyber Security Center). RM was CISO in Telecom Italia, IT Security Manager in Telecom Italia Information Technology, Technology Officer at Evidian-Bull–Italy and Security Consultant for different Private and Public Institutions. He hold a master degree in Electronic Engineering and he carried out extensive research activities at the CNR, working on computer security, cryptography, time series analysis and forecasting, multivariate statistical analysis. He also holds a Master's Degree in International Security Advanced Studies, Centre for Defense Higher Studies (CASD). He's coordinator of different EU R&D Projects (Horizon2020, EIT Digital), author of more than 40 scientific publications, member of different Italian and EU information security working group, senior member of IEEE, Computer Society and IEEE Biomedical Engineers.

Keynote Speakers (cont.)

Alessandro Aldini
University of Urbino, Italy

Title: Logics to reason formally about trust computation and manipulation
Date: Friday, September 27, 2019
Hour: 09:00
Room: Vianden
Workshop: ETAA

Abstract

Trust represents a fundamental ingredient for the widespread use of security mechanisms in computer science, as it goes beyond the intrinsic, technical aspects of cybersecurity, by involving the subjective perception of users, the willingness to collaborate and expose own resources and capabilities, and the judgement about the expected behavior of other parties. Computational notions of trust are formalized to support automatically the process of building and maintaining trust infrastructures, and mathematical logics provide the formal means to reason about the efficacy of such a process. The objective of this presentation is to discuss two logical approaches to the modeling and verification of the two main steps at the base of any trust infrastructure: the initial computation of trust values and the dynamic manipulation of such values.

Short Biography

Alessandro Aldini is Associate Professor in Computer Science at the University of Urbino Carlo Bo, Italy. He is member of the Scientific Committee of the International School on Foundations of Security Analysis and Design (FOSAD) and of the IFIP WG 11.14 on Secure Engineering. His research interests are focused on the study and application of automated methodologies for the design and verification of computer and network systems, with an emphasis on foundations of security, trust, and performance analysis and design.

CBT: Cryptocurrencies and Blockchain Technology

Thursday, September 26, 2019

08:00 – 08:45

Registration

08:45 – 10:00

Room: Schengen II
General Welcome & Invited Talk I
Chairs: Joaquin Garcia-Alfaro & Alex Biryukov
Invited Talk Title: *Off Blockchain Protocols*
Speaker: Arthur Gervais, Imperial College London, UK

10:00 – 10:30

Coffee Break

10:30 – 12:00

Session 1: Lightning Networks and Short Papers

Room: Schengen II
Chair: Rainer Böhme, University of Innsbruck, Austria

TEE-Based Distributed Watchtowers for Fraud Protection in the Lightning Network, *By Marc Leinweber, Matthias Grundmann, Leonard Schönborn and Hannes Hartenstein*

Payment Networks as Creation Games, *By Georgia Avarikioti, Rolf Scheuner and Roger Wattenhofer*

Short Papers

An Efficient Micropayment Channel on Ethereum, *By Hisham Galal, Muhammad Elsheikh and Amr Youssef*

Extending Atomic Cross-Chain Swaps, *By Jean Yves Zie, Jérémy Briffaut, Benjamin Nguyen and Jean-Christophe Deneuville*

12:00 – 13:30

Lunch Break

13:30 – 14:45

Session 2: Smart Contracts and Applications

Room: Schengen II
Chair: Hannes Hartenstein, KIT, Germany

The Operational Cost of Ethereum Airdrops, *By Michael Fröwis and Rainer Böhme*

Blockchain Driven Platform for Energy Distribution in a Microgrid, *By Arjun Choudhry, Ikechukwu Dimobi and Zachary Gould*

Practical Mutation Testing for Smart Contracts, *By Joran Honig, Maarten Everts and Marieke Huisman*

14:45 – 15:15

Coffee break

15:15 – 16:45

Session 3: Payment Systems & Invited Talk II

Room: Schengen II
Chair: Joaquin Garcia-Alfaro, Télécom SudParis, France

Online Payment Network Design, *By Georgia Avarikioti, Kenan Besic, Yuyi Wang and Roger Wattenhofer*

Invited Talk II

Title: *Compact Blockchains & Proofs-of-Necessary Work*
Speaker: Joseph Bonneau, New York University, USA

17:00 – 20:30

Social Activity

20:30 – 22:00

Gala Dinner

Friday, September 27, 2019

09:00 – 10:00

Invited Talk III

Room: Schengen II
Chair: Alex Biryukov, University of Luxembourg, Luxembourg
Invited Talk Title: *Finality from Proof-of-Work Quorums*
Speaker: Rainer Böhme, University of Innsbruck, Autria

10:00 – 10:30

Coffee break

10:30 – 13:00

Session 4: Privacy, Mining and Short papers

Room: Schengen II
Chair: Guillermo Navarro, Universitat Autonoma de Barcelona

Simulation Extractability in Groth's zk-SNARK, *By Shahla Atapoor and Karim Baghery*

Auditable Credential Anonymity Revocation Based on Privacy-Preserving Smart Contracts, By Rujia Li, David Galindo and Qi Wang

Bonded Mining: Difficulty Adjustment by Miner Commitment, *By George Bissias, David Thibodeau and Brian Levine*

A Multi-Protocol Payment System to Facilitate Financial Inclusion, *By Kazım Rıfat Özyılmaz, Nazmi Berhan Kongel, Ali Erhat Nalbant and Ahmet Özcan*

Short Papers

12 Angry Miners (Short Paper), *By Aryaz Eghbali and Roger Wattenhofer*

A minimal core calculus for Solidity contracts, *By Massimo Bartoletti, Letterio Galletta and Maurizio Murgia*

Multi-Stage Contracts in the UTXO Model, *By Alexander Chepurnoy and Amitabh Saxena*

13:00 – 14:00

Farewell Lunch

CyberICPS-SECPRE-SPOSE: Security of Industrial Control Systems and of Cyber-Physical Systems — Security and Privacy Requirements Engineering — Security, Privacy, Organizations, and Systems Engineering

Thursday, September 26, 2019

08:00 – 08:45

Registration

08:45 – 10:00

General Welcome & Invited Talk
Chair: Angela Sasse - Ruhr-Universität Bochum, Germany
Invited Talk Title: *A User-Centric Approach to Secure the Internet Ecosystem*
Speaker: Katharina Krombholz, Helmholtz Center for Information Security, Germany
Room: Hollenfels

10:00 – 11:00

Coffee Break

11:00 – 12:00

Session 1: Human-Organizational Issues of Security and Privacy

Room: Hollenfels
Chair: Jörg Pohle, Alexander von Humboldt Institute for Internet and Society (HIIG), Germany / Frank Pallas, Technische Universität Berlin, Germany

On the trade-off between privacy and utility in mobile services: A qualitative study, By Yang Liu and Andrew Simpson.

Discrete Event Simulation of Jail Operations in Pursuit of Organizational Culture Change, By Hugh Lester and Martin Miller.

12:00 – 13:30

Lunch Break

13:30 – 15:00

Session 2: Decision making and Automation in the Context of Security & Privacy

Room: Hollenfels

Chair: Frank Pallas, Technische Universität Berlin, Germany

Analysis of Automation Potentials in Privacy Impact Assessment Processes, By Jan Zibuschka.

An Insight into Decisive Factors in Cloud Provider Selection with a Focus on Security, By Sebastian Pape and Jelena Stankovic.

Shaping Digital Identities in Social Networks: Data Elements and the Role of Privacy Concerns, By Thanos Papaioannou, Aggeliki Tsohou and Maria Karyda.

15:00 – 15:15

Coffee Break

15:15-16:45

Session 3: GDPR Requirements and Compliance Issues

Room: Hollenfels

Chair: Sokratis Katsikas, Norwegian University of Science and Technology, Norway

Privacy, Security, Legal and Technology Acceptance Requirements for a GDPR Compliance Platform*, By Aggeliki Tsohou, Emmanouil Magkos, Haralambos Mouratidis, George Chrysoloras, Luca Piras, Michalis Pavlidis, Julien Debussche, Marco Rotoloni and Beatriz Gallego-Nicasio*

GDPR Compliance: Proposed Technical and Organizational measures for Cloud Providers, *By Zafeiroula Georgiopoulou, Costas Lambrinoudakis and Eleni Laskarina*

From ISO/IEC 27002:2013 Information Security Controls to Personal Data Protection Controls: Guidelines for GDPR Compliance*, By Vasiliki Diamantopoulou, Aggeliki Tsohou and Maria Karyda*

A Proposed Privacy Impact Assessment Method using Metrics based on Organizational Characteristics, *By Eleni Laskarina Makri, Zafeiroula Georgiopoulou and Lambrinoudakis Costas*

17:00 – 20:00

Social Activity

20:00 – 22:00

Gala Dinner

Friday, 27 September 2019

09:00-10:30

Session 4: Challenges on the applicability of security and privacy in various domains: Lessons learned

Room: Hollenfels
Chair: Aggeliki Tsohou, Ionian University, Greece

Uncertainty-Aware Authentication Model for IoT, *By Mohammad Heydari, Alexios Mylonas, Vasilios Katos, Emili Balaguer-Ballester and Vahid Heydari Fami Tafreshi*

On the applicability of security and privacy threat modeling for blockchain applications*, By Dimitri Van Landuyt, Laurens Sion, Emiel Vandeloo and Wouter Joosen*

How not to Use a Privacy-Preserving Computation Platform: Case Study of a Voting Application*, By Jan Willemson*

A modelling language redesign for cyber resiliency of healthcare systems*, By Myrsini Athinaiou, Haralambos Mouratidis, Theo Fotis and Michalis Pavlidis*

10:30 – 11:00

Coffee Break

11:00-12:30

Session 5: Attack detection and mitigation for Cyber Physical Systems

Room: Hollenfels
Chair: Sokratis Katsikas, Norwegian University of Science and Technology, Norway

Anomaly Detection for Industrial Control Systems Using Sequence-to-Sequence Neural Networks, *By Jonguk Kim, Jeong-Han Yun and Hyoung Chun*

Reflective Attenuation of Cyber-Physical Attacks, *By Mariana Segovia, Ana Cavalli, Nora Cuppens, Jose Rubio-Hernan and Joaquin Garcia-Alfaro*

Distributed UCON in CoAP and MQTT Protocols, *By Athanasios Rizos, Daniel Bastos, Andrea Saracino and Fabio Martinelli*

12:30 – 14:00

Lunch Break

14:00-16:00

Session 6: Secure Cyber Physical Systems in Critical Infrastructures)

Room: Hollenfels

Chair: Frédéric Cuppens, IMT Atlantique, France

Towards The Creation of A Threat Intelligence Framework for Maritime Infrastructures, *By Nikolaos Pitropakis, Marios Logothetis, Gennady Andrienko, Jason Stefanatos, Eirini Karapistoli and Costas Lambrinoudakis*

Connect and Protect: Requirements for Maritime Autonomous Surface Ship in Urban Passenger Transportation, *By Ahmed Amro, Sokratis Katsikas and Vasileios Gkioulos*

Simulation-based evaluation of DDoS against Smart Grid SCADAs, *By Damjan Gogić, Bojan Jelačić and Imre Lendák*

Identifying Safety and Human Factors Issues in Rail using IRIS and CAIRIS, *By Amna Altaf, Shamal Faily, Huseyin Dogan, Alexios Mylonas and Eylem Thron*

DPM: Data and Privacy Management

Thursday, September 26, 2019

08:00 – 08:45

Registration

08:45 – 10:00

General Welcome & Keynote (Shared with CBT 2019, Room Schengen II)
Invited Talk Title: *Off Blockchain Protocols*
Speaker: Arthur Gervais, Imperial College London, UK
Room: Schengen II

10:00 – 10:30

Coffee Break

10:30 – 12:00

Session 1: Privacy preserving data analysis

Room: Schengen I
Chair: Julian Salas, Universitat Oberta de Catalunya

Pinfer: Privacy-Preserving Inference, *By Marc Joye (OneSpan), Fabien Petitcolas (OneSpan)*

Integral Privacy Compliant Statistics Computation, *By Navoda Senavirathne (University of Skovde), Vicenç Torra (Maynooth University)*

Towards Data Anonymization in Data Mining via Meta-Heuristic Approaches, *By Fatemeh Amiri (University of Vienna), Gerald Quirchmayr (University of Vienna), Alessio Bertone (TU Dresden), Peter Kieseberg (SBA Research), Edgar Weippl (SBA Research)*

Skiplist Timing Attack Vulnerability, *By Eyal Nussbaum (Ben Gurion University), Michael Segal (Ben Gurion University)*

12:00 – 13:30

Lunch Break

13:30 – 15:00

Session 2: Field/lab studies

Room: Schengen I
Chair: Cristina Perez, Universitat Oberta de Catalunya

A Study on Subject Data Access in Online Advertising after the GDPR, By Tobias Urban (Institute for Internet Security), Dennis Tatang (Ruhr-University Bochum), Martin Degeling (Ruhr-University Bochum), Thorsten Holz (Ruhr-University Bochum), Norbert Pohlmann (Institute for Internet Security)

On Privacy Risks of Public WiFi Captive Portals, By Suzan Ali (Concordia University), Tousif Osman (Concordia University), Mohammad Mannan (Concordia University), Amr Youssef (Concordia University)

User Perceptions of Security and Usability of Mobile-based Single Password Authentication and Two-Factor Authentication, By Devriş İşler (Katholieke Universiteit Leuven), Alptekin Küpçü (Koç University), Aykut Coskun (Koç University)

15:00 – 15:30

Coffee Break

15:30 – 17:00

Session 3: Privacy by design and data anonymization

Room: Schengen I
Chair: Guillermo Navarro, Universitat Autònoma de Barcelona

Towards Minimising Timestamp Usage in Application Software, By Christian Burkert (University of Hamburg), Hannes Federrath (Univeristy of Hamburg)

Card-based Cryptographic Protocols with the Minimum Number of Rounds Using Private Operations, By Hibiki Ono (Kogakuin University), Yoshifumi Manabe (Kogakuin University)

Graph perturbation as noise graph addition: a new perspective for graph anonymization, By Julián Salas (Universitat Oberta de Catalunya), Vicenç Torra (Maynooth University)

17:00 – 20:30

Social Activity

20:30 – 22:00

Gala Dinner

ETAA: Emerging Technologies for Authorization and Authentication

Friday, September 27, 2019

08:45 – 09:00

Registration

09:00 – 10:00

General Welcome & Keynote
Invited Talk Title: Logics to reason formally about trust computation and manipulation
Speaker: Alessandro Aldini, University of Urbino, Italy
Chair: Andrea Saracino, IIT-CNR, Italy
Room: Vianden

10:00 – 10:30

Coffee Break

10:30 – 12:30

Session 1: Authorization solutions and tools

Room: Vianden
Chair: Paolo Mori, IIT-CNR, Italy

An Authorization Framework for Cooperative Intelligent Transport Systems, By Sowmya Ravidas, Priyanka Karkhanis, Yanja Dajsuren and Nicola Zannone

A Framework for the Validation of Access Control Systems, By Said Daoudagh, Francesca Lonetti and Eda Marchetti

The Structure and Agency Policy Language (SAPL) for Attribute Stream-Based Access Control (ASBAC), By Dominic Heutelbeck

How Efficiently Stop Crypto-Ransomware by Blocking Unauthorized Calls to Strong Pseudo-Random Generators, By Ziya A. Genc, Gabriele Lenzini and Peter Y. A. Ryan

12:30 – 13:30

Lunch Break

13:30 – 15:30

Session 2: Authentication solutions and tools (I)

Room: Vianden

Chairs: Alessandro Aldini, University of Urbino, Italy

Security Requirements for Store-on-Client and Verify-on-Server Secure Biometric Authentication, By Haruna Higo, Toshiyuki Isshiki, Masahiro Nara, Satoshi Obana, Toshihiko Okamura and Hiroto Tamiya

Reflexive Memory Authenticator: a proposal for effortless renewable biometrics, By Nikola K. Blanchard, Siargey Kachanovich, Ted Selker and Florentin Waligorski

Collaborative Authentication using Threshold Cryptography, By Aysajan Abidin, Abdelrahaman Aly and Mustafa A. Mustafa

MuFASA: a tool for high-level specification and analysis of multi-factor authentication protocols, By Federico Sinigaglia, Roberto Carbone, Gabriele Costa and Silvio Ranise

15:30 – 16:00

Coffee Break

16:00 – 17:00

Session 3: Authentication solutions and tools (II)

Room: Vianden

Chairs: Andrea Saracino, IIT-CNR, Italy

A Risk-driven Model to Minimize the Effects of Human Factors on Smart Devices, By Sandeep Gupta, Attaullah Buriro and Bruno Crispo

A formal analysis of a user-friendly authentication protocol for decentralized key distribution and end-to-end encrypted email, By Itzel Vazquez Sandoval and Gabriele Lenzini

IOSEC-MSTEC-FINSEC: Security for Financial Critical Infrastructures and Services — Information & Operational Technology Security Systems — Simulation and Training Environments for Cybersecurity

Thursday, September 26, 2019

08:00 – 08:45

Registration

08:45 – 10:00

Room: Diekirch
General Welcome IOSEC+MSTEC & Opening Keynote
Chairs: Apostolos P. Fournaris & Sotiris Ioannidis
Invited Talk Title: *Cybersecurity for the Protection of Critical Infrastructures*
Speaker: Prof. Vasilis Prevelakis

10:00 – 10:30

Coffee Break

10:30 – 12:00

Session 1: IOSEC (Web-based Attacks & Technologies)

Room: Diekirch
Chair: Konstantinos Lampropoulos

Event-Based Remote Attacks in HTML5-Based Mobile Apps, By Tuong Lau

Web Servers Protection Using Anomaly Detection for HTTP Requests, By Paul Satmarean and Ciprian Oprisa

Secure Data Exchange for Computationally Constrained Devices, By Vassilis Prevelakis, Mohammad Hamad, Jihane Najar and Ilias Spais

You Shall Not Register! Detecting Privacy Leaks across Registration Forms, By Manolis Chatzimpyrros, Konstantinos Solomos and Sotiris Ioannidis

12:00 – 13:30

Lunch Break

13:30 – 14:45

Session 2: IOSEC (SME Security)

Room: Diekirch
Chair: Vasilis Prevelakis

Horizontal Attacks against ECC: from Simulations to ASIC, By Ievgen Kabin, Zoya Dyka, Dan Klann and Peter Langendoerfer

Deploying Fog-to-Cloud Towards a Security Architecture for Critical Infrastructure Scenarios, By Sarang Kahvazadeh, Xavi Masip-Bruin, Pau Marcer and Eva Marín-Tordera

A comprehensive technical survey of contemporary cybersecurity products and solutions, By Christos Tselios, George Tsolis and Manos Athanatos

CyberSure: A Framework for Liability Based Trust, By George Christou, Eva Papadogiannaki, Michalis Diamantaris, Livia Torterolo and Panos Chatziadam

14:45 – 15:15

Coffee Break

15:15 – 16:45

Session 3: MSTEC (Introduction & Cyber Range Platforms)

Room: Diekirch
Chair: Sotiris Ioannidis

The THREAT-ARREST Cyber-Security Training Platform, By Othonas Soultatos, Konstantinos Fysarakis, George Spanoudakis, Hristo Koshutanski, Ernesto Damiani, Kristian Beckers, Dirk Wortmann, George Bravos, and Menelaos Ioannidis

An Open and Flexible CyberSecurity Training Laboratory in IT/OT Infrastructures, By Umberto Morelli, Lorenzo Nicolodi, Silvio Ranise

Model-driven Cyber Range Training - The Cyber Security Assurance Perspective, By Iason Somarakis, Michail Smyrlis, Konstantinos Fysarakis, and George Spanoudakis

A model-driven approach for cyber security scenarios deployment, Chiara Braghin, By Stelvio Cimato, Ernesto Damiani, Fulvio Frati, Lara Mauri, Elvinia Riccobene

17:00 – 20:30

Social Activity

20:30 – 22:00

Gala Dinner

Friday, September 27, 2019

09:00 – 10:30

Session 4: MSTEC (System Assurance & Training)

Room: Diekirch
Chair: Sotiris Ioannidis

Towards the Insurance of Healthcare Systems, By George Hatzivasilis, Panos Chatziadam, Andreas Miaoudakis, Eftychia Lakka, Alessia Alessio, Michail Smyrlis, George Spanoudakis, Artsiom Yautsiukhin, Michalis Antoniou, Nikos Stathiakis

Difficult XSS Code Patterns for Static Code Analysis Tools, By Felix Schuckert, Basel Katt, Hanno Langweg

PROTECT — An Easy Configurable Serious Game to Train Employees Against Social Engineering, By Ludger Goeke, Alejandro Quintanar, Kristian Beckers, Sebastian Pape

10:30 – 11:00

Coffee Break

11:00 – 12:00

Session 5: FINSEC (Introduction to the Workshop)

Room: Diekirch
General Welcome FINSEC & Keynote 2
Chairs: Habtamu Abie & Silvio Ranise
Invited Talk Title: *Cybersecurity for the Protection of Critical Infrastructures*
Speaker: Rocco Mammoliti, Poste Italiane

12:00 – 13:00

Lunch Break

13:00 – 15:00

Session 6: FINSEC (Identification, Mitigation, and Threats Mapping)

Room: Diekirch
Chair: Silvio Ranise & Habtamu Abie

Bunkers: Jail application level firewall for the mitigation and identification of service takeover attacks on HardenedBSD, By Alin-Adrian Anton and Razvan-Dorel Cioarga

A Language-Based Approach to Prevent DDoS Attacks in Distributed Financial Agent Systems, By Elahe Fazeldehkordi, Olaf Owe and Toktam Ramezanifarkhani

Blockchain based Sharing of Security Information for Critical Infrastructures of the Finance Sector, By Ioannis Karagiannis, Kostis Mavrogiannis, John Soldatos and Ariana Polyviou

dAPTaset: a Comprehensive Mapping of APT-related Data, By Giuseppe Laurenza and Riccardo Lazzeretti

15:00 – 15:30

Coffee Break

15:30 – 17:00

Session 7: FINSEC (Preliminary Projects Results)

Room: Diekirch
Chairs: Luca Verderame & Silvio Ranise

- **FINSEC Project (https://www.finsec-project.eu/), By Habtamu Abie**
- **DEFENDER (http://defender-project.eu/), By Dusan Gabrijelcic**
- **ANASTACIA Project (http://anastacia-h2020.eu/), By Stefano Bianchi**

SIOT-ADIOT: Secure Internet of Things — Attacks and Defenses for Internet-of-Thing

08:00 – 08:45

Registration

08:45 – 09:00

General Welcome
Room: Fischbach
Chairs: Alfredo RIAL & Weizhi Meng

09:00 – 10:00

Session 1: SIOT-I

Chair: Alfredo RIAL, University of Luxembourg, Luxembourg
Room: Fischbach

Finding Security Vulnerabilities in Unmanned Aerial Vehicles Using Software Verification, By Omar M. Alhawi, Mustafa A. Mustafa and Lucas C. Cordeiro

Automated Fuzzing of Automotive Control Units, By Timothy Werquin, Mathijs Hubrechtsen, Ashok Thangarajan, Frank Piessens and Jan Tobias Muehlberg

10:00 – 10:30

Coffee break

10:30 – 12:00

Session 2: SIOT-II

Chair: Alfredo RIAL, University of Luxembourg, Luxembourg
Room: Fischbach

Fast ECDH Key Exchange Using Twisted Edwards Curves with an Efficiently Computable Endomorphism, By Johann Groszschaedl

liOS: Lifting iOS Apps for Fun and Profit, By Julian Schütte and Dennis Titze

TIO - Secure Input/Output for Intel SGX Enclaves, By Florin-Alexandru Stancu, Dumitru Tranca and Mihai Chiroiu

12:00 – 13:30

Lunch Break

13:30 – 15:00

Session 3: ADIOT-I

Chair: Budi Arief, University of Kent, UK
Room: Fischbach

A Basic Theory of Lightweight Hierarchical Key Predistribution Scheme, By Deepak Kumar Dalai

Adversarial Examples for Hardware-Trojan Detection at Gate-Level Netlists, By Kohei Nozawa, Kento Hasegawa, Seira Hidano, Shinsaku Kiyomoto, Kazuo Hashimoto and Nozomu Togawa

Anomaly Detection in the HVAC System Operation by a RadViz Based Visualization-Driven Approach, By Evgenia Novikova, Mikhail Bestuzhev and Igor Kotenko

14:45 – 15:15

Coffee break

15:15 – 16:45

Session 4: ADIOT-II

Chair: Dennis Tatang, Ruhr University Bochum, Germany
Room: Fischbach

Denial-of-Service Attacks and Countermeasures in the RPL-Based Internet of Things, By Philokypros Ioulianou and Vassilios Vassilakis

Secure Location Verification: Why You Want Your Verifiers to be Mobile, By Matthias Schafer, Carolina Nogueira, Jens B. Schmitt, and Vincent Lenders

Selective Forwarding Attack on IoT Home Security Kits, By Ali Hariri, Nicolas Giannelos and Budi Arief

Study of DNS Rebinding Attacks on Smart Home Devices, By Dennis Tatang, Tim Suurland and Thorsten Holz

17:00 – 20:30

Social Activity

20:30 – 22:00

Gala Dinner

STAST: Socio-Technical Aspects in SecuriTy

Thursday, September 26, 2019

08:00 – 08:45

Registration

08:45 – 10:00

Room: Vianden
General Welcome & Keynote
Chairs: Giampaolo Bella & Gabriele Lenzini
Invited Talk Title: *A Holistic Approach to Secure Programming and Usable Security Research*
Speaker: Sascha Fahl

10:00 – 10:30

Coffee Break

10:30 – 12:00

Session 1: METHODS FOR SOCIOTECHNICAL SYSTEMS

Room: Vianden

Fidelity of Statistical Reporting in 10 Years of Cyber Security User Studies, By Thomas Gross

"I Don't Know Too Much About It": On the Security Mindsets of Computer Science Students, By Mohammad Tahaei, Adam Jenkins, Kami Vaniea and Maria Wolters

Data, data, everywhere: quantifying software developers' privacy attitudes, By Dirk van der Linden, Irit Hadar, Matthew Edwards and Awais Rashid

You've left me no choices: Security economics to inform behavior intervention support in organizations, By Albese Demjaha, Simon Parkin and David Pym

12:00 – 13:30

Lunch Break

13:30 – 15:00

Session 2: SYSTEMS SECURITY

Room: Vianden

What We Know About Bug Bounty Programs - an Exploratory Systematic Mapping Study, By Ana Magazinius, Niklas Mellegård and Linda Olsson

Association Attacks in IEEE 802.11: Exploiting WiFi Usability Features, By George Chatzisofroniou and Panayiotis Kotzanikolaou

A Security Analysis of the Danish Deposit Return System, By Ivan Garbacz, Rosario Giustolisi, Kasper Møller Nielsen and Carsten Schuermann

Moving to client-sided hashing for online authentication, By Nikola K. Blanchard, Xavier Coquand and Ted Selker

15:00 – 15:30

Coffee break

15:30 – 17:00

Session 3: PRIVACY CONTROLS

Room: Vianden

A Privacy-Preserving Infrastructure for Driver's Reputation Aware Automotive Services, By Gianpiero Costantino, Fabio Martinelli, Ilaria Matteucci and Paolo Santi

Case study: Disclosure of indirect device fingerprinting in privacy policies, By Julissa Milligan, Sarah Scheffler, Andrew Sellars, Trishita Tiwari, Ari Trachtenberg and Mayank Varia

Investigating the Effect of Incidental Affect States on Privacy Behavioural Intention, By Uchechi Phyllis Nwadike and Thomas Gross

Which Properties Has an Icon? A Critical Discussion on Evaluation Methods for Standardised Data Protection Iconography, By Arianna Rossi and Gabriele Lenzini

Farewell & Best Paper Award

17:00 – 20:30

Social Activity

20:30 – 22:00

Gala Dinner

STM: Security and Trust Management

Thursday, September 26, 2019

08:00 – 08:45

Registration

08:45 – 10:00

Room: Schengen II (shared with CBT and DPM)
General Welcome & Keynote 1 (shared with CBT and DPM, Room Schengen II)
Invited Talk Title: *Off Blockchain Protocols*
Speaker: Arthur Gervais

10:00 – 10:30

Coffee Break

10:30 – 12:00

Session 1: Authentication & Risk

Room: Wiltz

Improving Identity and Authentication Assurance in Research & Education Federations, *By Jule Anna Ziegler, Michael Schmidt and Mikael Linden*

Audit-Based Access Control with a Distributed Ledger: Applications to Healthcare Organizations, *By Umberto Morelli, Silvio Ranise, Damiano Sartori, Giada Sciarretta and Alessandro Tomasi*

Is a Smarter Grid Also Riskier? *By Karin Bernsmed, Martin Gilje Jaatun and Christian Frøystad*

12:00 – 13:30

Lunch Break

13:30 – 15:00

Session 2: Protocols

Room: Wiltz

BioID: a Privacy-Friendly Identity Document, *By Fatih Balli, F. Betül Durak and Serge Vaudenay*

On the Statistical Detection of Adversarial Instances over Encrypted Data, *By Mina Sheikhalishahi, Fabio Martinelli, Zeki Erkin and Majid Nateghizad*

Understanding Attestation: Analyzing Protocols that use Quotes, *By Joshua Guttman and John Ramsdell*

15:00 – 15:30

Coffee break

15:30 – 17:00

Short paper session & STM PhD award talk

Room: Wiltz

An OBDD-based Technique for the Efficient Synthesis of Garbled Circuits, By *Stelvio Cimato, Valentina Ciriani, Ernesto Damiani and Maryam Ehsanpour*

STM PhD award talk, *By Felix Günther*

17:00 – 20:30

Social Activity

20:30 – 22:00

Gala Dinner

Friday, September 27, 2019

09:00 – 10:30

Room: Wiltz
Keynote 2
Invited Talk Title: *A Cut Principle for Information Flow*
Speaker: Joshua Guttman

10:30 – 11:00

Coffee break

11:00 – 12:30

Session 3: Trust & Reputation

Room: Wiltz

Challenges of Using Trusted Computing for Collaborative Data Processing, By Paul Georg Wagner, Pascal Birnstill and Jürgen Beyerer

Secure Trust Evaluation Using Multipath and Referral Chain Methods, By Mohammad G. Raeini and Mehrdad Nojoumian

Personal Cross-Platform Reputation, By Johannes Blömer and Nils Löken

12:30 – 14:00

Farewell Lunch