ARES Conference
International Conference on Availability, Reliability and Security

ARES 2018

13th International Conference on Availability, Reliability and Security

August 27 – August 30, 2018
Hamburg, Germany

ARES 2018

13th International Conference on Availability, Reliability and Security

August 27 - 30, 2018
University of Hamburg, Hamburg, Germany

Organized by

SBA Research

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

The Association for Computing Machinery
2 Penn Plaza, Suite 701
New York New York 10121-0701

ACM ISBN: 978-1-4503-6448-5

The 13th International Conference on Availability, Reliability and Security (ARES 2018)

Welcome Message from ARES Program Committee Co-Chairs and General Chair

The 13th International Conference on Availability, Reliability and Security (ARES 2018) brings again together researchers and practitioners in the field of dependability and cybersecurity. ARES 2018 highlights the various aspects of this very important field, following the tradition of previous ARES conferences, with a special focus on the crucial linkage between availability, reliability, security and privacy. Again this year we are very happy to welcome famous keynote speakers from academia and industry.

This year, ARES has seen a record number of submissions, the highest in its history. From the many submissions, we have selected the 30 best ones as full paper. The quality of submissions has steadily improved over the last years and the conference officers sometimes faced a difficult decision when selecting which papers should be accepted. This year's acceptance rate for full papers is only 22,31%. In addition, several workshops and short papers are included in the program and show intermediate results of ongoing research projects and offer interesting starting points for discussions. Putting together ARES 2018 was a team effort. We first thank the authors for providing the content of the program. We are grateful to the program committee, which worked very hard in reviewing papers and providing feedback for authors. Finally, we thank all workshop chairs for their efforts in organizing interesting workshop sessions.

This year's conference is taking place in Hamburg, which is an old seafaring and trading city with the third-largest port in Europe. It is also one of the most popular touristic destinations in Germany. Hamburg has a history of pirates like the famous Klaus Störtebecker, who opposed the availability, reliability, and security of trading routes in the North and Baltic Sea in the 14th century. Thus, ARES is coming to a city that exactly knows that these topics are of outmost importance in our inter-connected societies.

Hamburg calls itself the German gate to the world. With ARES the world is coming to Hamburg.

We would like to thank the University of Hamburg for hosting ARES 2018!

Enjoy ARES 2018 and Hamburg!

Sebastian Doerr
TU Delft, Netherlands

Sebastian Schrittwieser
FH St. Pölten, Austria

Mathias Fischer
Universität Hamburg, Germany

Dominik Herrmann
Otto-Friedrich-Universität Bamberg, Germany

Committee ARES 2018

Steering Committee Chairpersons

Edgar Weippl*, SBA Research, Austria*
A Min Tjoa, *TU Vienna, Austria*

General Chair 2018

Mathias Fischer, *Universität Hamburg, Germany*
Dominik Herrmann, *Universität Hamburg, Germany*

Program Committee Chairs 2018

Christian Doerr, *TU Delft, Netherlands*
Sebastian Schrittwieser, *FH St. Pölten, Austria*

Workshop Chair 2018

Edgar Weippl, *SBA Research, Austria*

Program Committee 2018

- Isaac Agudo Ruiz, *University of Malaga, Spain*
- Esma Aimeur, *University of Montreal, Canada*
- Todd R. Andel, *University of South Alabama, US*
- Abdelmalek Benzekri, *University of Toulouse, France*
- Francesco Buccafurri, *University of Reggio Calabria, Italy*
- Lasaro Camargos, *Federal University of Uberlândia ,Brazil*
- Jordi Castellà-Roca, *Rovira i Virgili University of Tarragona, Spain*
- David Chadwick, *University of Kent, UK*
- Nathan Clarke, *Plymouth University, UK*
- Marijke Coetzee, *University of Johannesburg, South Africa*
- Nora Cuppens-Boulahia, *Université europée ne de Bretagne (UEB), France*
- Jörg Daubert, *TU Darmstadt, Germany*
- Luca De Cicco, *Politecnico di Bari, Italy*
- José Maria de Fuentes, *Carlos III University of Madrid, Spain*
- Pavlos Efraimidis, *Democritus University of Thrace, Greece*
- Dominik Engel, *Salzburg University of Applied Sciences, Austria*
- Christian Engelmann, *Oak Ridge National Laboratory, US*
- Aristide Fattori, *Università degli Studi di Milano, Italy*
- Hannes Federrath, *University of Hamburg, Germany*
- Christophe Feltus, *Luxembourg Institute of Science and Technology, Luxembourg*
- Umberto Ferraro Petrillo, *Universitá degli studi di Roma – La Sapienza, Italy*
- Steven Furnell, *Plymouth University, UK*
- Joaquin Garcia-Alfaro, *Télécom SudParis, France*
- Karl Goeschka, *Vienna University of Technology, Austria*
- Nico Golde, *Comsecuris UG, Germany*
- Lorena Gonzalez-Manzano, *Carlos III University of Madrid, Spain*
- Dimitris Gritzalis, *Athens University of Economics and Business, Greece*
- Bogdan Groza, *Politehnica University of Timisoara, Romania*
- Sheikh Mahbub *Habib, TU Darmstadt, Germany*

- Dominik Herrmann, *University Hamburg, Germany*
- Martin Gilje Jaatun, *SINTEF, Norway*
- Jan Jürjens, *TU Dortmund and Fraunhofer ISST, Germany*
- Anatoli Kalysch, *Friedrich-Alexander University Erlangen-Nuremberg, Germany*
- Vasilis Katos, *Bournemouth University, United Kingdom*
- Sokratis K. Katsikas, *NTNU: Norwegian University of Science and Technology, Norway*
- Peter Kieseberg, *SBA Research, Austria*
- Ezzat Kirmani, *St. Cloud State University, US*
- Ralf Kuesters, *University of Stuttgart, Germany*
- Oksana Kulyk, *TU Darmstadt, Germany*
- Romain Laborde, *University of Toulouse, France*
- Costas Lambrinoudakis, *University of Piraeus, Greece*
- Brian Lee, *Athlone Institute of Technology, Ireland*
- Shujun Li, *University of Surrey, UK*
- David Lillis, *University College Dublin, Ireland*
- Giovanni Livraga, *Universita' degli Studi di Milano, Italy*
- Robert Luh, Institute of IT Security Research, Austria
- Konstantinos Markantonakis, *Royal Holloway, University of London, UK*
- Keith Martin, *Royal Holloway, University of London, UK*
- Barbara Masucci, *University of Salerno, Italy*
- Ioannis Mavridis, *University of Macedonia, Greece*
- Wojciech Mazurczyk, *Warsaw University of Technology, Poland*
- Francesco Mercaldo, *Universita degli Studi del Sannio, Italy*
- Mattia Monga, *Universita` degli Studi di Milano, Italy*
- Haralambos Mouratidis, *University of Brighton, UK*
- Thomas Nowey, *Krones AG, Germany*
- Christoforos Ntantogian*, University of Piraeus, Greece*
- Jaehong Park, *University of Alabama in Huntsville, US*
- Günther Pernul, *University of Regensburg, Germany*
- Stefanie Rinderle-Ma, *Vienna University, Austria*
- Domenico Rosaci, *University of Reggio Calabria, Italy*
- Michael Roßberg, *TU Ilmenau, Germany*
- Volker Roth, *Freie Universität Berlin, Germany*
- Giovanni Russello, *University of Auckland, New Zealand*
- Luis Enrique Sánchez Crespo, *University of Castilla-la Mancha, Spain*
- Mark Scanlon, *University College Dublin, Ireland*
- Sebastian Schinzel, FH Münster, *Germany*
- Jörn-Marc Schmidt, *secunet, Germany*
- Max Schuchard, *University of Minnesota, US*
- Stefan Schulte, *Vienna University of Technology, Austria*
- Daniele Sgandurra, *Royal Holloway, University of London, UK*
- Jon A. Solworth, *University of Illinois at Chicago, US*
- Jordi Soria-Comas, *Universitat Rovira i Virgili, Spain*
- Mark Strembeck, *WU Vienna, Austria*

- Jakub Szefer, *Yale University, US*
- Oliver Theel, *Carl von Ossietzky Universität Oldenburg, Germany*
- Simon Tjoa, *St. Pölten University of Applied Sciences, Austria*
- Andreas Unterweger, *Salzburg University of Applied Sciences, Austria*
- Steven Van Acker, *Chalmers University, Sweden*
- Emmanouil Vasilomanolakis, *TU Darmstadt, Germany*
- Umberto Villano, *Universita' del Sannio, Italy*
- Corrado Aaron Visaggio, *Univeristà del Sannio, Italy*
- Xiao Wang, Carnegie *Mellon University, US*
- Christos Xenakis, *University of Piraeus, Greece*
- Zonghua Zhang, *IMT Lille Douai, Institue Mines-Télécom, France*
- Nicola Zannone, *Eindhoven University of Technology, Netherlands*

ARES 2018 Program: Full Papers

ARES Full I - Machine Learning

Modular Convolutional Neural Network for Discriminating between Computer-Generated Images and Photographic Images
Hong-Huy Nguyen (SOKENDAI (The Graduate University for Advanced Studies), Japan), Ngoc-Dung Tieu-Thi (SOKENDAI (The Graduate University for Advanced Studies), Japan), Hoang-Quoc Nguyen-Son (National Institute of Informatics, Japan), Vincent Nozick (Japanese-French Laboratory for Informatics (JFLI) (UMI 3527), Japan), Junichi Yamagishi (National Institute of Informatics, Japan) and Isao Echizen(National Institute of Informatics, Japan)

FALKE-MC: A Neural Network Based Approach to Locate Cryptographic Functions in Machine Code
Alexander Aigner (University of Applied Sciences Upper Austria, Austria)

ARES Full II - Best Paper Session

Secure Equality Testing Protocols in the Two-Party Setting
Majid Nateghizad (Delft University of Technology, Netherlands), Thijs Veugen (TNO, Netherlands), Zekeriya Erkin (Delft University of Technology, Netherlands) and Reginald L. Lagendijk (Delft University of Technology, Netherlands)

Android authorship attribution through string analysis
Vaibhavi Kalgutkar (University of New Brunswick, Canada), Natalia Stakhanova (University of New Brunswick, Canada), Paul Cook (University of New Brunswick, Canada) and Alina Matyukhina (University of New Brunswick, Canada)

Flashlight: A Novel Monitoring Path Identification Schema for Securing Cloud Services
Heng Zhang (DEEDS Group, Department of Computer Science, TU Darmstadt, Germany), Ruben Trapero (Atos Research & Innovation, Spain), Jesus Luna Garcia (TU Darmstadt, Germany) and Neeraj Suri (TU Darmstadt, Germany)

ARES Full III - Software Security

Discovering software vulnerabilities using data-flow analysis and machine learning
Jorrit Kronjee, Arjen Hommersom and Harald Vranken (Open University of the Netherlands, Netherlands)

Speeding Up Bug Finding using Focused Fuzzing

Ulf Kargén and Nahid Shahmehri (Linköping University, Sweden)

HYDRA- Hypothesis Driven Repair Automation

Partha Pal, Brett Benyo, Shane Clark and Aaron Paulos (Raytheon BBN, United States)

ARES Full IV - Security and the User

Protecting Patients' Data: An Efficient Method for Health Data Privacy

Mark Daniels, John Rose and Csilla Farkas (University of South Carolina, United States)

Influence Factors on the Quality of User Experience in OS Reliability: A Qualitative Experimental Study

Caio Augusto Rodrigues Dos Santos, Daniela Yabe, Lucas Miranda and Rivalino Matias (Federal University of Uberlandia, Brazil)

ARES Full V - Cryptography

Finally Johnny Can Encrypt. But Does This Make Him Feel More Secure?

Nina Gerber (KIT, Germany), Verena Zimmermann (TU Darmstadt, Germany), Birgit Henhapl (TU Darmstadt, Germany), Sinem Emeröz (TU Darmstadt, Germany) and Melanie Volkamer (KIT, Germany)

An Efficient Cryptography-Based Access Control Using Inner-Product Proxy Re-Encryption Scheme

Masoomeh Sepehri (University of Milan, Italy), Maryam Sepehri (University of Milan, Italy), Alberto Trombetta (Università degli Studi dell'Insubria, Italy) and Ernesto Damiani (Khalifa University of Science and Technology, United Arab Emirates)

Non-Interactive Key Exchange from Identity-Based Encryption

Olivier Blazy (Université de Limoges, France) and Céline Chevalier (ENS, France)

ARES Full VI - Anomaly Detection

Behavioural Comparison of Systems for Anomaly Detection

Martin Pirker, Patrick Kochberger and Stefan Schwandter (St. Pölten UAS, Austria)

Converting Unstructured System Logs into Structured Event List for Anomaly Detection

Zongze Li (University of north Texas, United States), Song Fu (University of north Texas, United States), Matthew Davidson (University of north Texas, United States), Sean Blanchard (Los Alamos National Laboratory, United States) and Michael Lang (Los Alamos National Laboratory, United States)

Stealthy Attacks on Smart Grid PMU State Estimation

Sarita Paudel (AIT Austrian Institute of Technology, Austria), Tanja Zseby (Vienna University of Technology, Austria) and Paul Smith (AIT Austrian Institute of Technology, Austria)

ARES Full VII - Network Security and Monitoring I

A Framework for Monitoring Net Neutrality

Wilfried Mayer (SBA Research, Austria), Thomas Schreiber (TU Wien, Austria) and Edgar Weippl (SBA Research, Austria)

The Other Side of the Coin: A Framework for Detecting and Analyzing Web-based Cryptocurrency Mining Campaigns

Julian Rauchberger, Sebastian Schrittwieser, Tobias Dam, Robert Luh, Damjan Buhov, Gerhard Pötzelsberger (St. Pölten UAS, Austria) and Hyoungshick Kim (Sungkyunkwan University, South Korea)

ARES Full VIII - Network Security and Monitoring II

A Pyramidal-based Model to Compute the Impact of Cyber Security Events

Gustavo Gonzalez (Atos, Spain), Jose Manuel Rubio Hernan (Télécom SudParis, CNRS UMR 5157 SAMOVAR, Université Paris-Saclay, France) and Joaquin Garcia-Alfaro (Télécom SudParis, CNRS UMR 5157 SAMOVAR, Université Paris-Saclay, France)

ToGather: Towards Automatic Investigation of Android Malware Cyber-Infrastructures

Elmouatez Billah Karbab Karbab and Mourad Debbabi (Concordia University, Canada)

ARES Full IX - Automotive

Attack Graph-Based Assessment of Exploitability Risks in Automotive On-Board Networks

Martin Salfer (Technical University of Munich, Germany) and Claudia Eckert (Technical University of Munich, Germany)

Anonymous Charging and Billing of Electric Vehicles

Daniel Zelle, Markus Springer, Maria Zhdanova and Christoph Krauß (Fraunhofer, Germany)

Comparison of Data Flow Error Detection Techniques in Embedded Systems: an Empirical Study

Venu Babu Thati (Katholieke Universiteit Leuven, Belgium), Jens Vankeirsbilck (Katholieke Universiteit Leuven, Belgium), Niels Penneman (Televic Healthcare, Belgium), Davy Pissoort (Katholieke Universiteit Leuven, Belgium) and Jeroen Boydens (Katholieke Universiteit Leuven, Belgium)

ARES Full X - Cloud Security

Distributed and Cooperative firewall/controller in cloud environments

Ferdaous Kamoun-Abid (NTS'COM, ENET'COM, Tunisia), Amel Meddeb-Makhlouf (NTS'COM, ENET'COM, Tunisia), Faouzi Zarai (NTS'COM, ENET'COM, Tunisia) and Mohsen Guizani (ECE Department, University of Idaho, United States)

Cloud Architectures for Searchable Encryption

Johannes Blömer and Nils Löken (University of Paderborn, Germany)

ARES 2018 Program: Short Papers

ARES Short I - Malware

An investigation of a deep learning based malware detection system

Mohit Sewak, Sanjay Sahay and Hemant Rathore (BITS, Pilani, Department of CS & IS, Goa Campus, India)

Towards the Automatic Generation of Low-Interaction Web Application Honeypots

Marius Musch (TU Braunschweig, Germany), Martin Johns (TU Braunschweig, Germany) andMartin Härterich (SAP Security Research, Germany)

Learning Malware Using Generalized Graph Kernels
Khanh Huu The Dam (LIPN and University Paris Diderot, France) and Tayssir Touili (LIPN, CNRS & University Paris 13, France)

ARES Short II - Monitoring

Assessing Internet-wide Cyber Situational Awareness of Critical Sectors
Martin Husák (Masaryk University, Czech Republic), Nataliia Neshenko (Florida Atlantic University, United States), Morteza Safaei Pour (Florida Atlantic University, United States), Elias Bou-Harb (Florida Atlantic University, United States) and Pavel Čeleda (Masaryk University, Czech Republic)

Spreading Alerts Quietly: New Insights from Theory and Practice
Olivier Blazy (Université de Limoges, France) and Céline Chevalier (ENS, France)

A Reactive Defense Against Bandwidth Attacks Using Learning Automata
Nafiseh Kahani (Queen's Univeristy, Canada) and Mehran Fallah (Amirkabir University of Technology, Iran)

ARES Short III - Embedded Systems

ATG: An Attack Traffic Generation Tool for Security Testing of In-vehicle CAN Bus
Tianxiang Huang (Chongqing University of Posts and Telecommunications, China), Jianying Zhou (Singapore University of Technology and Design, Singapore) and Andrei Bytes (Singapore University of Technology and Design, Singapore)

Let's shock our IoT's heart: ARMv7-M under (fault) attacks
Sebanjila K. Bukasa (LHS-PEC INRIA-RBA, France), Ronan Lashermes (LHS-PEC INRIA-RBA, France), Jean-Louis Lanet (LHS-PEC INRIA-RBA, France) and Axel Legay (TAMIS INRIA-RBA, France)

Enterprise WLAN Security Flaws: Current Attacks and Relative Mitigations
Mohamed Abo-Soliman and Marianne Azer (Nile University, Egypt)

ARES Short IV - Security Practices

What are Security Patterns? A Formal Model for Security and Design of Software
Anika Behrens (University of Bremen, Germany)

A Nlp-based Solution to Prevent from Privacy Leaks in Social Network Posts
Gerardo Canfora, Andrea Di Sorbo, Enrico Emanuele, Sara Forootani and Corrado A. Visaggio (University of Sannio, Italy)

(In)Secure Configuration Practices of WPA2 Enterprise Supplicants
Alberto Bartoli (Università degli Studi di Trieste – DEEI, Italy), Eric Medvet (DI3 – University of Trieste, Italy), Fabiano Tarlao (Department of Engineering and Architecture, University of Trieste, Italy) and Andrea De Lorenzo (University of Trieste – DIA, Italy)

The Workshops of the 13th International Conference on Availability, Reliability and Security (ARES 2018)

Welcome Message from ARES Workshop Chair

Welcome to the Workshops of the Twelfth International Conference on Availability, Reliability and Security (ARES 2018).

The workshops are central events for ARES as they provide an essential platform for researchers of various domains to present and discuss their current work and discuss work in progress. This year we can offer the conference attendees 12 workshops, which range from "start-ups" to well-established ones supporting ARES.

The succeeding listing comprises the workshops of ARES 2018:

- 13th International Workshop on Frontiers in Availability, Reliability and Security (FARES 2018)
- 11th International Workshop on Digital Forensics (WSDF 2018)
- 7th International Workshop on Security of Mobile Applications (IWSMA 2018)
- 7th International Workshop on Cyber Crime (IWCC 2018)
- 5th International Workshop on Software Assurance Workshop (SAW 2018)
- 4th International Workshop on Agile Secure Software Development (SSE 2018)
- 2nd International Workshop on Criminal Use of Information Hiding (CUING 2018)
- 1st International Workshop on Security and Forensics of IoT (IoT-SECFOR 2018)
- 1st Interdisciplinary Workshop on Privacy and Trust (iPAT 2018)
- 1st International Workshop on Security Engineering for Cloud Computing (IWSECC 2018)
- 1st International Workshop on Security and Privacy-Enhanced Big Data (SPEBD 2018)
- 1st International Workshop on Cyber Threat Intelligence (WCTI 2018)

These workshops are organized each on specific topics and thus offer researchers the opportunity to learn from a rich multi-disciplinary experience. The Workshop Chair would like to thank the workshop organizers for their great efforts and hard work in proposing the workshop, selecting the papers, the interesting programs and for the arrangements of the workshops during the conference days.

We hope you enjoy the workshops programs and proceedings.

Edgar Weippl
ARES 2018 Workshop Chair
SBA Research, Austria

The 13th International Workshop on Frontiers of Availability, Reliability and Security (FARES 2018)

Welcome Message from the FARES Workshop Organizers

The 13th International Workshop on Frontiers of Availability, Reliability and Security (FARES 2018) establishes an in-depth academic platform to exchange novel theories, designs, applications and on-going research results among researchers and practitioners in different Computing Dependability aspects, which emphasize the Practical Issues in Availability, Reliability and Security.

From the received submissions, we have selected the 8 best for presentation. These presentations have been grouped into 2 sessions. The first session deals with problems related to protection and detection. The second one collects papers focusing on security measurement and robust design.

Finally, our special thanks are due to Yvonne Poul and Julia Pammer for their kind assistance and help.

Francesco Buccafurri
FARES 2018 Program Co-Chair
University of Reggio Calabria, Italy

Gianluca Lax
FARES 2018 Program Co-Chair
University of Reggio Calabria, Italy

Workshop Program Committee FARES 2018

- Eduardo B. Fernandez, *Florida Atlantic University, USA*
- Manuel Eduardo Correia, *Porto University, Porto, Portugal*
- Giorgio Giacinto, *Università di Cagliari, Cagliari, Italy*
- Maria Krotsiani, *City, University of London, London (UK*
- Andrea Lanzi, *University of Milan, Milano, Italy*
- Roberto Nardone, *Università di Napoli Federico II, Napoli, Italy*
- Vishal Saraswat, *R.C.Bose Centre for Cryptology and Security Indian Statistical Institute, Kolkata, India*
- Aaron Visaggio, *Università del Sannio, Benevento, Italy*

FARES 2018 Program

FARES I - Protection and Detection

Recovery of Encrypted Mobile Device Backups from Partially Trusted Cloud Servers
Omid Mir, Rene Mayrhofer, Michael Hölzl and Thanh-Binh Nguyen (Institute of Networks and Security, Johannes Kepler University, Austria)

Reputation-Based Security System For Edge Computing
Francis Nwebonyi (University of Porto, Portugal), Rolando Martins (University of Porto, Portugal) and Manuel E. Correia (CRACS/INESC TEC; DCC/FCUP, Portugal)

New authentication concept using certificates for big data analytic tools
Paul Velthuis (Fraunhofer-Institute-for-Secure-Information-Technology-SIT, Netherlands), Marcel Schäfer and Martin Steinebach (Fraunhofer-Institute-for-Secure-Information-Technology-SIT, Germany)

Evaluation of Machine Learning-based Anomaly Detection Algorithms on an Industrial Modbus/TCP Data Set
Simon Duque Anton, Suneetha Kanoor, Daniel Fraunholz and Hans Dieter Schotten (Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Germany)

FARES II - Measurement and Robust Design

X.509 Certificate Error Testing
David Mcluskie and Xavier Bellekens (Abertay University, United Kingdom)

Evaluating the degree of security of a system built using security patterns
Eduardo B. Fernandez (Florida Atlantic University, United States), Nobukazu Yoshioka (National Institute of Informatics, Japan) and Hironori Washizaki (Waseda

Attack Difficulty Metric for Assessment of Network Security
Preetam Mukherjee and Chandan Mazumdar (Jadavpur University, India)

Robustness Estimation of Infrastructure Networks: On the Usage of Degree Centrality
Sebastian Wandelt and Xiaoqian Sun (Beihand University, China)

The 11th International Workshop on Digital Forensics (WSDF 2018)

Welcome Message from the WSDF Workshop Organizers

It is our great pleasure to welcome you to the 11th International Workshop on Digital Forensics (WSDF) which takes place in Hamburg (Germany) from 27 to 30 August 2018.

Digital forensics is a rapidly evolving field primarily focused on the extraction, preservation and analysis of digital evidence obtained from electronic devices in a manner that is legally acceptable. Research into new methodologies tools and techniques within this domain is necessitated by an ever-increasing dependency on tightly interconnected, complex and pervasive computer systems and networks. The ubiquitous nature of our digital lifestyle presents many avenues for the potential misuse of electronic devices in crimes that directly involve, or are facilitated by, these technologies. The aim of digital forensics is to produce outputs that can help investigators ascertain the overall state of a system. This includes any events that have occurred within the system and entities that have interacted with that system. Due care has to be taken in the identification, collection, archiving, maintenance, handling and analysis of digital evidence in order to prevent damage to data integrity. Such issues combined with the constant evolution of technology provide a large scope of digital forensic research. WSDF brings together experts from academia, industry, government and law enforcement who are interested in advancing the state of the art in digital forensics by exchanging their knowledge, results, ideas and experiences.

The aim of the workshop is to provide a relaxed atmosphere that promotes discussion and free exchange of ideas while providing a sound academic backing. The focus of this workshop is not only restricted to digital forensics in the investigation of crime. It also addresses security applications such as automated log analysis, forensic aspects of fraud prevention and investigation, policy and governance.

The acceptance rate of this edition of the workshop was 58%.

The Workshop organizing committee

Richard E. Overill, *King's College London, UK*
Virginia N. L. Franqueira**,** *University of Derby, UK*
Andrew Marrington, *Zayed University, UAE*
Andrew Jones, *University of Hertfordshire, UK*

Workshop Program Committee WSDF 2018

- Aniello Castiglione, *Università di Salerno, Italy*
- Aswami Ariffin, *Cyber Security Malaysia, Malaysia*
- Frank Bretinger, *University of New Haven, USA*
- George Grispos, *University of Nebraska Omaha, USA*
- Ibrahim Baggili, *University of New Haven, USA*
- Jeroen van der Bos, *Netherlands Forensic Institute, Netherlands*
- Jo Bryce, *University of Central Lancashire, UK*
- Joshua James, *Soon Chun Hyang University, South Korea*
- Kam-Pui Chow, *Hong Kong University, Hong Kong*
- Kim Kwang Raymond Choo, *University of South Australia, Australia*
- Kiran Kumar Muniswany Reddy, *Amazon Web Services, USA*
- Mark Scalon, *University College Dublin, Ireland*
- Olga Angelopoulou, *University of Hertfordshire, UK*
- Pedro Inácio, *Universidade da Beira Interior, Portugal*
- Reza Montasari, *Birmingham City University, UK*
- Simon Tjoa, *St. Pölten University of Applied Sciences, Austria*
- Sandra Avila, *University of Campinas, Brasil*
- Stefano Zanero, *Politecnico di Milano, Italia*
- Tim Storer, *University of Glasgow, UK*
- Vassil Roussev, *University of New Orleans, USA*
- Yijun Yu, *Open University, UK*

WSDF 2018 Program

WSDF I

Digital Forensics in the Next Five Years

Laoise Luciano, Mateusz Topor, Ibrahim Baggili and Frank Breitinger (University of New Haven, United States)

WSDF II

Forensic APFS File Recovery

Jonas Plum (Siemens AG, Germany) and Andreas Dewald (ERNW Research GmbH, Germany)

Volatile Memory Forensics Acquisition Efficacy: A Comparative Study Towards Analysing Firmware-Based Rootkits

Jacob Taylor, Benjamin Turnbull and Gideon Creech (The University of New South Wales, Australia)

I Know What You Did Last Summer: Your Smart Home Internet of Things and Your iPhone Forensically Ratting You Out

Gokila Dorai (Florida State University, United States), Shiva Houshmand (Southern Illinois University, United States) and Ibrahim Baggili (University of New Haven, United States)

WSDF III

Breaking down violence: A deep-learning strategy to model and classify violence in videos

Bruno Malveira Peixoto, Sandra Avila, Zanoni Dias and Anderson Rocha (Universidade Estadual de Campinas – Unicamp, Brazil)

Digitally Signed and Permission Restricted PDF Files: a Case Study on Digital Forensics

Patricio Domingues and Miguel Frade (Instituto Politécnico de Leiria, Portugal)

Investigating the Use of Online Open Source Information as Evidence in European Courts

Yi-Ching Liao (Noroff University College, Norway)

The 7th International Workshop on Security of Mobile Applications (IWSMA 2018)

Welcome Message from the IWSMA Workshop Organizers

Since the advent of Smartphones, mobile applications have been one of the most thriving areas in the last few years. Thus, securing mobile applications as well as protecting private user data has to be considered as key research topics in the realm of security research. In recent years, this focus on mobile application has been extended to other application fields, like autonomous cars and their specific security requirements. The International Workshop on Security of Mobile Applications (co-located with the ARES-conference) focuses on bringing together researchers from all over the world to share their experience and present recent research, as well as strives to initiate discussions regarding future research topics.

The papers that were selected for this workshop cover several interesting topics in this big area, thus they should give an ideal starting point for further discussion, which we are looking forward to participate in, together with the authors and an active audience.

The Workshop organizing committee

Peter Kieseberg, *SBA Research, Austria & UAS St. Pölten & SBA Research, Austria*
Sebastian Schrittwieser, *Josef Ressel Center for Unified Threat Intelligence on Targeted Attacks, UAS St. Pölten, Austria*

Workshop Program Committee IWSMA 2018

- Fatemeh Amiri, *University of Vienna, Austria*
- Amin Anjomshoaa, *Senseable City Lab, Massachusetts Institute of Technology, USA*
- Jakub Breier, *Nanyang Technological University, Singapore*
- Isao Echizen, *National Institute of Informatics (NII), Japan*
- Eduard Fosch Villaronga, *Microsoft Cloud Computing Research Center for Commercial Law Studies at Queen Mary University of London, UK*
- Peter Frühwirt, *Vienna University of Technology, Austria*
- Uschi Gonschor, *EntServ Enterprise Services, Austria*
- Johannes Heurix, *SBA Research, Austria*
- Andreas Hula, *AIT, Austria*
- Martin Husák, *Masaryk University, Czech Republic*
- Tiffany Li, *Yale Law School, USA*
- Francesco Mercaldo, *Institute for Informatics and Telematics (CNR), Italy*
- Raydel Montesino Perurena, *Universidad de las Ciencias Informáticas, Cuba*
- Lukasz Olejnik, *independent researcher, LukaszOlejnik.com, United Kingdom*
- Mayank Sinha, *Shell, The Netherlands*
- Ronald Tögl, *Infineon Technologies, Austria*
- Johanna Ullrich, *SBA Research, Austria*

IWSMA 2018 Program

IWSMA I

Toward a Distributed Trust Management scheme for VANET
Amira Kchaou (SUPCOM, Tunisia), Ryma Abassi (SUPCOM, Tunisia) and Sihem Guemara El Fatmi (High School of Communication, Sup'Com, Tunisia)

There Goes Your PIN: Exploiting Smartphone Sensor Fusion Under Single and Cross User Setting
David Berend (Nanyang Technological University, Singapore, University of Applied Sciences Wiesbaden, Rüsselsheim, Germany), Bernhard Jungk (Temasek Laboratories at Nanyang Technological University, Singapore) and Shivam Bhasin (Temasek Labs@NTU, Singapore)

Towards a Privacy Preserving and Flexible Scheme for Assessing the Credibility and the Accuracy of Safety Messages Exchanged in VANETs
Ons Chikhaoui, Aida Ben Chehida Douss, Ryma Abassi and Sihem Guemara El Fatmi (Higher School of Communication, Sup'Com, Tunisia)

IWSMA II

Practical Precise Taint-flow Static Analysis for Android App Sets
William Klieber, Lori Flynn, William Snavely and Michael Zheng (Carnegie Mellon Univ, Software Engineering Institute, United States)

Detection of Obfuscation Techniques in Android Applications
Alessandro Bacci (Dipartimento di Ingegneria e Architettura – Università degli Studi di Trieste, Italy), Alberto Bartoli (Dipartimento di Ingegneria e Architettura – Università degli Studi di Trieste, Italy), Fabio Martinelli (Istituto di Informatica e Telematica – Consiglio Nazionale delle Ricerche, Pisa, Italy), Eric Medvet (Dipartimento di Ingegneria e Architettura – Università degli Studi di Trieste, Italy) and Francesco Mercaldo (Istituto di Informatica e Telematica – Consiglio Nazionale delle Ricerche, Pisa, Italy)

Tackling Android's Native Library Malware with Robust, Efficient and Accurate Similarity Measures
Anatoli Kalysch, Mykolai Protsenko, Oskar Milisterfer and Tilo Müller (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany)

The 7th International Workshop on Cyber Crime (IWCC 2018)

Welcome Message from the IWCC Workshop Organizers

Today's world's societies are becoming more and more dependent on open networks such as the Internet – where commercial activities, business transactions and government services are realized. This has led to the fast development of new cyber threats and numerous information security issues which are exploited by cyber criminals. The inability to provide trusted secure services in contemporary computer network technologies has a tremendous socio-economic impact on global enterprises as well as individuals.

Moreover, the frequently occurring international frauds impose the necessity to conduct the investigation of facts spanning across multiple international borders. Such examination is often subject to different jurisdictions and legal systems. A good illustration of the above being the Internet, which has made it easier to perpetrate traditional crimes. It has acted as an alternate avenue for the criminals to conduct their activities, and launch attacks with relative anonymity. The increased complexity of the communications and the networking infrastructure is making investigation of the crimes difficult. Traces of illegal digital activities are often buried in large volumes of data, which are hard to inspect with the aim of detecting offences and collecting evidence. Nowadays, the digital crime scene functions like any other network, with dedicated administrators functioning as the first responders.

This poses new challenges for law enforcement policies and forces the computer societies to utilize digital forensics to combat the increasing number of cybercrimes. Forensic professionals must be fully prepared in order to be able to provide court admissible evidence. To make these goals achievable, forensic techniques should keep pace with new technologies.

The aim of the IWCC workshop is to bring together the research accomplishments provided by the researchers from academia and the industry. The other goal is to show the latest research results in the field of digital forensics and to present the development of tools and techniques, which assist the investigation process of potentially illegal cyber activity.

The Workshop organizing committee

Artur Janicki, *Warsaw University of Technology, Poland*
Wojciech Mazurczyk, *Warsaw University of Technology, Poland*
Krzysztof Szczypiorski, *Warsaw University of Technology, Poland*

Workshop Program Committee IWCC 2018

- Marc Chaumont, *LIRMM, France*
- Michal Choras, *ITTI Ltd., Poland*
- Xiaofeng Chen, *Xidian University, China*
- Guangjie Liu, *NJUST, China*
- Jozef Wozniak, *Gdansk University of Technology, Poland*
- Frédéric Cuppens, *TELECOM Bretagne, France*
- Prof. Dr. Jana Dittmann, *Otto-von-Guericke University Magdeburg, Germany*
- Steffen Wendzel, *Worms University of Applied Sciences and Fraunhofer FKIE, Germany*
- Stefan Katzenbeisser, *TU Darmstadt, Germany*
- Joanna Śliwa, *Military Communication Institute, Poland*
- Maciej Korczyñski, *Delft University of Technology, The Netherlands*
- Alessandro Checco, *University of Sheffield, UK*
- Nabil Schear, *MIT Lincoln Laboratory, USA*
- Bela Genge, *University of Tg Mures, Romania*
- Igor Kotenko, *Russian Academy of Sciences (SPIIRAS), Russia*
- Johnson Thomas, *Oklahoma State University, USA*
- Ewa Syta, *Trinity College, Ireland*
- Jean-Francois Lalande, *INSA Centre Val de Loire, France*
- Christian Kraetzer, *Otto-von-Guericke University Magdeburg, Germany*
- Pedro Luis Prospero Sanchez, *University of Sao Paulo, Brazil*
- Zbigniew Kotulski, *Warsaw University of Technology, Poland*
- Eric Chan-Tin, *Oklahoma State University, USA*
- Josef Pieprzyk, *Queensland University of Technology, Australia*
- Luca Caviglione, *ISSIA, CNR, Italy*
- Hui Tian, *National Huaqiao University, China*

IWCC 2018 Program

IWCC I

Monitoring Product Sales in Darknet Shops

York Yannikos (Fraunhofer, Germany), Annika Schäfer (TU Darmstadt, Germany) and Martin Steinebach (Fraunhofer, Germany)

IoT Forensic: identification and classification of evidence in criminal investigations

François Bouchaud (IRCGN, France), Gilles Grimaud (IRCICA – CRIStAL, France) and Thomas Vantroys (IRCICA – CRIStAL, France)

IWCC II

Recent Granular Computing Implementations and its Feasibility in Cybersecurity Domain

Marek Pawlicki (UTP Bydgoszcz, Poland), Michal Choras (ITTI Ltd., Poland) and Rafal Kozik (Institute of Telecommunications, UTP Bydgoszcz, Poland)

Determination of Security Threat Classes on the basis of Vulnerability Analysis for Automated Countermeasure Selection

Elena Doynikova, Andrey Fedorchenko and Igor Kotenko (St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Russia)

A New Classification of Attacks against the Cyber-Physical Security of Smart Grids

Ghada Elbez, Hubert B. Keller and Veit Hagenmeyer (Karlsruhe Institute of Technology, Germany)

The 5th International Workshop on Software Assurance (SAW 2018)

Welcome Message from the SAW Workshop Organizers

We would like to offer our warm welcome to our fourth Software Assurance Workshop (SAW) co-located with ARES 2018!

Software security is drawing more attention from the software engineering community, in part due to the many highly publicized attacks exploiting software vulnerabilities. Software increasingly affects our daily lives: our social networks, our automobiles, our smart home systems, our smart phones, and our financial well-being just to name a few.

Although many attempts have been made to improve software security over the years, the focus of these efforts has traditionally been limited to tools and techniques focusing on implementation and testing, such as static analysis, penetration testing, and secure coding.

We believe that the scope of software security is much wider than those heavily studied research areas and would like to invite researchers to explore other facets of software security, which have not been as thoroughly studied.

The vision of our workshop is to provide the state-of-the-art in Software Assurance as well as opportunities to network with academicians and professionals working in the software community. We look forward to getting to know you at the workshop and sincerely thank you for your participation.

The Workshop organizing committee

Jungwoo Ryoo, *Penn State Altoona, USA*
Simon Tjoa, *St. Pölten University of Applied Sciences, Austria*
Rick Kazman, *University of Hawaii/SEI, USA*

Workshop Program Committee SAW 2018

- Robert Ellison, *Software Engineering Institute (SEI)/Computer Emergency Response Team (CERT), USA*
- Rick Kazman*, University of Hawaii/SEI, USA*
- Dae-kyoo Kim, *Oakland University, USA*
- Suntae Kim, *Chonbuk National University, Republic of Korea*
- Phillip Laplante, *Pennsylvania State University, USA*
- Jungwoo Ryoo, *Pennsylvania State University, USA*
- Sebastian Schrittwieser, *St. Pölten University of Applied Sciences, Austria*
- Eunjee Song*, Baylor University, USA*
- Paul Tavolato*, St. Pölten University of Applied Sciences, Austria*
- A Min Tjoa, *Vienna University of Technology, Austria*
- Simon Tjoa, *St. Pölten University of Applied Sciences, Austria*
- Edgar Weippl, *Secure Business Austria (SBA) Research, Austria*
- Carol Woody, *SEI/CERT, USA*

SAW 2018 Program

SAW I - Software Security Testing and Cyber-Resilience

Mission-Centric Automated Cyber Red Teaming

Suneel Randhawa (Defence Science and Technology, Department of Defence, Australia), Benjamin Turnbull (The University of New South Wales, Australia), Joseph Yuen (The University of New South Wales, Australia) and Jonathan Dean (Defence Science and Technology, Department of Defence, Australia)

Ransomware's early mitigation mechanisms

Ruta Mussaileb (IMT-Atlantique, France), Nora Cuppens (IMT-Atlantique, France), Jean Louis Lanet (INRIA, France), Helene Bouder (IMT-Atlantique, France), Benjamin Bouget (DGA, France) and Aurelien Palisse (INRIA, France)

A GDPR compliance module for supporting the exchange of information between CERTs

Otto Hellwig (SBA-Research, Austria), Gerald Quirchmayr (University of Vienna, Austria), Walter Hötzendorfer (Research Institute AG & Co KG, Austria), Christof Tschohl (Research Institute AG & Co KG, Austria), Edith Huber (Danube University Krems, Austria), Franz Vock (Federal Chancellery, Austria), Florian Nentwich (IKARUS Security Software, Austria), Bettina Pospisil (Danube University Krems, Austria), Matthias Gusenbauer (SBA-Research, Austria) and Gregor Langner (University of Vienna, Austria)

SAW II - Secure Software Development

CryptSDLC: Embedding Cryptographic Engineering into Secure Software Development Lifecycle

Thomas Lorünser (AIT Austrian Institute of Technology, Austria), Thomas Länger (University of Lausanne, Austria), Henrich C. Pöhls (University of Passau, Germany) and Leon Sell (University of Passau, Germany)

Architectural Solutions to Mitigate Security Vulnerabilities in Software Systems

Priya Anand and Jungwoo Ryoo (The Pennsylvania State University, United States)

The 4th International Workshop on Secure Software Engineering (SSE 2018)

Welcome Message from the SSE Workshop Organizers

It is our pleasure to welcome you to the Fourth International Workshop on Secure Software Engineering (SSE 2018), organized in conjunction with the International Conference on Availability, Reliability and Security (ARES 2018) in University of Hamburg, Germany.

The goal of the workshop is to bring together security and software development researchers to share their finding, experiences, and positions about developing secure software. The workshop aims to encourage the use of scientific methods to investigate the challenges related to developing secure software. It aims also to increase the communication between security researchers and software development researchers to enable the development of techniques and best practices for developing secure software.

We have assembled this year a program to challenge the participants and stimulate the discussion. We selected 3 papers. We thank the members of the Program Committee for their support, and all the authors for their contribution to the workshop. Each paper has been reviewed by minimum 3 members of the Program Committee.

We hope you will enjoy it!

The Workshop organizing committee

Juha Röning, *University of Oulu, Finland*

Lotfi ben Othmane, *Iowa State University, USA*

Workshop Program Committee SSE 2018

- Benjamin Aziz, *University of Portsmouth, UK*
- Bhargava, Bharat, *Purdue University, USA*
- Achim Brucker, *University of Sheffield, UK*
- Joern Eichler, *Fraunhofer AISEC, Germany*
- Michael Felderer, *Universität Innsbruck, Austria*
- Vimal Kumar, *University of Waikato, New Zealand*
- Lotfi ben Othmane, *Iowa State University, USA*
- Sandra Ringman, *Konstanz University of Applied Sciences, Germany*
- Juha Röning, *University of Oulu, Finland*
- Markus Wagner, *St.Pölten University of Applied Sciences, Austria*
- Edgar Weippl, *SBA Research, Austria*
- Hasan Yasar, *Carnegie Mellon University, USA*
- Koen Yskout, KU Leuven, Belgium
- Mohammad Zulkernine, *Queen's University, Canada*

SSE 2018 Program

SSE I - Secure software development and DevOps

Surveying Secure Software Development Practices in Finland
Kalle Rindell (University of Turku, Finland), Jukka Ruohonen (University of Turku, Finland) and Sami Hyrynsalmi (Tampere University of Technology, Finland)

Challenges and Mitigation Approaches for Getting Secured Applications in a Big Company
Pawel Rajba (University of Wroclaw, Poland)

Software Security Activities that Support Incident Management in Secure DevOps
Martin Gilje Jaatun (SINTEF Digital, Norway)

The 2nd International Workshop on Criminal Use of Information Hiding (CUING 2018)

Welcome Message from the CUING Workshop Organizers

With the constant rise of the number of Internet users, available bandwidth and an increasing number of services shifting into the connected world, criminals are increasingly active in the virtual world. With improving defensive methods, cybercriminals have to utilize increasingly sophisticated ways to perform their malicious activities. While protecting the privacy of users, many technologies used in current malware and network attacks have been abused in order to allow criminals to carry out their activities undetected.

The aim of the Second International Workshop on Criminal Use of Information Hiding (CUIng) is to bring together researchers, practitioners, law enforcement representatives, and security professionals in the area of analysis of information hiding (e.g. steganography, covert channels), obfuscation techniques and underground networks (darknets) in order to present novel research regarding the use of data and communication hiding methods in criminal environments and to discuss ideas for fighting misuse of privacy enhancing technologies.

The Workshop organizing committee

Philipp Amann, *Europol, European Cybercrime Centre, The Netherlands*
Jart Armin, *CyberDefcon, The Netherlands*
Wojciech Mazurczyk, *Warsaw University of Technology, Poland*
Angelo Consoli, *Scuola universitaria professionale della Svizzera italiana (SUPSI), Switzerland*
Peter Kieseberg, *SBA Research, Austria*
Joerg Keller, *FernUniversitaet in Hagen, Germany*

Workshop Program Committee CUING 2018

- Robert Ellison, *Software Engineering Institute (SEI)/Computer Emergency Response Team (CERT), USA*
- Rick Kazman, *University of Hawaii/SEI, USA*
- Dae-kyoo Kim, *Oakland University, USA*
- Suntae Kim, *Chonbuk National University, Republic of Korea*
- Phillip Laplante, *Pennsylvania State University, USA*
- Jungwoo Ryoo, *Pennsylvania State University, USA*
- Sebastian Schrittwieser, *St. Pölten University of Applied Sciences, Austria*
- Eunjee Song, *Baylor University, USA*
- Paul Tavolato, *St. Pölten University of Applied Sciences, Austria*
- A Min Tjoa, *Vienna University of Technology, Austria*
- Simon Tjoa, *St. Pölten University of Applied Sciences, Austria*
- Edgar Weippl, *SBA Research, Austria*
- Carol Woody, *SEI/CERT, USA*

CUING 2018 Program

CUING I

Channel Steganalysis
Martin Steinebach (Fraunhofer, Germany)

Towards Deriving Insights into Data Hiding Methods Using Pattern-based Approach
Wojciech Mazurczyk (Warsaw University of Technology, Poland), Steffen Wendzel (Worms University of Applied Sciences and Fraunhofer FKIE, Germany) and Krzysztof Cabaj (Warsaw University of Technology, Poland)

Steganography by synthesis - Can commonplace image manipulations like face morphing create plausible steganographic channels?
Christian Kraetzer and Jana Dittmann (Dept. of Computer Science, Otto-von-Guericke University Magdeburg, Germany)

CUING II

Towards Distributed Network Covert Channels Detection Using Data Mining-based Approach
Krzysztof Cabaj, Wojciech Mazurczyk, Piotr Nowakowski and Piotr Żórawski (Warsaw University of Technology, Poland)

Get Me Cited, Scotty! Analysis of Academic Publications in Covert Channel Research
Steffen Wendzel (Fraunhofer FKIE / Worms University of Applied Sciences, Germany)

CUING III

Towards Utilization of Covert Channels as a Green Networking Technique
Daniel Geisler (FernUniversitaet in Hagen, Germany), Wojciech Mazurczyk (Warsaw University of Technology, Poland) and Joerg Keller (FernUniversitaet in Hagen, Germany)

Enhanced Electromagnetic Side-channel Eavesdropping Attacks on Computer Monitors
Asanka Sayakkara, Nhien An Le Khac and Mark Scanlon (University College Dublin, Ireland)

The 2nd International Workshop on Security and Forensics of IoT (IoT-SECFOR 2018)

Welcome Message from the IoT-SECFOR Workshop Organizers

It is our great pleasure to welcome you to the 2nd International Workshop on Security and Forensics of IoT (IoT-SECFOR) which takes place in Hamburg (Germany) from 27 to 30 August 2018.

The main ambition of the workshop is to provide a venue and forum for researchers and practitioners, from both the security and forensics communities, to discuss problems and solutions regarding IoT. Internet-of-Things (IoT) are becoming increasingly prevalent in our society, as the backbone of interconnected smart homes, smart hospitals, smart cities, smart wearables and other smart environments. Such *things* leverage embedded technologies equipped with sensors and communication capabilities; they are able to broadcast their presence to other objects and interact with them using different protocols. Gartner predicts that, by 2020, 21 billion IoT endpoints will be in use. Along with usability, efficiency, and cost savings benefits, increasingly, the use of IoT poses security risks and raises challenges to digital forensics that need to be addressed.

Eight submissions were accepted for presentation and publication in this edition of IoT-SECFOR. They were organised in two sessions. The first session is more focused in IoT security assessment and analysis, while the second session is more focused on IoT security attacks and solutions.

The acceptance rate of this edition of the workshop was 57%.

The Workshop organizing committee

Virginia N. L. Franqueira, *University of Derby, UK*
Aleksandra Mileva, *University of Goce Delcev, Macedonia*
Ville Leppänen, *University of Turku, Finland*
Pedro Inácio, *Universidade da Beira Interior, Portugal*
Mauro Conti, *University of Padua, Italy*
Raul H. C. Lopes, *Brunel University, JISC & CMS/CERN, UK*

Publicity co-chairs

Chhagan Lal, *University of Padua, IT*
Chia-Mu Yu, *National Chung Hsing University, TW*

Workshop Program Committee IoT-SECFOR 2018

- Alberto Compagno, *Cisco Systems, France*
- Andrew Jones, *University of Hertfordshire, UK*
- Chhagan Lal, *University of Padua, Italy*
- Chia-Mu Yu, *National Chung Hsing University, Taiwan*
- Damien Magoni, *University of Bordeaux, France*
- Danilo Gligoroski, *Norwegian University of Science and Technology, Norway*
- Diogo Fernandes, *PepsiCo, Poland*
- George Grispos, *University of Nebraska Omaha, USA*
- Henrique Santos, *University of Minho, Portugal*
- Hugues Mercier, *University of Neuchatel, Switzerland*
- Judith Rossebo, *ABB AS, Norway*
- Katinka Wolter, *Freie Universität Berlin, Germany*
- Krzysztof Szczypiorski, *Warsaw University of Technology, Poland*
- Miguel Correia, *University of Lisbon, Portugal*
- Miguel Pardal, *University of Lisbon, Portugal*
- Moreno Ambrosin, *Intel Labs, USA*
- Patrik Ekdahl, *Ericsson AB, Sweden*
- Richard Hill, *University of Huddersfield, UK*
- Ricardo Neisse, *European Commission Joint Research Centre, Italy*
- Samuel Lauren, *University of Turku, Finland*
- Simona Bernardi, *Universidad de Zaragoza, Spain*
- Simona Samardjiska, *Radboud University, Netherlands*
- Vesna Dimitrova, *University Ss.Cyril and Methodius, Macedonia*

IoT-SECFOR 2018 Program

IoT-SECFOR I– Security Assessment & Analysis

Security Threats and Possible Countermeasures in Applications Covering Different Industry Domains

Musa Samaila, João Sequeiros, Mário Freire and Pedro Inácio (Instituto de Telecomunicações and Department of Computer Science, Universidade da Beira Interior, Covilhã, Portugal)

IoT-SECFOR II – Security Attacks & Solutions

Denial-of-Service Attacks on LoRaWAN

Eef van Es, Harald Vranken and Arjen Hommersom (Open University of the Netherlands, Netherlands)

Towards In-Network Security for Smart Homes

Martin Serror (RWTH Aachen University, Germany), Martin Henze (RWTH Aachen University, Germany), Sacha Hack (FH Aachen University of Applied Sciences, Germany), Marko Schuba (FH Aachen University of Applied Sciences, Germany) and Klaus Wehrle (RWTH Aachen University, Germany)

On Track of Sigfox Confidentiality with End-to-End Encryption

Radek Fujdiak (Brno University of Technology, Czech Republic), Petr Petr (Brno University of Technology, Czech Republic), Konstantin Mikhaylov (University of Oulu, Finland), Lukas Malina (Brno University of Technology, Czech Republic), Petr Mlynek (Brno University of Technology, Czech Republic), Jiri Misurec (Brno University of Technology, Czech Republic) and Vojtech Blazek (Brno University of Technology, Czech Republic)

Improved RNS-Based PRNGs

Alan Michaels (Virginia Tech, United States)

IoT-SECFOR III– Security Assessment & Analysis

Correlation Power Analysis on the PRESENT Block Cipher on an Embedded Device

Owen Lo (Edinburgh Napier University, United Kingdom), Bill Buchanan (Edinburgh Napier University, United Kingdom) and Douglas Carson (Keysight Technologies, United Kingdom)

Adding Salt to Pepper: A Structured Security Assessment over a Humanoid Robot

Alberto Giaretta (Örebro Universitet, Sweden), Michele De Donno (Technical University of Denmark, Denmark) and Nicola Dragoni (Technical University of Denmark, Denmark)

Towards Wireless Secret key Agreement with LoRa Physical Layer

Henri Ruotsalainen (St. Pölten University of Applied Sciences, Austria) and Stepan Grebeniuk (VACE Systemtechnik GmbH, Austria)

The 1st Interdisciplinary Privacy and Trust workshop (iPAT 2018)

Welcome Message from the iPAT Workshop Organizers

We are pleased to welcome you to the first edition of the Interdisciplinary Privacy and Trust workshop (iPAT), co-located with ARES 2018 in Hamburg.

iPAT aims to provide a platform to discuss privacy and trust - and not to the least their interplay - from an interdisciplinary perspective. The focus of the workshop lies on contributions that not only address the technical aspects of privacy and trust, but also consider the equally relevant challenges related to usability, psychology, economy, sociology, philosophy, and law.

We have selected the best four of the nine received submissions for presentation with the help of a double-blind peer-review process; at least two reviews have been provided for each submission. The accepted papers will be presented in one session. An introductory keynote will precede the paper session and set the stage. We encourage every participant to contribute their thoughts on interdisciplinary approaches to privacy and trust, seizing the various opportunities for discussions provided throughout our workshop.

We would like to thank our invited speaker for sharing their vision, the program committee for their careful reviews, as well as the ARES organization team for their efforts and kind assistance.

A special thank you goes to all authors for submitting their contributions. Researching a topic from multiple, oftentimes very different perspectives is challenging at its best and requires you to place yourself outside of your research comfort zone and community.

Despite its importance, interdisciplinary research is often times underappreciated. So lastly, we would like to thank all attendees for showing their interest in interdisciplinary research and hope iPAT will be a lively and inspiring forum, and a milestone on our journey towards a truly interdisciplinary understanding of the much needed support for privacy and trust in the digital world. Enjoy!

Workshop and Program Chairs

Prof. Dr. Max Mühlhäuser	Prof. Dr. Stephen Marsh
TU Darmstadt, Germany	*University of Ontario, Canada*

Workshop Organizing Committee iPAT 2018

- Spyros Boukoros, *TU Darmstadt, Germany*
- Jacqueline Brendel, *TU Darmstadt, Germany*
- Dr. Jörg Daubert, *TU Darmstadt, Germany*
- Nina Gerber, *KIT, Germany*
- Tim Grube, *TU Darmstadt, Germany*

iPAT 2018 Program

iPAT I

The user-centered privacy-aware control system PRICON: An interdisciplinary evaluation
Jonas Walter (TU Darmstadt, Germany), Bettina Abendroth (TU Darmstadt, Germany), Thilo von Pape (Université de Franche-Comté, France), Christian Plappert (Fraunhofer, Germany), Daniel Zelle (Fraunhofer, Germany), Christoph Krauß (Fraunhofer, Germany), Gundula Gagzow (Unabhängiges Landeszentrum für Datenschutz, Germany) and Hendrik Decke (Volkswagen, Germany)

User privacy attitudes regarding proximity sensing
Håkan Jonsson (Lund University, Sweden) and Carl Magnus Olsson (Malmö University, Sweden)

Critical Analysis of LPL according to Articles 12 - 14 of the GDPR
Armin Gerl and Dirk Pohl (Universität Passau, Germany)

Privacy and DRM Requirements for Collaborative Development of AI Applications
Vida Ahmadi Mehri, Dragos Ilie and Kurt Tutschku (Blekinge Institute of Technology, Sweden)

The 1st International Workshop on Security Engineering for Cloud Computing (IWSECC 2018)

Welcome Message from the IWSECC Workshop Organizers

The International Workshop on Security Engineering for Cloud Computing (IWSECC 2018) have a hybrid approach that will combine a traditional scientific workshop with an interactive forum for discussion of the main workshop topics, seeking the creation of a community and a clear focus on producing tangible results and making an impact on the situation of web service security and assurance.

From the received submissions, we have selected the 4 best for presentation. These presentations have been grouped into 2 sessions. The first session deals with Security Engineering topics for cloud and the second session deals with actual implementations.

We are very grateful to Yvonne Poul and Bettina Bauer for their kind assistance, support and help.

The Workshop organizing committee

ANTONIO MUÑOZ (Session Chairman),*University of Málaga, Spain*
CARSTEN RUDOLPH, *Monash University, Australia*

Workshop Program Committee IWSECC 2018

- BOYD, COLIN, *Queensland U. of Tech., Australia*
- CUELLAR, JORGE, *Siemens, Germany*
- DAVIDS, CAROL, *Illinois Institute of Technology, USA*
- DUSIT NIYATO, *Nanyang Technological U., Singapore*
- FERNANDEZ, EDUARDO B., *Florida Atlantic U., USA*
- GIORGINI, PAOLO, *University of Trento, Italy*
- GRAWROCK, DAVID, *Intel, USA*
- GÜRGENS, SIGRID, *Fraunhofer SIT, Germany*
- JÜRJENS, JAN, *TU of Dortmund, Germany*
- KIYOMOTO, SHINSAKU, *KDDI R&D Labs, Japan*
- KOTENKO, IGOR, *SPIIRAS and ITMO University, Russia*
- LAMBRINOUDAKIS, COSTAS*, U. of Piraeus, Greece*
- LEVI, ALBERT, *Sabanci University, Turkey*
- LOPEZ-MUÑOZ, Javier, *University of Málaga, Spain*
- LOSAVIO, MICHAEL, *U. of Kentucky, USA*
- LOTZ, VOLKMAR, *SAP AG, France*
- MARTINELLI, FABIO, *CNR-IIT, Italy*
- MARTINEZ-PEREZ, GREGORIO, *U. of Murcia, Spain*
- MICHELE BEZZI, *SAP, France*
- NADARAJAM, R., *PSG College of Technology, India*
  POSEGGA, JOAQUM, *U. of Passau, Germany*
- PRESENZA, DOMENICO, *Engineering, Italy*
- QUISQUATER, JEAN-JACQUES, *U. Catholique De Louvain, Belgium*
- RAY, INDRAKSHI, *Colorado State University, USA*
- SABETTA, ANTONINO, *SAP, France*
- SENG-PHIL, HONG, *Sungshin Women's University, Korea*
- WEISONG SHI, *Wayne State University, USA*
- SORIA-RODRIGUEZ, PEDRO, *ATOS R&D, Spain*
- SKIANIS CHARALABOS, *University of Aegean, Greece*
- SPANOUDAKIS, GEORGE, *City University, UK*
- WASHIZAKI, HIRONORI, *Waseda University, Japan*
- WESPI, ANDREAS, *IBM, Switzerland*
- YOSHIOKA, NOBUKAZU, *Nat. I. of Informatics, Japan*
- ZHANG, TAO, *Cisco, USA*
- ZULKERNINE, MOHAMMAD, *Queen's U., Canada*

IWSECC 2018 Program

IWSECC I – Security Implementations for Cloud Computing

A Process Framework for Stakeholder-specific Visualization of Security Metrics

Tanja Hanauer (Leibniz-Rechenzentrum der BAdW, Germany), Wolfgang Hommel (Universität der Bundeswehr München, Germany), Stefan Metzger (Leibniz-Rechenzentrum der BAdW, Germany) and Daniela Pöhn (Fraunhofer-Institut für Angewandte und Integrierte Sicherheit, Germany)

Security Wrapper Orchestration in Cloud

Aapo Kalliola (Nokia Bell Labs, Finland), Shankar Lal (Aalto University,Finland), Kimmo Ahola (VTT Technical Research Centre of Finland, Finland), Ian Oliver (Nokia Bell Labs, Finland), Yoan Miche (Nokia Bell Labs, Finland) and Tuomas Aura (Aalto University, Finland)

A Simulation Tool for Cascading Effects in Interdependent Critical Infrastructures

Stefan Rass, Thomas Grafenauer (Universitaet Klagenfurt, Austria), Sandra König and Stefan Schauer (Austrian Institute of Technology, Austria)

IWSECC II – Security Engineering Solutions for Cloud Computing

A reference architecture for the container ecosystem

Madiha Syed and Eduardo B. Fernandez (Florida Atlantic University, United States)

Evolution Oriented Monitoring oriented to Security Properties for Cloud Applications

Jamal Toutouh (University of Malaga, Spain), Antonio Muñoz (University of Malaga, Spain) and Sergio Nesmachnow (Universidad de la Républica – Engineering Faculty, Uruguay)

The 1st Workshop on Security and Privacy-Enhanced Big Data (SPEBD 2018)

Welcome Message from SPEBD Workshop Organizers

The Workshop on Security and Privacy-Enhanced Big Data (SPEBD 2018) aims to highlight emerging security and privacy challenges as enterprises continue to adopt and incorporate big data capabilities and technologies into business operations. The workshop highlights research into technologies and techniques that will mitigate these challenges. In an age when news of large data breaches, impacting many millions of people around the world, has become commonplace, the workshop organizers maintain that individuals and organizations need not relinquish expectations of security and privacy in order to live in a society that makes use of the power of big data analytics.

SPEBD 2018 is affiliated with the Homomorphic Encryption Standardization Consortium, a coalition of personnel from across academia, industry, and government that are seeking to bring the technology into mainstream use. We would like to express their gratitude to the Consortium for support in helping to publicize the workshop in 2018 and going forward.

Finally, we would like to express our sincere thanks to the ARES Conference, in particular Yvonne Paul and Julia Pammer, for their assistance leading up to the conference and workshop.

The Workshop organizing committee

Roger A. Hallman
SPEBD 2018 Co-Chair
SPAWAR Systems Center Pacific, San Diego, California, USA

Jason R.C. Nurse
SPEBD 2018 Co-Chair
University of Oxford, UK

Victor Chang
SPEBD 2018 Co-Chair
Xi'an Jiaotong-Liverpool University, Souzhou, China

Workshop Program Committee SPEBD 2018

- David Archer, *Galois, Inc., USA*
- Oliver Buckley, *University of East Anglia, UK*
- Hao Chen, *Microsoft Research, USA*
- Tiago Cruz, *University of Coimbra, Portugal*
- Mamadou Diallo, *SPAWAR Systems Center Pacific, USA*
- Hongxin Hu, *Clemson University, USA*
- Taeho Jung, *University of Notre Dame, USA*
- Kim Laine, *Microsoft Research, USA*
- Iván Palomares *Carrascosa, University of Bristol, UK*
- Kurt Rohloff, *New Jersey Institute of Technology, USA*
- Paulo Simões, *University of Coimbra, Portugal*

SPEBD 2018 Program

SPEBD I

Secure Fixed-point Division for Homomorphically Encrypted Operands
Chibuike Ugwuoke, Zekeriya Erkin and Reginald Lagendijk (Delft University of Technology, Netherlands)

Attribute Based Content Security and Caching in Information Centric IoT
Nurefsan Sertbas (Bogazici University, Turkey), Samet Aytac (Bogazici University, Turkey), Orhan Ermis (Bogazici University, Turkey), Gurkan Gur (ZHAW Zurich University of Applied Sciences, Switherlands) and Fatih Alagoz (Bogazici University, Turkey)

Evidence Identification in Heterogenous Data Using Clustering
Hussam Mohammed, Nathan Clarke and Fudong Li (University of Plymouth, United Kingdom)

The 1st International Workshop on Cyber Threat Intelligence (WCTI2018)

Welcome Message from the WCTI Workshop Organizers

In order to effectively defend a system against malicious activities, information about the nature of the adversaries, their available skills and resources is essential. Without this information, we run the risk that the portfolio of countermeasures does not turn out to be adequate to thwart off cyber threats, or that the defender deploys unnecessary resources.

Cyber Threat Intelligence is an emerging new discipline, which aims to develop methods and techniques to assemble information about compromises, extract information about the infrastructure and tools used, investigate adversarial techniques and practices and their evolution, structure and share this information and thus help detect and prevent future incidents.

WCTI brings together experts from academia, industry, government and law enforcement who are interested to advance the state of the art in cyber threat intelligence. The aim of the workshop is to present mature and early stage ideas, promote discussion and exchange, and build a community of researchers and practitioners in cyber threat intelligence. Discussions within the workshop will hopefully lead to joint activities in the future towards addressing shared problems.

Christian Doerr
TU Delft, Netherlands

Thomas Quilinan
Thales Research and Technology, Netherlands

Workshop Program Committee WCTI 2018

- Sean Moore, Centripetal Networks, USA
- Alexandre Dulaunoy, Computer Incident Response Center, Luxemburg
- Paul Samwel, Rabobank, Netherlands
- Christian Doerr, TU Delft, Netherlands
- Thomas Quillinan, Thales, Netherlands

WCTI 2018 Program

WCTI I

CRUSOE: Data Model for Cyber Situation Awareness
Jana Komárková, Martin Husák, Martin Laštovička and Daniel Tovarňák (Masaryk University, Czech Republic).

Integrating Threat Intelligence to Enhance an Organization's Information Security Management
Mathias Gschwandtner (Leopold-Franzens University Innsbruck, Austria), Lukas Demetz (University of Applied Sciences Kufstein, Austria), Matthias Gander (Leopold-Franzens University Innsbruck, Austria) and Ronald Maier (Department of Information Systems, Production and Logistics Management, Austria)

MAL (the Meta Attack Language): A Language for Domain-Specific Probabilistic Threat Modeling and Attack Simulation
Pontus Johnson, Robert Lagerström and Mathias Ekstedt (KTH Royal Institute of Technology, Sweden)

The 4th ARES 2018 EU Projects Symposium

Welcome to the ARES EU Projects Symposium!

The ARES EU Projects Symposium is held for the fourth time in conjunction with the ARES Conference.

The goal is to disseminate the results of EU research projects, meet potential project partners and exchange ideas within the scientific community.

This year, six workshops will be held within the ARES EU Projects Symposium:

- 3rd Workshop on Security, Privacy, and Identity Management in the Cloud (SECPID 2018)
- 1st International Workshop on 5G Networks Security (5G-NS 2018)
- 1st International Workshop on Cyber Threat Intelligence Management (CyberTIM 2018)
- 1st International Workshop on Organized Cybercrime, Cybersecurity and Terrorist Networks (IWOCCTN 2018)
- 1st International Workshop on European projects Clustering workshop On Cybersecurity and Privacy (ECoSP 2018)
- 1st International Workshop on Physical and Cyber Security in Port Infrastructures (PCSCP 2018)

We would like to thank the workshop organizers for their great efforts and hard work in proposing the workshop, selecting the papers, the interesting programs and for the arrangements of the workshops during the conference days.

We hope you enjoy the ARES EU Projects Symposium!

Edgar Weippl
SBA Research, Austria

The 3rd International Workshop on Security, Privacy, and Identity Management in the Cloud (SECPID 2018)

Welcome Message from the SECPID Workshop Organizers

Over the last years, the computing paradigm has experienced a massive shift from local to cloud-based applications. As a result, users and organizations do no longer have full control over their data and services, but they rely on third-party cloud providers.

This development poses various challenges concerning the integrity and confidentiality of data as well as the privacy of users of such systems. Currently, no satisfactory solutions to these challenges exist, which is a roadblock for the large-scale deployment of cloud-based applications handling sensitive data such as electronic health records.

As in previous years, the purpose of SECPID is therefore to provide a platform to present and discuss innovative ideas related to security, cryptography, trust, and identity management in and for the cloud.

SECPID was jointly organized by the EU-H2020 projects CREDENTIAL and PRISMACLOUD, together with the DPSP cluster on data protection, security, and privacy, which was in particular supported by the European projects MUSA and SWITCH. Furthermore, the would like to thank the TRUSTEE cluster of European cloud security and research projects.

We are looking forward to fruitful and interesting discussions in Hamburg!

The Workshop organizing committee

Stephan Krenn, *AIT Austrian Institute of Technology GmbH, Austria*
Thomas Lorünser, *AIT Austrian Institute of Technology GmbH, Austria*
Erkuden Rios Velasco, *Fundación Tecnalia Research & Innovation, Spain*

Workshop Program Committee SECPID 2018

- Manuel Barbosa, *University of Porto, Portugal*
- Jan Camenisch, *IBM Research – Zurich, Switzerland*
- Sherman S. M. Chow, *The Chinese University of Hong Kong, Hong Kong*
- Simone Fischer-Hübner, *Karlstad University, Sweden*
- Octavian Fratu, *University Politehnica of Bucharest, Romania*
- Thomas Gross, *Newcastle University, UK*
- Reto Koenig, *Bern University of Applied Sciences, Switzerland*
- Andreas Mauthe, *Lancaster University, United Kingdom*
- Henrich Pöhls, *University of Passau, Germany*
- Jetzabel Serna, *Goethe University Frankfurt, Germany*
- Alexandru Vulpe, *University Politehnica of Bucharest, Romania*
- Octavian Fratu, *University Politehnica of Bucharest, Romania*

In addition, the program committee was supported by the following subreviewers:

- Kai Samelin
- Christoph Striecks

SECPID 2018 Program

SECPID I

Fingerprint Recognition on Mobile Devices: Widely Deployed, Rarely Understood.
Farzaneh Karegar, John Sören Pettersson and Simone Fischer-Hübner (Karlstad University, Sweden)

Keys in the Clouds: Auditable Multi-device Access to Cryptographic Credentials.
Arseny Kurnikov (Aalto University, Finland), Andrew Paverd (Aalto University, Finland), Mohammad Mannan (Concordia University, Canada) and N. Asokan (Aalto University, Finland)

Definitions for Plaintext-Existence Hiding in Cloud Storage.
Colin Boyd (Norwegian University of Science and Technology, Norway), Gareth T. Davies (Norwegian University of Science and Technology, Norway), Kristian Gjøsteen (Norwegian University of Science and Technology, Norway), Håvard Raddum (Simula Research Laboratories, Norway) and Mohsen Toorani (University of Bergen, Norway)

Fully-Featured Anonymous Credentials with Reputation System.
Kai Bemmann, Jan Bobolz, Henrik Bröcher, Denis Diemert, Fabian Eidens, Lukas Eilers, Jan Haltermann, Jakob Juhnke, Burhan Otour, Laurens Porzenheim, Simon Pukrop, Erik Schilling, Michael Schlichtig and Marcel Stienemeier (Paderborn University, Germany)

The 1st International Workshop on 5G Networks Security (5G-NS 2018)

Welcome Message from the 5G-NS Workshop Organizers

With the great success and development of 4G mobile networks it is expected that the 5th generation wireless systems (in short 5G) will be a continued effort toward rich ubiquitous communication infrastructure, promising wide range of high-quality services. It is envisioned that 5G communication will offer significantly greater data bandwidth and almost infinite capability of networking resulting in unfaltering user experiences for (among others): virtual/augmented reality, massive content streaming, telepresence, user-centric computing, crowded area services, smart personal networks, Internet of Things (IoT), smart buildings, smart cities, to name just a few.

The 5G communication is currently in the center of attention of industry, academia, and government worldwide. 5G drives many new requirements for different network capabilities. As 5G aims at utilizing many promising network technologies, such as Software Defined Networking (SDN), Network Functions Virtualization (NFV), Information Centric Network (ICN), Network Slicing, Cloud Computing, etc. and supporting a huge number of connected devices integrating above mentioned advanced technologies and innovating new techniques will surely bring tremendous challenges for security, privacy and trust. Therefore, secure network architectures, mechanisms, and protocols are required as the basis for 5G to address this problem and follow security-by-design rule. Finally, as in 5G networks even more user data and network traffic will be transferred, the big data security solutions should be sought in order to address the magnitude of the data volume and to ensure data security and privacy.

From this perspective, 5G-NS 2018 workshop aims at collecting the most relevant ongoing research efforts in 5G networks security field. It also serves as a forum for 5G-PPP Phase 1 & Phase 2 projects in order to disseminate their security-related results and tighten & boost cooperation, and foster development of the 5G Security Community made of 5G security experts and practitioners who pro-actively discuss and share information to collectively progress and align on the field.

The Workshop organizing committee

Pascal Bisson, *Thales, France (5G-Ensure H2020 Project)*
Krzysztof Cabaj, *Warsaw University of Technology, Poland (IoRL H2020 Project)*
John Cosmas, *Brunel University, UK (IoRL H2020 Project)*
Wojciech Mazurczyk, *Warsaw University of Technology, Poland (IoRL H2020 Project)*

Workshop Program Committee 5G-NS 2018

- Michael Montag, *Nokia Bell Labs, Germany*
- Jani Suomalainen, *VTT, Finland*
- Thomas Carnehult, *RISE SICS, Sweden*
- Madhusanka Liyanage, *University of Oulu, Finland*
- Edgardo Montes de Oca, *Montimage, France*
- Georgios Karopoulos, *National and Kapodistrian University of Athens, Greece*
- Gino Carrozzo, *Nextworks, Italy*
- Jin Hong, *University of Western Australia, Australia*
- Gregory Blanc, *Télécom SudParis, Institut Mines-Télécom, France*
- Gregorio Martinez-Perez, *University of Murcia, Spain*
- Joo Cho, *Adva Optical, Germany*
- Seungwon Shin, *KAIST, Korea*
- Dhouha Ayed, *Thales, France*
- Peter Schneider, *Nokia Bell Labs, Germany*
- Luca Caviglione, *CNR, Italy*
- Hui Tian, *National Huaqiao University, China*
- Michal Choras, *ITTI Ltd., Poland*
- Zbigniew Kotulski, *Warsaw University of Technology, Poland*

5G-NS 2018 Program

5G-NS I

To Trust or Not to Trust: Data Origin Authentication for Group Communication in 5G Networks
Robert Annessi, Joachim Fabini and Tanja Zseby (Vienna University of Technology, Austria)

Universal Trusted Execution Environments for Securing SDN/NFV Operations
Vincent Lefebvre (tages sas, France), Gianni Santinelli (tages sas, Italy), Tilo MÜller (FAU Erlangen-Nürnberg, Germany) and Johannes Götzfried (FAU Erlangen-Nürnberg, Germany)

Enhancing NFV Orchestration with Security Policies
Christian Banse and Florian Wendland (Fraunhofer, Germany)

Identity and Access Control for micro-services based 5G NFV platforms
Daniel Guija and Muhammad Shuaib Siddiqui (i2CAT, Spain)

5G-NS II

Towards a 5G Security Architecture: Articulating Software-Defined Security and Security as a Service
Gregory Blanc (Institut Mines-Télécom, Télécom SudParis, France), Nizar Kheir (Thales Group, France), Dhouha Ayed (Thales Group, France), Vincent Lefebvre (Tages SAS, France), Edgardo Montes de Oca (Montimage, France) and Pascal Bisson (Thales Group, France)

A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation
Marco Antonio Sotelo Monge, Jorge Maestre Vidal and Luis Javier García Villalba (Universidad Complutense de Madrid, Spain)

SDN-based Mitigation of Scanning Attacks for the 5G Internet of Radio Light System
Krzysztof Cabaj, Marcin Gregorczyk, Wojciech Mazurczyk, Piotr Nowakowski and Piotr Żórawski (Warsaw University of Technology, Poland)

5G-NS III

Detecting Workload-based and Instantiation-based Economic Denial of Sustainability on 5G environments
Jorge Maestre Vidal, Marco Antonio Sotelo Monge and Luis Javier García Villalba (Universidad Complutense de Madrid, Spain)

Framework for Security Event Management in 5G
Iris Adam (Nokia Bell Labs, Germany) and Jing Ping (Nokia Software, China)

1st International Workshop on Cyber Threat Intelligence Management (CyberTIM 2018)

Message from the CyberTim Workshop Organizers

It is our great pleasure to welcome you to the first International Workshop on Cyber Threat Intelligence Management (CyberTIM) which takes place in conjunction with the ARES EU Project Symposium and the ARES conference in Hamburg, Germany from 27-30 of August 2018.

The increased sophistication of cyber-attacks have created a technology arm race between attackers and defenders. However, this arm race is not fought in equal terms. Defenders are falling behind due to lack of manpower coupled with an overwhelming number of sophisticated attacks, e.g. advanced persistent threats, making cyber defense extremely difficult. This is also due to lack of collaboration among the network security solutions, e.g., intrusion detection systems and honeypots, which are in possession of different organizations across the globe. In the recent years, organizations like CERTs, NRENs, as well as industry organizations slowly move towards proactive detection capabilities leveraging Cyber Threat Intelligence (CTI) platforms. These platforms aim at advanced alert aggregation, correlation, and prioritization considering the asset criticality of organizations as well as the quality of shared threat intelligence.

CyberTIM is bridging the gap between researchers, industry practitioners and engineers from the domains of network security, network measurements, cyber incident monitoring, trust and risk management, cyber situational awareness, security analytics, and security visualization.

The CyberTIM workshop is jointly organized by three H2020 projects that are funded by the European Commission:

- **PROTECTIVE** (https://protective-h2020.eu/)
- **C3ISP** (c3isp.eu/)
- **SHIELD** (https://www.shield-h2020.eu/)

From the received submissions (18 papers) and after an in-depth review process, as well as discussions of the organizing committee, we have decided to accept the **eight** best papers for presentation in the workshop. This results to an acceptance rate of 44%. We separate the talks into two main blocks on the basis of the topics, namely: i) **attack detection and mitigation** and ii) **threat intelligence sharing**. Lastly, we are grateful to Prof. Dr. Kim-Kwang Raymond Choo as well as Prof. Dr. Hervé Debar for their agreement to give keynote talks.

The Workshop organizing committee

Brian Lee, *Athlone Institute of Technology, Ireland*
Emmanouil Vasilomanolakis, *Technische Universität Darmstadt, Germany*
Fabio Martinelli, *IIT, C.N.R, Italy*
Georgios Gardikis, *SPACE Hellas S. A., Greece*
Sheikh Mahbub Habib*, Technische Universität Darmstadt, Germany*

Workshop Program Committee CyberTim 2018

- Hamza Attak, *Hewlett Packard Enterprise, United Kingdom*
- Enda Barrett, *National University of Ireland, Galway, Ireland*
- David Chadwick, *University of Kent, United Kingdom*
- Michal Choras, *ITTI Ltd., Poland*
- Francesco Di Cerbo, *SAP Research Sophia-Antipolis, France*
- Theo Dimitrakos, *European Security Competence Center, Huawei Technologies, United Kingdom*
- Bernat Gaston, *Fundació Privada I2CAT, Spain*
- Jassim Happa, *University of Oxford, United Kingdom*
- Dimitris Katsianis, *Incites Consulting, Luxembourg*
- Antonis Litke, *Infili Technologies, Greece*
- Maciej Miłostan, *PSNC, Poznań University of Technology, Poland*
- Paolo Mori, *IIT-CNR, Italy*
- Jason Nurse, *University of Oxford, United Kingdom*
- Dimitris Papadopoulos, *Infili Technologies, Greece*
- Marcin Przybyszewski, *ITTI Sp. z o.o., Poznań, Poland*
- Olga Segou, *Orion Innovations PC, Greece*
- George Xylouris, *ORION Innovations PC, Greece*

CyberTIM 2018 Program

CyberTIM I - Attack Detection and Mitigation

Evaluation of Apache Spot's machine learning capabilities in an SDN/NFV enabled environment

Christos M. Mathas (University of Peloponnese, Greece), Olga E. Segou (Orion Innovations PC, Greece), Georgios Xylouris (Orion Innovations PC, Greece), Dimitris Christinakis (Orion Innovations PC, Greece), Michail – Alexandros Kourtis (Institute of Informatics and Telecommunications National Centre for Scientific Research "Demokritos", Greece), Costas Vassilakis (University of Peloponnese, Greece) and Anastasios Kourtis (Institute of Informatics and Telecommunications National Centre for Scientific Research "Demokritos", Greece)

Towards an Automated Recognition System for Chat-based Social Engineering Attacks in Enterprise Environments

Nikolaos Tsinganos, George Sakellariou, Panagiotis Fouliras and Ioannis Mavridis (University of Macedonia, Greece)

Augmented DDoS Mitigation with Reputation Scores

Tomáš Jánský (Faculty of Information Technology, CTU in Prague, Czech Republic), Tomáš Čejka (Faculty of Information Technology, CTU in Prague, Czech Republic), Martin Žádník (CESNET a.l.e., Czech Republic) and Václav Bartoš (CESNET a.l.e., Czech Republic)

The challenge of detecting sophisticated attacks: Insights from SOC Analysts

Olusola Akinrolabu, Ioannis Agrafiotis and Arnau Erola (University of Oxford, United Kingdom)

CyberTIM II - Threat Intelligence Sharing

Mission-Centric Risk Assessment to Improve Cyber Situational Awareness

Franklin Silva and Paul Jacob (Athlone IT, Ireland)

The Mouseworld, a security traffic analysis lab based on NFV/SDN

Antonio Pastor (Telefonica I+D, Spain), Alberto Mozo Velasco (Universidad Politécnica de Madrid, Spain), Diego R. Lopez (Telefonica I+D, Spain), Jesús Luis Folgueira (Telefonica I+D, Spain) and Georgios Gardikis (Space Hellas S.A., Greece)

Risks of Sharing Cyber Incident Information

Adham Albakri (University of Kent, United Kingdom), Eerke Boiten (De Montfort University, United Kingdom) and Rogério de Lemos (University of Kent, United Kingdom)

Hunting Observable Objects for Indication of Compromise

Arnold Sykosch, Michael Meier and Marc Ohm (University of Bonn, Germany)

The 1st International Workshop on Organized Cybercrime, Cybersecurity and Terrorist Networks (IWOCCTN 2018)

Welcome Message from the IWOCCTN Workshop Organizers

We would like to offer our warm welcome to the International Workshop on Organized Cybercrime, Cybersecurity and Terrorist Networks (IWOCCTN 2018) co-located with ARES 2018.

Organized (cyber-)crime (OC) and terrorist networks (TN) are major threats for the European Union and its population. On the one hand, the number and value of assets confiscated from organized crime are more and more increasing in Europe, which indicates its rise in Europe and its challenge of the legal economy or tax base of many nation states. On the other hand, Europe is facing an increasing number of individuals, who are recruited as foreign fighters or for terrorist attacks within Europe. In addition, the direct implications, an atmosphere of fear is created. Additionally, the economic costs for prevention and fighting OC and TN are increasing. This is particularly relevant in times of austerity measures, when the reduction of integration programs and support of marginalized groups is increasing the boundaries between the milieus. Even in allegedly "egalitarian" societies, the entrenchment within societies is increasing and producing classes of "left-behinds" with no chance for upwards social mobility. And it is often young people with no future perspectives, who are at risk of becoming engaged in criminal organizations or in terrorist networks. It is the combination of these challenges and respective policies, which are ultimately challenging social cohesion in Europe. Towards such field are currently devoted several research projects such as TAKEDOWN, a European Research project, where 18 European partners (ranging from Academy, Industry and Law Enforcement Agency) aims to analyze and get a deeper knowledge on OC and TN in order to advance the State-of-the-art and providing more effective digital and non-digital solutions for first line practitioners, law enforcement agencies and policy makers.

In this perspective, the IWOCCTN Workshop aims at (i) bringing together Experts, Solution Providers and Professionals, in different fields of Security; (ii) promoting and disseminating existing tools in terms of digital and non-digital solutions ranging from models, methods, methodologies, approaches, technologies and services and discussing their possible involvement against OC and TN; as well as (iii) discussing and evaluating their societal and ethical impact and related issues.

The Workshop organizing committee

Matteo Bonfanti, *ETH Center for Security Studies, Switzerland*

Andrea Tundis, *Technische Universität Darmstadt, Germany*

Workshop Program Committee IWOCCTN 2018

- Maxim Anikeev, *Southern Federal University, Russia*
- Matteo Bonfanti, *ETH Center for Security Studies, Switzerland*
- Florian Huber, *SYNYO, Austria*
- Bernhard Jäger, *SYNYO, Austria*
- Wojciech Mazurczyk, *Warsaw University of Technology, Poland*
- Andrej Pastorek, *Czech Technical University in Prague, Czech Republic*
- Karin Ranier, *Agency for European Integration and Economic Development, Austria*
- Antonio Segura Serrano, *Universidad de Granada, Spain*
- Diana Silvestru, *Agency for European Integration and Economic Development, Austria*
- Andrea Tundis, *Technische Universität Darmstadt, Germany*
- David Wall, University of Leeds, United Kingdom

IWOCCTN 2018 Program

IWOCCTN I – Cyber Organized Crime and Terrorism

Conceptualizing the digital TAKEDOWN platforms for supporting first-line-practitioners and law enforcement agencies
Florian Huber (SYNYO GmbH, Austria)

Cybercrime and Organized Crime
Václav Jirovský and Andrej Pastorek (Czech Technical University, Czech Republic)

The AWID and TAKEDOWN prevention approach. The generation of a holistic good practice model for prevention of radicalization in youth work
Karin Rainer, Mario Springnagel and Diana Silvestru (Agency for European Integration and Economic Development, Austria)

IWOCCTN II – Cyber Security

Challenges of Cryptocurrencies Forensics – A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals
Syed Naqvi (Birmingham City University, United Kingdom)

Enhancing Cyber-Security by Safeguarding Information Privacy: the European Union and the Implementation of the "Data Protection by Design" Approach
Matteo E. Bonfanti (ETH Center for Security Studies, Switzerland)

A review of network vulnerabilities scanning tools: types, capabilities and functioning
Andrea Tundis (TU Darmstadt, Germany), Wojciech Mazurczyk (Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications, Poland) and Max Mühlhäuser (TU Darmstadt, Germany)

The 1st projects Clustering workshop On Cybersecurity and Privacy (ECoSP 2018)

Welcome Message from the ECoSP Workshop Organizers

We would like to offer our warm welcome to the *European projects Clustering workshop on cyber-Security and Privacy* (ECoSP 2018).

Cybersecurity and Privacy issues are becoming an important barrier for a trusted and dependable global digital society development. The European Union is addressing the challenge through different means, including the Horizon 2020 Research and Innovation program, thereby financing innovative projects that can cope with the increasing cyberthreat landscape. This workshop promotes international dialogue and cooperation among H2020 European research projects aimed to cope with digital security and privacy aspects, risks, threats and cybersecurity issues.

The ECoSP workshop intents to emphasize the interplay within relative European Research projects in the field of privacy and security as well as related cybersecurity issues and challenges, and therefore, establishing tight connections among the EU projects.

This clustering workshop is organized by ARIES and LIGHTest H2020 projects coordinating several presentations from different EU R&D projects articulated around security and privacy fields. The workshop enables that experts can present and exchange their views in the latest advances and challenges about security and privacy, giving the audience the opportunity to interact with the speakers.

Representatives of several H2020 European research projects (16 confirmed) in the scope of Security and Privacy will present their latest research advances, challenges, techniques and outcomes in the scope of their projects.

The Workshop organizing committee:

Jorge Bernal Bernabé
University of Murcia

Antonio Skarmeta Gomez
University of Murcia

Jon Shamah
EEMA

EU projects participating in ECoSP 2018:

- **Block 1- Cybersecurity:** ANASTACIA, SAINT, YAKSHA, FORTIKA, CYBECO, SISSDEN, CIPSEC, CS-AWARE, RED-Alert, TRUESSEC.EU
- **Block 2- Privacy and Trust:** ARIES, LIGHTest, CREDENTIAL , LEPS, FutureTrust, SPECIAL

The 1st International Workshop on Physical and Cyber Security in Port Infrastructures (PCSCP 2018)

Welcome Message from the IWOCCTN Workshop Organizers

Nowadays, coordinated and every time more complex terrorist attacks are shocking the world. Due to the progressive dependency of the industrial sector and many critical infrastructures, particularly EU port infrastructures, on ICT systems, the impact of a coordinated physical attack, a deliberate disruption of critical automation systems or even a combined scenario could have disastrous consequences for the European Member States' regions and social wellbeing in general.

In our Workshop on Physical and Cyber Security in Port Infrastructures (PSCSP 2018), we want to present novel approaches for situational awareness stemming from the current H2020 research Project SAURON. These approaches support port operators to increase the protection and resilience for EU ports against physical and cyber threats to an adequate level. This concept of a Hybrid Situational Awareness capable of determining the potential consequences of any threat allows to identify potential cascading effects of a detected threat in the physical and the cyber domain.

The workshop starts with a short introduction into the SAURON project to set the general scenario of physical, cyber and Hybrid Situational Awareness. Then, two presentations provide an in-depth overview on the main parts of the Hybrid Situational Awareness, i.e., the event correlation and the threat propagation. A short outline of one of the SAURON use case scenarios describes how the SAURON system can be applied in praxis. The last presentation gives an overview on the legal aspects of situational awareness under current EU legislation.

Finally, our special thanks are due to Yvonne Poul and Julia Pammer for their kind assistance and help.

Stefan Schauer
PSCSP 2018 Workshop Chair
AIT Austrian Institute of Technology, Austria

Rafa Company
PSCSP 2018 Workshop Chair
Fundación Valenciaport, Spain

Federico Carvajal
PSCSP 2018 Workshop Chair
Universidad Politécnica de Valencia, Spain

Richard Chisnall
PSCSP 2018 Workshop Chair
Innovasec, UK

ARES Full Papers

ARES Full I - Machine Learning

A1: Modular Convolutional Neural Network for Discriminating between Computer-Generated Images and Photographic Images

Hong-Huy Nguyen (SOKENDAI (The Graduate University for Advanced Studies), Japan), Ngoc-Dung Tieu-Thi (SOKENDAI (The Graduate University for Advanced Studies), Japan), Hoang-Quoc Nguyen-Son (National Institute of Informatics, Japan), Vincent Nozick (Japanese-French Laboratory for Informatics (JFLI) (UMI 3527), Japan), Junichi Yamagishi (National Institute of Informatics, Japan) and Isao Echizen(National Institute of Informatics, Japan)

A2: FALKE-MC: A Neural Network Based Approach to Locate Cryptographic Functions in Machine Code

Alexander Aigner (University of Applied Sciences Upper Austria, Austria)

ARES Full II - Best Paper Session

A3: Secure Equality Testing Protocols in the Two-Party Setting

Majid Nateghizad (Delft University of Technology, Netherlands), Thijs Veugen (TNO, Netherlands), Zekeriya Erkin (Delft University of Technology, Netherlands) and Reginald L. Lagendijk (Delft University of Technology, Netherlands)

A4: Android authorship attribution through string analysis

Vaibhavi Kalgutkar (University of New Brunswick, Canada), Natalia Stakhanova (University of New Brunswick, Canada), Paul Cook (University of New Brunswick, Canada) and Alina Matyukhina (University of New Brunswick, Canada)

A5: Flashlight: A Novel Monitoring Path Identification Schema for Securing Cloud Services

Heng Zhang (DEEDS Group, Department of Computer Science, TU Darmstadt, Germany), Ruben Trapero (Atos Research & Innovation, Spain), Jesus Luna Garcia (TU Darmstadt, Germany) and Neeraj Suri (TU Darmstadt, Germany)

ARES Full III - Software Security

A6: Discovering software vulnerabilities using data-flow analysis and machine learning

Jorrit Kronjee, Arjen Hommersom and Harald Vranken (Open University of the Netherlands, Netherlands)

A7: Speeding Up Bug Finding using Focused Fuzzing

Ulf Kargén and Nahid Shahmehri (Linköping University, Sweden)

A8: HYDRA- Hypothesis Driven Repair Automation

Partha Pal, Brett Benyo, Shane Clark and Aaron Paulos (Raytheon BBN, United States)

ARES Full IV - Security and the User

A9: Protecting Patients' Data: An Efficient Method for Health Data Privacy

Mark Daniels, John Rose and Csilla Farkas (University of South Carolina, United States)

A10: Influence Factors on the Quality of User Experience in OS Reliability: A Qualitative Experimental Study

Caio Augusto Rodrigues Dos Santos, Daniela Yabe, Lucas Miranda and Rivalino Matias (Federal University of Uberlandia, Brazil)

ARES Full V - Cryptography

A11: Finally Johnny Can Encrypt. But Does This Make Him Feel More Secure?

Nina Gerber (KIT, Germany), Verena Zimmermann (TU Darmstadt, Germany), Birgit Henhapl (TU Darmstadt, Germany), Sinem Emeröz (TU Darmstadt, Germany) and Melanie Volkamer (KIT, Germany)

A12: An Efficient Cryptography-Based Access Control Using Inner-Product Proxy Re-Encryption Scheme

Masoomeh Sepehri (University of Milan, Italy), Maryam Sepehri (University of Milan, Italy), Alberto Trombetta (Università degli Studi dell'Insubria, Italy) and Ernesto Damiani (Khalifa University of Science and Technology, United Arab Emirates)

A13: Non-Interactive Key Exchange from Identity-Based Encryption

Olivier Blazy (Université de Limoges, France) and Céline Chevalier (ENS, France)

ARES Full VI - Anomaly Detection

A14: Behavioural Comparison of Systems for Anomaly Detection

Martin Pirker, Patrick Kochberger and Stefan Schwandter (St. Pölten UAS, Austria)

A15: Converting Unstructured System Logs into Structured Event List for Anomaly Detection

Zongze Li (University of north Texas, United States), Song Fu (University of north Texas, United States), Matthew Davidson (University of north Texas, United States), Sean Blanchard (Los Alamos National Laboratory, United States) and Michael Lang (Los Alamos National Laboratory, United States)

A16: Stealthy Attacks on Smart Grid PMU State Estimation

Sarita Paudel (AIT Austrian Institute of Technology, Austria), Tanja Zseby (Vienna University of Technology, Austria) and Paul Smith (AIT Austrian Institute of Technology, Austria)

ARES Full VII - Network Security and Monitoring I

A17: A Framework for Monitoring Net Neutrality

Wilfried Mayer (SBA Research, Austria), Thomas Schreiber (TU Wien, Austria) and Edgar Weippl (SBA Research, Austria)

A18: The Other Side of the Coin: A Framework for Detecting and Analyzing Web-based Cryptocurrency Mining Campaigns

Julian Rauchberger, Sebastian Schrittwieser, Tobias Dam, Robert Luh, Damjan Buhov, Gerhard Pötzelsberger (St. Pölten UAS, Austria) and Hyoungshick Kim (Sungkyunkwan University, South Korea)

ARES Full VIII - Network Security and Monitoring II

A19: A Pyramidal-based Model to Compute the Impact of Cyber Security Events

Gustavo Gonzalez (Atos, Spain), Jose Manuel Rubio Hernan (Télécom SudParis, CNRS UMR 5157 SAMOVAR, Université Paris-Saclay, France) and Joaquin Garcia-Alfaro (Télécom SudParis, CNRS UMR 5157 SAMOVAR, Université Paris-Saclay, France)

A20: ToGather: Towards Automatic Investigation of Android Malware Cyber-Infrastructures

Elmouatez Billah Karbab Karbab and Mourad Debbabi (Concordia University, Canada)

ARES Full IX - Automotive

A21: Attack Graph-Based Assessment of Exploitability Risks in Automotive On-Board Networks
Martin Salfer (Technical University of Munich, Germany) and Claudia Eckert (Technical University of Munich, Germany)

A22: Anonymous Charging and Billing of Electric Vehicles
Daniel Zelle, Markus Springer, Maria Zhdanova and Christoph Krauß (Fraunhofer, Germany)

A23: Comparison of Data Flow Error Detection Techniques in Embedded Systems: an Empirical Study
Venu Babu Thati (Katholieke Universiteit Leuven, Belgium), Jens Vankeirsbilck (Katholieke Universiteit Leuven, Belgium), Niels Penneman (Televic Healthcare, Belgium), Davy Pissoort (Katholieke Universiteit Leuven, Belgium) and Jeroen Boydens (Katholieke Universiteit Leuven, Belgium)

ARES Full X - Cloud Security

A24: Distributed and Cooperative firewall/controller in cloud environments
Ferdaous Kamoun-Abid (NTS'COM, ENET'COM, Tunisia), Amel Meddeb-Makhlouf (NTS'COM, ENET'COM, Tunisia), Faouzi Zarai (NTS'COM, ENET'COM, Tunisia) and Mohsen Guizani (ECE Department, University of Idaho, United States)

A25: Cloud Architectures for Searchable Encryption
Johannes Blömer and Nils Löken (University of Paderborn, Germany)

ARES Short Papers

ARES Short I - Malware

A26: An investigation of a deep learning based malware detection system
Mohit Sewak, Sanjay Sahay and Hemant Rathore (BITS, Pilani, Department of CS & IS, Goa Campus, India)

A27: Towards the Automatic Generation of Low-Interaction Web Application Honeypots
Marius Musch (TU Braunschweig, Germany), Martin Johns (TU Braunschweig, Germany) andMartin Härterich (SAP Security Research, Germany)

A28: Learning Malware Using Generalized Graph Kernels
Khanh Huu The Dam (LIPN and University Paris Diderot, France) and Tayssir Touili (LIPN, CNRS & University Paris 13, France)

ARES Short II - Monitoring

A29: Assessing Internet-wide Cyber Situational Awareness of Critical Sectors
Martin Husák (Masaryk University, Czech Republic), Nataliia Neshenko (Florida Atlantic University, United States), Morteza Safaei Pour (Florida Atlantic University, United States), Elias Bou-Harb (Florida Atlantic University, United States) and Pavel Čeleda (Masaryk University, Czech Republic)

A30: Spreading Alerts Quietly: New Insights from Theory and Practice
Olivier Blazy (Université de Limoges, France) and Céline Chevalier (ENS, France)

A31: A Reactive Defense Against Bandwidth Attacks Using Learning Automata
Nafiseh Kahani (Queen's Univeristy, Canada) and Mehran Fallah (Amirkabir University of Technology, Iran)

ARES Short III - Embedded Systems

A32: ATG: An Attack Traffic Generation Tool for Security Testing of In-vehicle CAN Bus

Tianxiang Huang (Chongqing University of Posts and Telecommunications, China), Jianying Zhou (Singapore University of Technology and Design, Singapore) and Andrei Bytes (Singapore University of Technology and Design, Singapore)

A33: Let's shock our IoT's heart: ARMv7-M under (fault) attacks

Sebanjila K. Bukasa (LHS-PEC INRIA-RBA, France), Ronan Lashermes (LHS-PEC INRIA-RBA, France), Jean-Louis Lanet (LHS-PEC INRIA-RBA, France) and Axel Legay (TAMIS INRIA-RBA, France)

A34: Enterprise WLAN Security Flaws: Current Attacks and Relative Mitigations

Mohamed Abo-Soliman and Marianne Azer (Nile University, Egypt)

ARES Short IV - Security Practices

A35: What are Security Patterns? A Formal Model for Security and Design of Software

Anika Behrens (University of Bremen, Germany)

A36: A Nlp-based Solution to Prevent from Privacy Leaks in Social Network Posts

Gerardo Canfora, Andrea Di Sorbo, Enrico Emanuele, Sara Forootani and Corrado A. Visaggio (University of Sannio, Italy)

A37: (In)Secure Configuration Practices of WPA2 Enterprise Supplicants

Alberto Bartoli (Università degli Studi di Trieste – DEEI, Italy), Eric Medvet (DI3 – University of Trieste, Italy), Fabiano Tarlao (Department of Engineering and Architecture, University of Trieste, Italy) and Andrea De Lorenzo (University of Trieste – DIA, Italy)

FARES 2018

FARES I - Protection and Detection

A38: Recovery of Encrypted Mobile Device Backups from Partially Trusted Cloud Servers

Omid Mir, Rene Mayrhofer, Michael Hölzl and Thanh-Binh Nguyen (Institute of Networks and Security, Johannes Kepler University, Austria)

A39: Reputation-Based Security System For Edge Computing

Francis Nwebonyi (University of Porto, Portugal), Rolando Martins (University of Porto, Portugal) and Manuel E. Correia (CRACS/INESC TEC; DCC/FCUP, Portugal)

A40: New authentication concept using certificates for big data analytic tools

Paul Velthuis (Fraunhofer-Institute-for-Secure-Information-Technology-SIT, Netherlands), Marcel Schäfer and Martin Steinebach (Fraunhofer-Institute-for-Secure-Information-Technology-SIT, Germany)

A41: Evaluation of Machine Learning-based Anomaly Detection Algorithms on an Industrial Modbus/TCP Data Set

Simon Duque Anton, Suneetha Kanoor, Daniel Fraunholz and Hans Dieter Schotten (Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Germany)

FARES II - Measurement and Robust Design

A42: X.509 Certificate Error Testing

David Mcluskie and Xavier Bellekens (Abertay University, United Kingdom)

A43: Evaluating the degree of security of a system built using security patterns

Eduardo B. Fernandez (Florida Atlantic University, United States), Nobukazu Yoshioka (National Institute of Informatics, Japan) and Hironori Washizaki (Waseda

A44: Attack Difficulty Metric for Assessment of Network Security

Preetam Mukherjee and Chandan Mazumdar (Jadavpur University, India)

A45: Robustness Estimation of Infrastructure Networks: On the Usage of Degree Centrality

Sebastian Wandelt and Xiaoqian Sun (Beihand University, China)

WSDF 2018

WSDF I

A46: Digital Forensics in the Next Five Years

Laoise Luciano, Mateusz Topor, Ibrahim Baggili and Frank Breitinger (University of New Haven, United States)

WSDF II

A47: Forensic APFS File Recovery

Jonas Plum (Siemens AG, Germany) and Andreas Dewald (ERNW Research GmbH, Germany)

A48: Volatile Memory Forensics Acquisition Efficacy: A Comparative Study Towards Analysing Firmware-Based Rootkits

Jacob Taylor, Benjamin Turnbull and Gideon Creech (The University of New South Wales, Australia)

A49: I Know What You Did Last Summer: Your Smart Home Internet of Things and Your iPhone Forensically Ratting You Out

Gokila Dorai (Florida State University, United States), Shiva Houshmand (Southern Illinois University, United States) and Ibrahim Baggili (University of New Haven, United States)

WSDF III

A50: Breaking down violence: A deep-learning strategy to model and classify violence in videos

Bruno Malveira Peixoto, Sandra Avila, Zanoni Dias and Anderson Rocha (Universidade Estadual de Campinas – Unicamp, Brazil)

A51: Digitally Signed and Permission Restricted PDF Files: a Case Study on Digital Forensics

Patricio Domingues and Miguel Frade (Instituto Politécnico de Leiria, Portugal)

A52: Investigating the Use of Online Open Source Information as Evidence in European Courts

Yi-Ching Liao (Noroff University College, Norway)

IWSMA 2018

IWSMA I

A53: Toward a Distributed Trust Management scheme for VANET

Amira Kchaou (SUPCOM, Tunisia), Ryma Abassi (SUPCOM, Tunisia) and Sihem Guemara El Fatmi (High School of Communication, Sup'Com, Tunisia)

A54: There Goes Your PIN: Exploiting Smartphone Sensor Fusion Under Single and Cross User Setting

David Berend (Nanyang Technological University, Singapore, University of Applied Sciences Wiesbaden, Rüsselsheim, Germany), Bernhard Jungk (Temasek Laboratories at Nanyang Technological University, Singapore) and Shivam Bhasin (Temasek Labs@NTU, Singapore)

A55: Towards a Privacy Preserving and Flexible Scheme for Assessing the Credibility and the Accuracy of Safety Messages Exchanged in VANETs

Ons Chikhaoui, Aida Ben Chehida Douss, Ryma Abassi and Sihem Guemara El Fatmi (Higher School of Communication, Sup'Com, Tunisia)

IWSMA II

A56: Practical Precise Taint-flow Static Analysis for Android App Sets

William Klieber, Lori Flynn, William Snavely and Michael Zheng (Carnegie Mellon Univ, Software Engineering Institute, United States)

A57: Detection of Obfuscation Techniques in Android Applications

Alessandro Bacci (Dipartimento di Ingegneria e Architettura – Università degli Studi di Trieste, Italy), Alberto Bartoli (Dipartimento di Ingegneria e Architettura – Università degli Studi di Trieste, Italy), Fabio Martinelli (Istituto di Informatica e Telematica – Consiglio Nazionale delle Ricerche, Pisa, Italy), Eric Medvet (Dipartimento di Ingegneria e Architettura – Università degli Studi di Trieste, Italy) and Francesco Mercaldo (Istituto di Informatica e Telematica – Consiglio Nazionale delle Ricerche, Pisa, Italy)

A58: Tackling Android's Native Library Malware with Robust, Efficient and Accurate Similarity Measures

Anatoli Kalysch, Mykolai Protsenko, Oskar Milisterfer and Tilo Müller (Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany)

IWCC 2018

IWCC I

A59: Monitoring Product Sales in Darknet Shops

York Yannikos (Fraunhofer, Germany), Annika Schäfer (TU Darmstadt, Germany) and Martin Steinebach (Fraunhofer, Germany)

A60: IoT Forensic: identification and classification of evidence in criminal investigations

François Bouchaud (IRCGN, France), Gilles Grimaud (IRCICA – CRIStAL, France) and Thomas Vantroys (IRCICA – CRIStAL, France)

IWCC II

A61:Recent Granular Computing Implementations and its Feasibility in Cybersecurity Domain

Marek Pawlicki (UTP Bydgoszcz, Poland), Michal Choras (ITTI Ltd., Poland) and Rafal Kozik (Institute of Telecommunications, UTP Bydgoszcz, Poland)

A62: Determination of Security Threat Classes on the basis of Vulnerability Analysis for Automated Countermeasure Selection

Elena Doynikova, Andrey Fedorchenko and Igor Kotenko (St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Russia)

A63: A New Classification of Attacks against the Cyber-Physical Security of Smart Grids

Ghada Elbez, Hubert B. Keller and Veit Hagenmeyer (Karlsruhe Institute of Technology, Germany)

SAW 2018

SAW I - Software Security Testing and Cyber-Resilience

A64: Mission-Centric Automated Cyber Red Teaming

Suneel Randhawa (Defence Science and Technology, Department of Defence, Australia), Benjamin Turnbull (The University of New South Wales, Australia), Joseph Yuen (The University of New South Wales, Australia) and Jonathan Dean (Defence Science and Technology, Department of Defence, Australia)

A65: Ransomware's early mitigation mechanisms

Ruta Mussaileb (IMT-Atlantique, France), Nora Cuppens (IMT-Atlantique, France), Jean Louis Lanet (INRIA, France), Helene Bouder (IMT-Atlantique, France), Benjamin Bouget (DGA, France) and Aurelien Palisse (INRIA, France)

A66: A GDPR compliance module for supporting the exchange of information between CERTs

Otto Hellwig (SBA-Research, Austria), Gerald Quirchmayr (University of Vienna, Austria), Walter Hötzendorfer (Research Institute AG & Co KG, Austria), Christof Tschohl (Research Institute AG & Co KG, Austria), Edith Huber (Danube University Krems, Austria), Franz Vock (Federal Chancellery, Austria), Florian Nentwich (IKARUS Security Software, Austria), Bettina Pospisil (Danube University Krems, Austria), Matthias Gusenbauer (SBA-Research, Austria) and Gregor Langner (University of Vienna, Austria)

SAW II - Secure Software Development

A67: CryptSDLC: Embedding Cryptographic Engineering into Secure Software Development Lifecycle

Thomas Lorünser (AIT Austrian Institute of Technology, Austria), Thomas Länger (University of Lausanne, Austria), Henrich C. Pöhls (University of Passau, Germany) and Leon Sell (University of Passau, Germany)

A68: Architectural Solutions to Mitigate Security Vulnerabilities in Software Systems

Priya Anand and Jungwoo Ryoo (The Pennsylvania State University, United States)

SSE 2018

SSE I - Secure software development and DevOps

A69: Surveying Secure Software Development Practices in Finland

Kalle Rindell (University of Turku, Finland), Jukka Ruohonen (University of Turku, Finland) and Sami Hyrynsalmi (Tampere University of Technology, Finland)

A70: Challenges and Mitigation Approaches for Getting Secured Applications in a Big Company

Pawel Rajba (University of Wroclaw, Poland)

A71: Software Security Activities that Support Incident Management in Secure DevOps

Martin Gilje Jaatun (SINTEF Digital, Norway)

CUING 2018

CUING I

A72: Channel Steganalysis

Martin Steinebach (Fraunhofer, Germany)

A73: Towards Deriving Insights into Data Hiding Methods Using Pattern-based Approach

Wojciech Mazurczyk (Warsaw University of Technology, Poland), Steffen Wendzel (Worms University of Applied Sciences and Fraunhofer FKIE, Germany) and Krzysztof Cabaj (Warsaw University of Technology, Poland)

A74: Steganography by synthesis - Can commonplace image manipulations like face morphing create plausible steganographic channels?

Christian Kraetzer and Jana Dittmann (Dept. of Computer Science, Otto-von-Guericke University Magdeburg, Germany)

CUING II

A75:Towards Distributed Network Covert Channels Detection Using Data Mining-based Approach
Krzysztof Cabaj, Wojciech Mazurczyk, Piotr Nowakowski and Piotr Żórawski (Warsaw University of Technology, Poland)

A76: Get Me Cited, Scotty! Analysis of Academic Publications in Covert Channel Research
Steffen Wendzel (Fraunhofer FKIE / Worms University of Applied Sciences, Germany)

CUING III

A77: Towards Utilization of Covert Channels as a Green Networking Technique
Daniel Geisler (FernUniversitaet in Hagen, Germany), Wojciech Mazurczyk (Warsaw University of Technology, Poland) and Joerg Keller (FernUniversitaet in Hagen, Germany)

A78: Enhanced Electromagnetic Side-channel Eavesdropping Attacks on Computer Monitors
Asanka Sayakkara, Nhien An Le Khac and Mark Scanlon (University College Dublin, Ireland)

IoT-SECFOR 2018

IoT-SECFOR I– Security Assessment & Analysis

A79: Security Threats and Possible Countermeasures in Applications Covering Different Industry Domains
Musa Samaila, João Sequeiros, Mário Freire and Pedro Inácio (Instituto de Telecomunicações and Department of Computer Science, Universidade da Beira Interior, Covilhã, Portugal)

IoT-SECFOR II – Security Attacks & Solutions

A80: Denial-of-Service Attacks on LoRaWAN
Eef van Es, Harald Vranken and Arjen Hommersom (Open University of the Netherlands, Netherlands)

A81: Towards In-Network Security for Smart Homes
Martin Serror (RWTH Aachen University, Germany), Martin Henze (RWTH Aachen University, Germany), Sacha Hack (FH Aachen University of Applied Sciences, Germany), Marko Schuba (FH Aachen University of Applied Sciences, Germany) and Klaus Wehrle (RWTH Aachen University, Germany)

A82: On Track of Sigfox Confidentiality with End-to-End Encryption
Radek Fujdiak (Brno University of Technology, Czech Republic), Petr Petr (Brno University of Technology, Czech Republic), Konstantin Mikhaylov (University of Oulu, Finland), Lukas Malina (Brno University of Technology, Czech Republic), Petr Mlynek (Brno University of Technology, Czech Republic), Jiri Misurec (Brno University of Technology, Czech Republic) and Vojtech Blazek (Brno University of Technology, Czech Republic)

A83: Improved RNS-Based PRNGs
Alan Michaels (Virginia Tech, United States)

IoT-SECFOR III– Security Assessment & Analysis

A84: Correlation Power Analysis on the PRESENT Block Cipher on an Embedded Device
Owen Lo (Edinburgh Napier University, United Kingdom), Bill Buchanan (Edinburgh Napier University, United Kingdom) and Douglas Carson (Keysight Technologies, United Kingdom)

A85: Adding Salt to Pepper: A Structured Security Assessment over a Humanoid Robot
Alberto Giaretta (Örebro Universitet, Sweden), Michele De Donno (Technical University of Denmark, Denmark) and Nicola Dragoni (Technical University of Denmark, Denmark)

A86: Towards Wireless Secret key Agreement with LoRa Physical Layer

Henri Ruotsalainen (St. Pölten University of Applied Sciences, Austria) and Stepan Grebeniuk (VACE Systemtechnik GmbH, Austria)

iPAT 2018

iPAT I

A87: The user-centered privacy-aware control system PRICON: An interdisciplinary evaluation

Jonas Walter (TU Darmstadt, Germany), Bettina Abendroth (TU Darmstadt, Germany), Thilo von Pape (Université de Franche-Comté, France), Christian Plappert (Fraunhofer, Germany), Daniel Zelle (Fraunhofer, Germany), Christoph Krauß (Fraunhofer, Germany), Gundula Gagzow (Unabhängiges Landeszentrum für Datenschutz, Germany) and Hendrik Decke (Volkswagen, Germany)

A88: User privacy attitudes regarding proximity sensing

Håkan Jonsson (Lund University, Sweden) and Carl Magnus Olsson (Malmö University, Sweden)

A89: Critical Analysis of LPL according to Articles 12 - 14 of the GDPR

Armin Gerl and Dirk Pohl (Universität Passau, Germany)

A90: Privacy and DRM Requirements for Collaborative Development of AI Applications

Vida Ahmadi Mehri, Dragos Ilie and Kurt Tutschku (Blekinge Institute of Technology, Sweden)

IWSECC 2018

IWSECC I – Security Implementations for Cloud Computing

A91: A Process Framework for Stakeholder-specific Visualization of Security Metrics

Tanja Hanauer (Leibniz-Rechenzentrum der BAdW, Germany), Wolfgang Hommel (Universität der Bundeswehr München, Germany), Stefan Metzger (Leibniz-Rechenzentrum der BAdW, Germany) and Daniela Pöhn (Fraunhofer-Institut für Angewandte und Integrierte Sicherheit, Germany)

A92: Security Wrapper Orchestration in Cloud

Aapo Kalliola (Nokia Bell Labs, Finland), Shankar Lal (Aalto University,Finland), Kimmo Ahola (VTT Technical Research Centre of Finland, Finland), Ian Oliver (Nokia Bell Labs, Finland), Yoan Miche (Nokia Bell Labs, Finland) and Tuomas Aura (Aalto University, Finland)

A93: A Simulation Tool for Cascading Effects in Interdependent Critical Infrastructures

Stefan Rass, Thomas Grafenauer (Universitaet Klagenfurt, Austria), Sandra König and Stefan Schauer (Austrian Institute of Technology, Austria)

IWSECC II – Security Engineering Solutions for Cloud Computing

A94: A reference architecture for the container ecosystem

Madiha Syed and Eduardo B. Fernandez (Florida Atlantic University, United States)

A95: Evolution Oriented Monitoring oriented to Security Properties for Cloud Applications

Jamal Toutouh (University of Malaga, Spain), Antonio Muñoz (University of Malaga, Spain) and Sergio Nesmachnow (Universidad de la Républica – Engineering Faculty, Uruguay)

SPEBD 2018

SPEBD I

A96: Secure Fixed-point Division for Homomorphically Encrypted Operands

Chibuike Ugwuoke, Zekeriya Erkin and Reginald Lagendijk (Delft University of Technology, Netherlands)

A97: Attribute Based Content Security and Caching in Information Centric IoT

Nurefsan Sertbas (Bogazici University, Turkey), Samet Aytac (Bogazici University, Turkey), Orhan Ermis (Bogazici University, Turkey), Gurkan Gur (ZHAW Zurich University of Applied Sciences, Switherlands) and Fatih Alagoz (Bogazici University, Turkey)

A98: Evidence Identification in Heterogenous Data Using Clustering

Hussam Mohammed, Nathan Clarke and Fudong Li (University of Plymouth, United Kingdom)

WCTI 2018

WCTI I

A99: CRUSOE: Data Model for Cyber Situation Awareness

Jana Komárková, Martin Husák, Martin Laštovička and Daniel Tovarňák (Masaryk University, Czech Republic).

A100: Integrating Threat Intelligence to Enhance an Organization's Information Security Management

Mathias Gschwandtner (Leopold-Franzens University Innsbruck, Austria), Lukas Demetz (University of Applied Sciences Kufstein, Austria), Matthias Gander (Leopold-Franzens University Innsbruck, Austria) and Ronald Maier (Department of Information Systems, Production and Logistics Management, Austria)

A101: MAL (the Meta Attack Language): A Language for Domain-Specific Probabilistic Threat Modeling and Attack Simulation

Pontus Johnson, Robert Lagerström and Mathias Ekstedt (KTH Royal Institute of Technology, Sweden)

SECPID 2018

SECPID I

A102: Fingerprint Recognition on Mobile Devices: Widely Deployed, Rarely Understood.

Farzaneh Karegar, John Sören Pettersson and Simone Fischer-Hübner (Karlstad University, Sweden)

A103: Keys in the Clouds: Auditable Multi-device Access to Cryptographic Credentials.

Arseny Kurnikov (Aalto University, Finland), Andrew Paverd (Aalto University, Finland), Mohammad Mannan (Concordia University, Canada) and N. Asokan (Aalto University, Finland)

A104: Definitions for Plaintext-Existence Hiding in Cloud Storage.

Colin Boyd (Norwegian University of Science and Technology, Norway), Gareth T. Davies (Norwegian University of Science and Technology, Norway), Kristian Gjøsteen (Norwegian University of Science and Technology, Norway), Håvard Raddum (Simula Research Laboratories, Norway) and Mohsen Toorani (University of Bergen, Norway)

A105: Fully-Featured Anonymous Credentials with Reputation System.

Kai Bemmann, Jan Bobolz, Henrik Bröcher, Denis Diemert, Fabian Eidens, Lukas Eilers, Jan Haltermann, Jakob Juhnke, Burhan Otour, Laurens Porzenheim, Simon Pukrop, Erik Schilling, Michael Schlichtig and Marcel Stienemeier (Paderborn University, Germany)

5G-NS 2018

5G-NS I

A106: To Trust or Not to Trust: Data Origin Authentication for Group Communication in 5G Networks

Robert Annessi, Joachim Fabini and Tanja Zseby (Vienna University of Technology, Austria)

A107: Universal Trusted Execution Environments for Securing SDN/NFV Operations

Vincent Lefebvre (tages sas, France), Gianni Santinelli (tages sas, Italy), Tilo MÜller (FAU Erlangen-Nürnberg, Germany) and Johannes Götzfried (FAU Erlangen-Nürnberg, Germany)

A108: Enhancing NFV Orchestration with Security Policies

Christian Banse and Florian Wendland (Fraunhofer, Germany)

A109: Identity and Access Control for micro-services based 5G NFV platforms

Daniel Guija and Muhammad Shuaib Siddiqui (i2CAT, Spain)

5G-NS II

A110: Towards a 5G Security Architecture: Articulating Software-Defined Security and Security as a Service

Gregory Blanc (Institut Mines-Télécom, Télécom SudParis, France), Nizar Kheir (Thales Group, France), Dhouha Ayed (Thales Group, France), Vincent Lefebvre (Tages SAS, France), Edgardo Montes de Oca (Montimage, France) and Pascal Bisson (Thales Group, France)

A111: A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation

Marco Antonio Sotelo Monge, Jorge Maestre Vidal and Luis Javier García Villalba (Universidad Complutense de Madrid, Spain)

A112: SDN-based Mitigation of Scanning Attacks for the 5G Internet of Radio Light System

Krzysztof Cabaj, Marcin Gregorczyk, Wojciech Mazurczyk, Piotr Nowakowski and Piotr Żórawski (Warsaw University of Technology, Poland)

5G-NS III

A113: Detecting Workload-based and Instantiation-based Economic Denial of Sustainability on 5G environments

Jorge Maestre Vidal, Marco Antonio Sotelo Monge and Luis Javier García Villalba (Universidad Complutense de Madrid, Spain)

A114: Framework for Security Event Management in 5G

Iris Adam (Nokia Bell Labs, Germany) and Jing Ping (Nokia Software, China)

CyberTIM 2018

CyberTIM I - Attack Detection and Mitigation

A115: Evaluation of Apache Spot’s machine learning capabilities in an SDN/NFV enabled environment

Christos M. Mathas (University of Peloponnese, Greece), Olga E. Segou (Orion Innovations PC, Greece), Georgios Xylouris (Orion Innovations PC, Greece), Dimitris Christinakis (Orion Innovations PC, Greece), Michail – Alexandros Kourtis (Institute of Informatics and Telecommunications National Centre for Scientific Research “Demokritos”, Greece), Costas Vassilakis (University of Peloponnese, Greece) and Anastasios Kourtis (Institute of Informatics and Telecommunications National Centre for Scientific Research “Demokritos”, Greece)

A116: Towards an Automated Recognition System for Chat-based Social Engineering Attacks in Enterprise Environments

Nikolaos Tsinganos, George Sakellariou, Panagiotis Fouliras and Ioannis Mavridis (University of Macedonia, Greece)

A117: Augmented DDoS Mitigation with Reputation Scores

Tomáš Jánský (Faculty of Information Technology, CTU in Prague, Czech Republic), Tomáš Čejka (Faculty of Information Technology, CTU in Prague, Czech Republic), Martin Žádník (CESNET a.l.e., Czech Republic) and Václav Bartoš (CESNET a.l.e., Czech Republic)

A118: The challenge of detecting sophisticated attacks: Insights from SOC Analysts

Olusola Akinrolabu, Ioannis Agrafiotis and Arnau Erola (University of Oxford, United Kingdom)

CyberTIM II - Threat Intelligence Sharing

A119: Mission-Centric Risk Assessment to Improve Cyber Situational Awareness
Franklin Silva and Paul Jacob (Athlone IT, Ireland)

A120: The Mouseworld, a security traffic analysis lab based on NFV/SDN
Antonio Pastor (Telefonica I+D, Spain), Alberto Mozo Velasco (Universidad Politécnica de Madrid, Spain), Diego R. Lopez (Telefonica I+D, Spain), Jesús Luis Folgueira (Telefonica I+D, Spain) and Georgios Gardikis (Space Hellas S.A., Greece)

A121: Risks of Sharing Cyber Incident Information
Adham Albakri (University of Kent, United Kingdom), Eerke Boiten (De Montfort University, United Kingdom) and Rogério de Lemos (University of Kent, United Kingdom)

A122: Hunting Observable Objects for Indication of Compromise
Arnold Sykosch, Michael Meier and Marc Ohm (University of Bonn, Germany)

IWOCCTN 2018

IWOCCTN I – Cyber Organized Crime and Terrorism

A123: Conceptualizing the digital TAKEDOWN platforms for supporting first-line-practitioners and law enforcement agencies
Florian Huber (SYNYO GmbH, Austria)

A124: Cybercrime and Organized Crime
Václav Jirovský and Andrej Pastorek (Czech Technical University, Czech Republic)

A125: The AWID and TAKEDOWN prevention approach. The generation of a holistic good practice model for prevention of radicalization in youth work
Karin Rainer, Mario Springnagel and Diana Silvestru (Agency for European Integration and Economic Development, Austria)

IWOCCTN II – Cyber Security

A126: Challenges of Cryptocurrencies Forensics – A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals
Syed Naqvi (Birmingham City University, United Kingdom)

A127: Enhancing Cyber-Security by Safeguarding Information Privacy: the European Union and the Implementation of the “Data Protection by Design” Approach
Matteo E. Bonfanti (ETH Center for Security Studies, Switzerland)

A128: A review of network vulnerabilities scanning tools: types, capabilities and functioning
Andrea Tundis (TU Darmstadt, Germany), Wojciech Mazurczyk (Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications, Poland) and Max Mühlhäuser (TU Darmstadt, Germany)