ARES Conference
International Conference on Availability, Reliability and Security

ARES 2019

14th International Conference on Availability, Reliability and Security

August 26 – August 29, 2019
Canterbury, UK

ARES Conference 2019
14th International Conference on Availability, Reliability and Security
August 26-29, 2019
University of Kent, Canterbury, UK

Organized by

SBA Research

University of Kent

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

ACM ISBN: 978-1-4503-7164-3

The 14th International Conference on Availability, Reliability and Security (ARES 2019)

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

It is our great pleasure to welcome you to the Fourteenth International Conference on Availability, Reliability and Security (ARES 2019).

The Fourteenth International Conference on Availability, Reliability and Security (ARES 2019) brings again together researchers and practitioners in the field of dependability and cybersecurity. ARES 2019 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. This year we are again very happy to welcome famous keynote speakers from academia and industry Alastair MacWillson, Chair of Institute of Information Security and Chair of Qufaro@Bletchley Park and Awais Rashid, Professor of Cyber Security, University of Bristol.

2019, ARES has again received a high number of submissions. From the many submissions, we have selected the 21 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 20.75%. 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 2019 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.

We would like to thank the University of Kent for hosting ARES 2019!

Enjoy ARES 2019 and Canterbury!

Steven Furnell
University of Plymouth, UK

Vasilis Katos
Bournemouth University, UK

Shujun Li
University of Kent, UK

Gareth Howells
University of Kent, UK

Julio Hernandez-Castro
University of Kent, UK

Committee ARES 2019

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

General Chair 2019
Shujun Li, *University of Kent, UK*

General Co-Chairs 2019
Gareth Howells, *University of Kent, UK*
Julio Hernandez-Castro, *University of Kent, UK*

Program Committee Chairs 2019
Steven Furnell, *University of Plymouth, UK*
Vasilis Katos, *Bournemouth University, UK*

Local Arrangement Chair 2019
Budi Arief, *University of Kent, UK*

Workshop Chair 2019
Edgar Weippl, *SBA Research, Austria*

Program Committee 2019

- Isaac Agudo Ruiz, University of Malaga, Spain
- Esma Aimeur, University of Montreal, Canada
- Todd R. Andel, University of South Alabama, United States
- Abdelmalek Benzekri, University of Toulouse, France
- Francesco Buccafurri, University of Reggio Calabria, Italy
- Lasaro Camargos, Federal University of Uberlândia, Brazil
- Jordi Castellà Roca, Universitat Rovira i Virgili, Spain
- David Chadwick, University of Kent, United Kingdom
- Nathan Clarke, University of Plymouth, United Kingdom
- Marijke Coetzee, University of Johannesburg, South Africa
- Nora Cuppens-Boulahia, Université européene 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, United States
- 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
- Mathias Fischer, University of Hamburg, Germany
- Steven Furnell, University of Plymouth, United Kingdom

- Joaquin Garcia-Alfaro, Télécom SudParis, France
- Karl Goeschka, Vienna University of Technology, Austria
- Golden G Richard III, Louisiana State University
- 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, Continental AG, Germany
- Dominik Herrmann, University Bamberg, Germany
- Martin Gilje Jaatun, University of Stavanger, 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, St. Pölten University of Applied Sciences, Austria
- Ezzat Kirmani, St. Cloud State University, US
- Oksana Kulyk, ITU Copenhagen, Denmark
- Romain Laborde, University of Toulouse, France
- Costas Lambrinoudakis, University of Piraeus, Greece
- Brian Lee, Athlone Institute of Technology, Ireland
- Shujun Li, University of Kent, United Kingdom
- 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 and Bedford New College, 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, University of Molise, Italy
- Mattia Monga, Universita` degli Studi di Milano, Italy
- Haralambos Mouratidis, University of Brighton, United Kingdom
- Thomas Nowey, Syskron Security, Germany
- Christoforos Ntantogian, University of Piraeus, Greece
- Jaehong Park, University of Alabama in Huntsville, United States
- 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, Deutsche Bank, Germany

- Max Schuchard, University of Minnesota, United States
- Stefan Schulte, Vienna University of Technology, Austria
- Daniele Sgandurra, Royal Holloway, University of London, United Kingdom
- Jon A. Solworth, University of Illinois at Chicago, United States
- Jordi Soria-Comas, Universitat Rovira i Virgili, Spain
- Mark Strembeck, WU Vienna, Austria
- Jakub Szefer, Yale University, United States
- 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, Aalborg University, Denmark
- Umberto Villano, Universita' del Sannio, Italy
- Corrado Aaron Visaggio, Univeristà del Sannio, Italy
- Xiao Wang, Carnegie Mellon University, United States
- Christos Xenakis, University of Piraeus, Greece
- Zonghua Zhang, IMT Lille Douai, Institue Mines-Télécom, France
- Nicola Zannone, Eindhoven University of Technology, Netherlands
- Antonella Santone, University of Molise, Italy
- Andrea Di Sorbo, University of Sannio, Italy
- Giorgio Giacinto, University of Cagliari, Italy

ARES 2019 Program: Full Papers

ARES Full I - Dependability and resilience

Using Context and Provenance to defend against USB-borne attacks
Tobias Mueller (University of Hamburg, Germany), Ephraim Zimmer (University of Hamburg, Germany) and Ludovico De Nittis (GNOME, Italy)

Plug-and-Patch: Secure Value Added Services for Electric Vehicle Charging
Lucas Buschlinger (Fraunhofer, Germany), Markus Springer (Fraunhofer, Germany) and Maria Zhdanova (Fraunhofer, Germany)

Efficient attack countermeasure selection accounting for recovery and action costs
Jukka Soikkeli (Imperial College London, United Kingdom), Luis Muñoz-González (Imperial College London, United Kingdom) and Emil Lupu (Imperial College London, United Kingdom)

ARES Full II - Best Paper Session

Thieves in the Browser: Web-based Cryptojacking in the Wild
Marius Musch (TU Braunschweig, Germany), Christian Wressnegger (TU Braunschweig, Germany), Martin Johns (TU Braunschweig, Germany) and Konrad Rieck (TU Braunschweig, Germany)

Behavior-Aware Network Segmentation using IP Flows
Juraj Smeriga (Institute of Computer Science, Masaryk University, Czechia) and Tomas Jirsik (Institute of Computer Science, Masaryk University, Czechia)

Data-driven Curation, Learning and Analysis for Inferring Evolving IoT Botnets in the Wild

Morteza Safaei Pour (Cyber Threat Intelligence Lab, Florida Atlantic University, United States), Antonio Mangino (Cyber Threat Intelligence Lab, Florida Atlantic University, United States), Kurt Friday (Cyber Threat Intelligence Lab, Florida Atlantic University, United States), Matthias Rathbun (Cyber Threat Intelligence Lab, Florida Atlantic University, United States), Elias Bou-Harb (Cyber Threat Intelligence Lab, Florida Atlantic University, United States), Farkhund Iqbal (Zayed University, United Arab Emirates), Khaled Shaban (Qatar University, Qatar) and Abdelkarim Erradi (Qatar University, Qatar)

ARES Full III - Software security

A First ISA-Level Characterization of EM Pulse Effects on Superscalar Microarchitectures — A Secure Software Perspective

Julien Proy (INVIA, France), Karine Heydemann (LIP6 – Sorbonne Université, France), Fabien Majéric (Gemalto/Université Jean-Monnet, France), Alexandre Berzati (INVIA, France) and Albert Cohen (Google, France)

Obfuscation-Resilient Code Recognition in Android Apps

Johannes Feichtner (Graz University of Technology, Austria) and Christof Rabensteiner (Graz University of Technology, Austria)

Costing Secure Software Development Study – A Systematic Mapping Study

Elaine Venson (University of Southern California, United States), Xiaomeng Guo (University of Southern California, United States), Zidi Yan (University of Southern California, United States) and Barry Boehm (University of Southern California, United States)

ARES Full IV - Cryptographic mechanisms and applications I

Practical Group-Signatures with Privacy-Friendly Openings

Stephan Krenn (AIT Austrian Institute of Technology GmbH, Austria), Kai Samelin (TÜV Rheinland i-sec GmbH, Germany) and Christoph Striecks (AIT Austria, Austria)

E2E Verifiable Borda Count Voting System without Tallying Authorities

Samiran Bag (The University of Warwick, United Kingdom), Muhammad Ajmal Azad (University of Derby, United Kingdom) and Feng Hao ((The University of Warwick, United Kingdom)

ARES Full V - Cryptographic mechanisms and applications II

SET-OT: A Secure Equality Testing Protocol Based on Oblivious Transfer

Ferhat Karakoç (Kuveyt Türk Participation Bank Research and Development Center, Turkey), Majid Nateghizad (Cyber Security Group, Department of Intelligent Systems, Delft University of Technology, Netherlands) and Zekeriya Erkin (Cyber Security Group, Department of Intelligent Systems, Delft University of Technology, Netherlands)

Anonymous Identity Based Encryption with Traceable Identities

Olivier Blazy (Université de Limoges, France), Laura Brouilhet (Université de Limoges, France) and Duong-Hieu Phan (Université de Limoges, France)

ARES Full VI - Network Security I

Towards Efficient Reconstruction of Attacker Lateral Movement

Florian Wilkens (University of Hamburg, Germany), Steffen Haas (University of Hamburg, Germany), Dominik Kaaser (University of Hamburg, Germany), Peter Kling (University of Hamburg, Germany) and Mathias Fischer (University of Hamburg, Germany)

Strong Tenant Separation in Cloud Computing Platforms

Michael Pfeiffer (Technische Universität Ilmenau, Germany), Michael Rossberg (Technische Universität Ilmenau, Germany), Simon Buttgereit (Technische Universität Ilmenau, Germany) and Guenter Schaefer (Technische Universität Ilmenau, Germany)

Blockchain Trilemma Solver Algorand has Dilemma over Undecidable Messages

Mauro Conti (University of Padua, Italy), Ankit Gangwal (University of Padova, Italy) and Michele Todero (University of Padova, Italy)

ARES Full VII – Web security and attacks

PoliDOM: Mitigation of DOM-XSS by Detection and Prevention of Unauthorized DOM Tampering

Junaid Iqbal (University of New Brunswick, Canada), Ratinder Kaur (University of Saskatchewan, Canada) and Natalia Stakhanova (University of Saskatchewan, Canada)

Towards a framework for detecting advanced Web bots

Christos Iliou (Information Technologies Institute, CERTH, Greece), Theodoros Kostoulas (Department of Computing and Informatics, Bournemouth University, United Kingdom), Theodora Tsikrika (Information Technologies Institute, CERTH, Greece), Vasilis Katos (Department of Computing and Informatics, Bournemouth University, United Kingdom), Stefanos Vrochidis (Information Technologies Institute, CERTH, Greece) and Yiannis Kompatsiaris (Information Technologies Institute, CERTH, Greece)

Characterizing the Redundancy of DarkWeb .onion Services

Pavlo Burda (Eindhoven University of Technology, Netherlands), Coen Boot (Radboud University, Netherlands)and Luca Allodi (Eindhoven University of Technology, Netherlands)

ARES Full VIII - Network Security I

Detecting DGA domains with recurrent neural networks and side information

Ryan Curtin (Symantec Corporation, United States), Andrew Gardner (Symantec Corporation, United States), Slawomir Grzonkowski (Symantec Corporation, Ireland), Alexey Kleymenov (Symantec Corporation, Ireland) and Alejandro Mosquera Lopez (Symantec Corporation, United States)

Black Box Attacks on Deep Anomaly Detectors

Aditya Kuppa (Symantec Corporation and School of Computer Science University College, Dublin, Ireland), Slawomir Grzonkowski (Symantec Corporation, Ireland), Muhammad Rizwan Asghar (School of Computer Science The University of Auckland, New Zealand) and Nhien An Le Khac (School of Computer Science University College, Dublin, Ireland)

ARES 2019 Program: Short Papers

ARES Short I - Identity, authorization and privacy

On the Exploitation of Online SMS Receiving Services to Forge ID Verification

Muhammad Hajian Berenjestanaki (University of Tehran, Iran), Mauro Conti (University of Padua, Italy) and Ankit Gangwal (University of Padova, Italy)

Does “www.” Mean Better Transport Layer Security?

Eman Alashwali (University of Oxford, United Kingdom), Pawel Szalachowski (Singapore University of Technology and Design (SUTD), Singapore) and Andrew Martin (University of Oxford, United Kingdom)

An Attribute-Based Privacy-Preserving Ethereum Solution for Service Delivery with Accountability Requirements

Francesco Buccafurri (DIIES – Universita’ Mediterranea di Reggio Calabria, Italy), Vincenzo De Angelis (DIIES – Universita’ Mediterranea di Reggio Calabria, Italy), Gianluca Lax (DIIES – Universita’ Mediterranea di Reggio Calabria, Italy), Lorenzo Musarella (DIIES – Universita’ Mediterranea di Reggio Calabria, Italy) and Antonia Russo (DIIES – Universita’ Mediterranea di Reggio Calabria, Italy)

ARES Short II - Threat detection and response

STAMAD – a STAtic MAlware Detector

Khanh Huu The Dam (Nha Trang University, Viet Nam) and Tayssir Touili (LIPN, CNRS & University Paris 13, France)

Enhancing credibility of digital evidence through provenance-based incident response handling

Ludwig Englbrecht (University of Regensburg, Germany), Gregor Langner (University of Vienna, Austria), Günther Pernul (University of Regensburg, Germany) and Gerald Quirchmayr (University of Vienna, Austria)

Language-based Integration of Digital Forensics & Incident Response

Christopher Stelly (University of New Orleans, United States) and Vassil Roussev (University of New Orleans, United States)

ARES Short III -

Post-Quantum UC-Secure Oblivious Transfer in the Standard Model with Adaptive Corruptions

Olivier Blazy (Université de Limoges, France), Céline Chevalier (ENS, France) and Quoc Huy Vu (DIENS, École normale supérieure, CNRS, INRIA, PSL University, Paris, France)

On the Utility of Synthetic Data: An Empirical Evaluation on Machine Learning

Markus Hittmeir (SBA Research, Austria), Andreas Ekelhart (SBA Research, Austria) and Rudolf Mayer (SBA Research, Austria)

Building Taxonomies based on Human-Machine Teaming: Cyber Security as an Example

Mohamad Imad Mahaini (The University of Kent, United Kingdom), Shujun Li (The University of Kent, United Kingdom) and Rahime Belen Sağlam (Ankara Yıldırım Beyazıt University, Turkey)

The Workshops of the 14th International Conference on Availability, Reliability and Security (ARES 2019)

Welcome Message from ARES Workshop Chair

Welcome to the Workshops of the Twelfth International Conference on Availability, Reliability and Security (ARES 2019).

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 15 workshops, which range from "start-ups" to well-established ones supporting ARES.

The succeeding listing comprises the workshops of ARES 2019:

- 14th International Workshop on Frontiers in Availability, Reliability and Security (FARES 2019)
- 12th International Workshop on Digital Forensics (WSDF 2019)
- 8th International Workshop on Security of Mobile Applications (IWSMA 2019)
- 8th International Workshop on Cyber Crime (IWCC 2019)
- 6th International Workshop on Agile Secure Software Development (SSE 2019)
- 3rd International Workshop on Criminal Use of Information Hiding (CUING 2019)
- 3rd International Workshop on Security and Forensics of IoT (IoT-SECFOR 2019)
- 2nd Interdisciplinary Workshop on Privacy and Trust (iPAT 2019)
- 2nd International Workshop on Security Engineering for Cloud Computing (IWSECC 2019)
- 2nd International Workshop on Cyber Threat Intelligence (WCTI 2019)
- 2nd International Workshop on Behavioral Authentication for System Security (BASS 2019)
- 2nd International Workshop on Cyber Threat Intelligence Management (CyberTIM 2019)
- 1st International Workshop on Information Security Methodology and Replication Studies (IWSMR 2019)
- 1st International Workshop on Location Privacy (LPW 2019)
- 1st International Workshop on Industrial Security and IoT (WISI 2019)

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 2019 Workshop Chair
SBA Research, Austria

The 14th International Workshop on Frontiers of Availability, Reliability and Security (FARES 2019)

Welcome Message from the FARES Workshop Organizers

The 14th International Workshop on Frontiers of Availability, Reliability and Security (FARES 2019) 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 7 best for presentation. These presentations have been grouped into two sessions. The first session deals with problems related to protection and detection. The second one collects papers focusing on measurement, standards and compliance.

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 2019

- 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*
- Roberto Nardone, *University of Reggio Calabria, Italy*
- Vishal Saraswat, *R.C.Bose Centre for Cryptology and Security Indian Statistical Institute, Kolkata, India*
- Aaron Visaggio, *Università del Sannio, Benevento, Italy*

FARES 2019 Program

FARES I - Protection and Detection

A Pattern for a Virtual Network Function (VNF)
Ahmed Alwakeel (Florida Atlantic University, United States), Abdulrahman Alnaim (Florida Atlantic University, United States) and Eduardo B. Fernandez (Florida Atlantic University, United States)

Near-optimal Evasion of Randomized Convex-inducing Classifiers in Adversarial Environments
Pooria Madani (York University, Canada) and Natalija Vlajic (York University, Canada)

AMON: an Automaton MONitor for Industrial Cyber-Physical Security
Giuseppe Bernieri (Department of Mathematics University of Padua, Italy), Mauro Conti (Department of Mathematics University of Padua, Italy) and Gabriele Pozzan (Department of Mathematics University of Padua, Italy)

Decision Support for Mission-Centric Cyber Defence
Michal Javorník (Masaryk University, Czechia), Jana Komárková (Masaryk University, Czechia) and Martin Husák (Masaryk University, Czechia)

FARES II - Measurement and Robust Design

Managing the over-estimation of resilience
Thomas Clédel (IMT Atlantique, France), Frédéric Cuppens (TELECOM Bretagne, France) and Nora Cuppens-Boulahia (IMT Atlantique, France)

GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform
Martin Horák (Masaryk University, Czechia), Václav Stupka (Masaryk University, Czechia) and Martin Husák (Masaryk University, Czechia)

Cyber Security Skill Set Analysis for Common Curricula Development
Muhammad Mudassar Yamin (Norwegian University of Science and Technology, Norway) and Basel Katt (Norwegian University of Science and Technology, Norway)

The 12th International Workshop on Digital Forensics (WSDF 2019)

Welcome Message from the WSDF Workshop Organizers

It is our great pleasure to welcome you to the 12th International Workshop on Digital Forensics (WSDF) which takes place in Canterbury (UK) from 26 to 29 August 2019.

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 aims to bring 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 50%.

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*
Kim-Kwang Raymond Choo, *University of Texas at San Antonio, US*

Workshop Program Committee WSDF 2019

- 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*
- Jeroen van der Bos, *Netherlands Forensic Institute, Netherlands*
- Joshua James, *Soon Chun Hyang University, South Korea*
- Kam-Pui Chow, *Hong Kong University, Hong Kong*
- Mark Scalon, *University College Dublin, Ireland*
- Olga Angelopoulou, *University of Hertfordshire, UK*
- Simon Tjoa, *St. Pölten University of Applied Sciences, Austria*
- Sandra Avila, *University of Campinas, Brasil*
- Stefano Zanero, *Politecnico di Milano, Italia*
- Vassil Roussev, *University of New Orleans, USA*
- Christopher Hargreaves, *University of Oxford, UK*
- Graeme Horsman, *Teesside University, UK*
- Jai Vasanth, *Google, USA*
- Muhammad Nadeem, *University of Derby, UK*
- Oren Halvani, *Fraunhofer Institute, Germany*

WSDF 2019 Program

WSDF I

Assessing the Applicability of Authorship Verification Methods
Oren Halvani (The Fraunhofer Institute for Secure Information Technology SIT, Germany), Christian Winter (The Fraunhofer Institute for Secure Information Technology SIT, Germany) and Lukas Graner (The Fraunhofer Institute for Secure Information Technology SIT, Germany)

Improved Manipulation Detection with Convolutional Neural Network for JPEG Images
Huajian Liu (Fraunhofer, Germany), Martin Steinebach (Fraunhofer, Germany) and Kathrin Schölei (Fraunhofer, Germany)

Deep Learning-based Facial Detection and Recognition in Still Images for Digital Forensics
Patricio Domingues (ESTG – Leiria, Portugal) and Alexandre Frazão Rosário (IT, Portugal)

WSDF II

Revisiting Data Hiding Techniques for Apple File System
Thomas Göbel (University of Applied Sciences Darmstadt, Germany), Jan Türr (University of Applied Sciences Darmstadt, Germany) and Harald Baier (University of Applied Sciences Darmstadt, Germany)

Map My Murder! A Digital Forensic Study of Mobile Health and Fitness Applications
Courtney Hassenfeldt (University of New Haven, United States), Shabana Baig (University of New Haven, United States), Ibrahim Baggili (University of New Haven, United States) and Xiaolu Zhang (University of Texas at San Antonio, United States)

Methodology for the Automated Metadata-Based Classification of Incriminating Digital Forensic Artefacts
Xiaoyu Du (University College Dublin, Ireland) and Mark Scanlon (University College Dublin, Ireland)

WSDF III

A Study of Network Forensic Investigation in Docker Environments
Daniel Spiekermann (FernUniversität in Hagen, Germany), Tobias Eggendorfer (HS Weingarten, Germany) and Jörg Keller (FernUniversität in Hagen, Germany)

IO-Trust: An out-of-band trusted memory acquisition for intrusion detection and Forensics investigations in cloud IOMMU based systems
Ahmad Atamli (Alan Turing Institute, University of Cambridge, United Kingdom) and Jon Crowcroft (Alan Turing Institute, University of Cambridge, United Kingdom)

IoT Ignorance is Digital Forensics Research Bliss: A Survey to Understand IoT Forensics Definitions, Challenges and Future Research Directions

Tina Wu (University of Oxford, United Kingdom), Frank Breitinger (University of New Haven, United States) and Ibrahim Baggili (University of New Haven, United States)

The 8th International Workshop on Security of Mobile Applications (IWSMA 2019)

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, *UAS St. Pölten, Austria*
Sebastian Schrittwieser, *Josef Ressel Center for Unified Threat Intelligence on Targeted Attacks, UAS St. Pölten, Austria*

Workshop Program Committee IWSMA 2019

- 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*
- Mayank Sinha, *Shell, The Netherlands*
- Ronald Tögl, *Infineon Technologies, Austria*
- Johanna Ullrich, *SBA Research, Austria*

IWSMA 2019 Program

IWSMA I

Analyzing Android's File-Based Encryption: Information Leakage through Unencrypted Metadata
Tobias Groß (Friedrich-Alexander University, Germany), Matanat Ahmadova (University of Bonn, Germany) and Tilo Müller (Friedrich-Alexander University, Germany)

Post-Quantum Cryptography in Embedded Systems
Soundes Marzougui (TU Darmstadt, Germany) and Juliane Krämer (TU Darmstadt, Germany)

The Internet Banking [in]Security Spiral: Past, Present, and Future of Online Banking Protection Mechanisms based on a Brazilian case study

Marcus Botacin (Federal University of Brazil, Brazil), Anatoli Kalysch (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany), Tilo Mueller (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany) and Andre Gregio (UFPR, Brazil)

The 8th International Workshop on Cyber Crime (IWCC 2019)

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 2019

- Michal Choras, *ITTI Ltd., Poland*
- 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*
- Nabil Schear, *MIT Lincoln Laboratory, USA*
- Bela Genge, *University of Medicine, Pharmacy, Sciences and Technology of Targu Mures, Romania*
- Igor Kotenko, *Russian Academy of Sciences (SPIIRAS), Russia*
- 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*
- Eric Chan-Tin, *Oklahoma State University, USA*
- Luca Caviglione, *ISSIA, CNR, Italy*
- Hui Tian, *National Huaqiao University, China*
- Elias Bou-Harb, *National Cyber Forensics and Traning Alliance & Florida Atlantic University, USA*
- Samia Bouzefrane, *CEDRIC Lab Conservatoire National des Arts et Métiers, France*
- Roberto Di Pietro, *Hamad Bin Khalifa University, Doha-Qatar*

IWCC 2019 Program

IWCC I

An Analysis Framework for Product Prices and Supplies in Darknet Marketplaces
York Yannikos (Fraunhofer, Germany), Julian Heeger (Fraunhofer, Germany) and Maria Brockmeyer (TU Darmstadt, Germany)

Limits in the data for detecting crimincals on social media
Andrea Tundis (TU Darmstadt, Germany), Leon Böck (Technische Universität Darmstadt (TUDA), Germany), Victoria Stanilescu (Siemens AG, Germany) and Max Mühlhäuser (TU Darmstadt, Germany)

IWCC II

Ontology of Metrics for Cyber Security Assessment
Elena Doynikova (St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Russia), Andrey Fedorchenko (St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Russia) and Igor Kotenko (St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Russia)

Large-Scale Analysis of Pop-Up Scam on Typosquatting URLs
Tobias Dam (FHSTP UAS, Austria), Lukas Daniel Klausner (FHSTP UAS, Austria), Damjan Buhov (Josef Ressel Center TARGET, Austria) and Sebastian Schrittwieser (SBA Research, Austria)

Realistically Fingerprinting Social Media Webpages in HTTPS Traffic
Mariano Di Martino (Hasselt University / Expertise Center For Digital Media, Belgium), Peter Quax (Hasselt University / Expertise Center For Digital Media, Belgium) and Wim Lamotte (Hasselt University / Expertise Center For Digital Media, Belgium)

IWCC III

Fake News Detection by Image Montage Recognition
Martin Steinebach (Fraunhofer, Germany), Huajian Liu (Fraunhofer, Germany) and Karol Gotkowski (Fraunhofer, Germany)

HEHLKAPPE: Utilizing Deep Learning to Manipulate Surveillance Camera Footage in Real-Tim
Alexander Aigner (University of Applied Sciences Upper Austria, Austria) and Rene Zeller (University of Applied Sciences Upper Austria, Austria)

Improving Borderline Adulthood Facial Age Estimation through Ensemble Learning
Felix Anda (University College Dublin, Ireland), David Lillis (University College Dublin, Ireland), Aikaterini Kanta (University College Dublin, Ireland), Brett Becker (University College Dublin, Ireland), Elias Bou-Harb (Cyber Threat Intelligence Lab, Florida Atlantic University, United States), Nhien An Le Khac (University College Dublin, Ireland) and Mark Scanlon (University College Dublin, Ireland)

The 5th International Workshop on Secure Software Engineering (SSE 2019)

Welcome Message from the SSE Workshop Organizers

It is our pleasure to welcome you to the Fourth International Workshop on Secure Software Engineering (SSE 2019), organized in conjunction with the International Conference on Availability, Reliability and Security (ARES 2019) in University of Kent, Canterbury, UK.

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 5 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 2019 Program

SSE I - Secure Software Development

Learning Software Security in Context: An Evaluation in Open Source Software Development Environment

Shao-Fang Wen (Norwegian University of Science and Technology, Norway) and Basel Katt (Norwegian University of Science and Technology, Norway)

The Security Intention Meeting Series as a way to increase visibility of software security decisions in agile development projects

Inger Anne Tøndel (Norwegian University of Science and Technology, Norway), Daniela S. Cruzes (SINTEF Digital, Norway), Martin Gilje Jaatun (SINTEF Digital, Norway) and Kalle Rindell (SINTEF Digital, Norway)

SSE II - Managing security on applications

Managing Security in Software Or: How I Learned to Stop Worrying and Manage the Security Technical Debt

Kalle Rindell (SINTEF Digital, Norway), Martin Gilje Jaatun (SINTEF Digital, Norway) and Karin Bernsmed (SINTEF Digital, Norway)

Applying Security Testing Techniques to Automotive Engineering

Irdin Pekaric (University of Innsbruck, Austria), Clemens Sauerwein (University of Innsbruck, Austria) and Michael Felderer (University of Innsbruck, Austria)

Model Driven Security in a Mobile Banking Application Context

Serafettin Senturk (Gebze Technical University, Turkey), Hasan Yasar (Software Engineering Institute, Carnegie Mellon University, United States) and Ibrahim Sogukpinar (Gebze Technical University, Turkey)

The 3rd International Workshop on Criminal Use of Information Hiding (CUING 2019)

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 more and more 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. This poses a lot of new challenges for digital forensics analysts, academics, law enforcement agencies (LEAs), and security professionals.

The aim of the Third 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. However data hiding is understood here in a wider manner than in the academic world i.e. all techniques that pertain to camouflaging/masking/hiding various types of data (e.g. identities, behavior, communication, etc.) are included here. This means not only digital steganography/covert channels but also obfuscation/anti-forensics techniques and even underground networks (darknets) or activities related to behavior impersonation or mimicking. This will allow to present a more complete picture on novel research regarding the use of data and communication hiding methods in criminal environments and discuss ideas for fighting misuse of privacy enhancing technologies.

Moreover, this year the CUING workshop is co-organized with the SIMARGL (Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware) H2020 project.

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 2019

- Ahmed A. Abd El-Latif, *Menoufia University, Egypt*
- Soumya Banerjee, *CNAM-CEDRIC LAB, INRIA-EVA, Paris, France*
- Krzysztof Cabaj, *Warsaw University of Technology, Poland*
- Luca Caviglione, *IMATI CNR, Italy*
- Marco Cremonini, *University of Milan, Italy*
- Jana Dittmann, *Otto-von-Guericke University Magdeburg, Germany*
- Mattia Epifani, *CNR, Italy*
- Zeno Geradts, *NFI, The Netherlands*
- Julio Hernandez-Castro, *School of Computing, University of Kent, UK*
- Felix Iglesias, *Vienna University of Technology, Austria*
- Stefan Katzenbeisser, *TU Darmstadt, Germany*
- Zbigniew Kotulski, *Warsaw University of Technology, Poland*
- Christian Kraetzer, *Otto-von-Guericke University Magdeburg, Germany*
- Jean-Francois Lalande, *CentraleSupélec, France*
- Daniel Lerch-Hostalot, *Universitat Oberta de Catalunya, Spain*
- Shujun Li, *University of Kent, UK*
- David Megias, *Universitat Oberta de Catalunya, Spain*
- Aleksandra Mileva, *University Goce Delcev, Republic of Macedonia*
- Avinash Srinivasan, *Temple University, USA*
- Hui Tian, *National Huaqiao University, China*
- Edgar Weippl, *SBA Research, Austria*
- Steffen Wendzel, *Worms University of Applied Sciences and Fraunhofer FKIE, Germany*
- Tanja Zseby, *Vienna University of Technology, Austria*

CUING 2019 Program

CUING I – Keynote Session

CUING II

Protocol-independent Detection of `Messaging Ordering' Network Covert Channels
Steffen Wendzel (Worms University of Applied Sciences and Fraunhofer FKIE, Germany)

Introducing Dead Drops to Network Steganography using ARP-Caches and SNMP-Walks
Tobias Schmidbauer (University of Hagen, Germany), Steffen Wendzel (Worms University of Applied Sciences and Fraunhofer FKIE, Germany), Aleksandra Mileva (University Goce Delcev, Macedonia) and Wojciech Mazurczyk (Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications, Poland)

Fine-tuning of Distributed Network Covert Channels Parameters and Their Impact on Undetectability
Krzysztof Cabaj (Warsaw University of Technology, Poland), Wojciech Mazurczyk (Warsaw University of Technology, Poland), Piotr Nowakowski (Warsaw University of Technology, Poland) and Piotr Żórawski (Warsaw University of Technology, Poland)

CUING III

Detection and Analysis of Tor Onion Services
Martin Steinebach (Fraunhofer, Germany), Marcel Schäfer (Fraunhofer CESE, United States) and York Yannikos (Fraunhofer, Germany)

Productivity and Patterns of Activity in Bug Bounty Programs: Analysis of HackerOne and Google Vulnerability Research
Donatello Luna (Tribunale di Busto Arsizio, Italy), Luca Allodi (Eindhoven University of Technology, Netherlands) and Marco Cremonini (University of Milan, Italy)

SocialTruth Project Approach to Online Disinformation (Fake News) Detection and Mitigation
Michal Choras (UTP Bydgoszcz, Poland), Marek Pawlicki (Uniwersytet Technologiczno-Przyrodniczy, Poland) and Rafal Kozik (Institute of Telecommunications, UTP Bydgoszcz, Poland)

CUING IV

Towards Reversible Storage Network Covert Channels
Wojciech Mazurczyk (Warsaw University of Technology, Poland), Przemysław Szary (Warsaw University of Technology, Poland), Steffen Wendzel (Worms University of Applied Sciences and Fraunhofer FKIE, Germany) and Luca Caviglione (CNR – IMATI, Italy)

Privacy and Robust Hashes
Martin Steinebach (Fraunhofer, Germany), Sebastian Lutz (Fraunhofer, Germany) and Huajian Liu (Fraunhofer, Germany)

The 3rd 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 3rd International Workshop on Security and Forensics of IoT (IoT-SECFOR) which takes place in Canterbury (UK) from 26 to 29 August 2019.

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 Internet of Things (IoT). IoT systems 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.

The acceptance rate of this edition of the workshop was 45%.

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*
Asma Adnane, *Loughborough University, UK*
Xiaojun Zhai, *University of Essex, UK*

Publicity co-chairs

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

Workshop Program Committee IoT-SECFOR 2019

- Alberto Compagno, *Cisco Systems, France*
- Diogo Fernandes, *PepsiCo, Poland*
- Henrique Santos, *University of Minho, Portugal*
- Judith Rossebo, *ABB AS, Norway*
- Katinka Wolter, *Freie Universität Berlin, Germany*
- Miguel Pardal, *University of Lisbon, Portugal*
- Moreno Ambrosin, *Intel Labs, USA*
- Patrik Ekdahl, *Ericsson AB, Sweden*
- Ricardo Neisse, *European Commission Joint Research Centre, Italy*
- Simona Bernardi, *Universidad de Zaragoza, Spain*
- Chaker Abdelaziz Kerrache, Université Amar Telidji de Laghouat, Algeria
- João Vilela, University of Coimbra, Portugal
- Sampsa Rauti, University of Turku, Finland
- Savio Sciancalepore, Hamad bin Khalifa University, Qatar
- Seppo Virtanen, University of Turku, Finland
- Steffen Wendzel, Worms University of Applied Sciences, Germany
- Tomasz Szydlo, AGH University of Science and Technology, Poland

IoT-SECFOR 2019 Program

IoT-SECFOR I

Securing the Device Drivers of Your Embedded Systems: Framework and Prototype

Zhuohua Li (The Chinese University of Hong Kong, Hong Kong), Jincheng Wang (The Chinese University of Hong Kong, Hong Kong), Mingshen Sun (Baidu X-Lab, United States) and John C.S. Lui (The Chinese University of Hong Kong, Hong Kong)

IoT-HarPSecA: A Framework for Facilitating the Design and Development of Secure IoT Devices

Musa Samaila (Universidade da Beira Interior and Instituto de Telecomunicações, Covilhã, Portugal), Moser José (Universidade da Beira Interior and Instituto de Telecomunicações, Covilhã, Portugal), João Bernardo Sequeiros (Universidade da Beira Interior and Instituto de Telecomunicações, Covilhã, Portugal), Mario Freire (Universidade da Beira Interior and Instituto de Telecomunicações, Covilhã, Portugal) and Pedro Inácio (Universidade da Beira Interior and Instituto de Telecomunicações, Covilhã, Portugal)

IoT-SECFOR II

Privacy-Enhancing Fall Detection from Remote Sensor Data Using Multi-Party Computation

Pradip Mainali (OneSpan, Belgium) and Carlton Shepherd (OneSpan, United Kingdom)

Energy Attack in LoRaWAN: Experimental Validation

Konstantin Mikhaylov (University of Oulu, Finland), Radek Fujdiak (Brno University of Technology, Czechia), Miroslav Voznak (Technical University of Ostrava, Czechia), Ari Pouttu (University of Oulu, Finland) and Petr Mlynek (Brno University of Technology, Czechia)

A Secure Publish/Subscribe Protocol for Internet of Things

Lukas Malina (Brno University of Technology, Czechia), Gautam Srivastava (Brandon University, Canada), Petr Dzurenda (Brno University of Technology, Czechia) and Jan Hajny (Brno University of Technology, Czechia)

The 2nd Interdisciplinary Privacy and Trust workshop (iPAT 2019)

Welcome Message from the iPAT Workshop Organizers

We are pleased to welcome you to the second edition of the Interdisciplinary Privacy and Trust workshop (iPAT), co-located with ARES 2019 in Canterbury.

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.

After taking input from the community during the first iPAT workshop in Hamburg last year, this year's iPAT contributes back to the community with a well-selected round of invited talks. The motto for iPAT 2019 is "privacy and trust with publicly available data" and addresses not only technical solutions that leverage public & open data but also addresses economic and legal challenges and chances.

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 speakers for sharing their visions, as well as the program committee for their careful reviews. A special thank you goes to all authors for submitting their contributions.

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

Max Mühlhäuser, *TU Darmstadt, Germany*

Stephen Marsh, *Ontario Tech University, Canada*

Jörg Daubert, *Philipps-Universität Marburg, Germany*

Workshop Program Committee iPAT 2019

- Nina Gerber, *KIT, Germany*
- Tim Grube, *TU Darmstadt, Germany*
- Gareth T. Davies, *University of Paderborn, Germany*
- Mathias Humbert, *EPFL, Switzerland*
- Dominik Herrmann, *University of Bamberg, Germany*
- Christian Janson, *TU Darmstadt, Germany*
- Igor Bilogrevic, *Google, Switzerland*
- Oksana Kulyk, *IT University of Copenhagen, Denmark*
- Max Maass, *TU Darmstadt, Germany*
- Aidmar Wainakh, *TU Darmstadt, Germany*
- Kris Shrishak, *Fraunhofer SIT, Germany*

The 2nd International Workshop on Security Engineering for Cloud Computing (IWSECC 2019)

Welcome Message from the IWSECC Workshop Organizers

It is our great pleasure to welcome you to the 2nd International Workshop on Security Engineering for Cloud Computing (IWSECC 2019) will be held in conjunction with the 14th International Conference on Availability, Reliability and Security ARES in August 28, 2019, University of Kent, Canterbury, UK.

We are witnessing the importance of cloud computing and its role in current panorama, but cloud technology is exposed to security and privacy and many challenges to overcome. The application of software engineering to Cloud computing is a primary aspect to obtain a systematic approach to the development, operation and maintenance of software. There is no perfect security and when a cybersecurity incident occurs, digital investigation will require the identification, preservation and analysis of evidential data.

The main ambition of the workshop is to provide a venue and forum for researchers from security engineering and cloud computing to to explore techniques that enable security mechanisms to be engineered and implemented in Cloud systems.

The Workshop organizing committee

Antonio, Muñoz, *University of Málaga, Spain*
Eduardo B., Fernández, Florida Atlantic *University, USA*

Workshop Program Committee IWSECC 2019

- ASTUDILLO HERNÁN, *Universidad Técnica Federico Santa María, Chile*
- BOYD, COLIN, *Queensland U. of Tech., Australia*
- DAVIDS, CAROL, *Illinois Institute of Technology, USA*
- DUSIT NIYATO, *Nanyang Technological U., Singapore*
- GIORGINI, PAOLO, *University of Trento, Italy*
- GÜRGENS, SIGRID, *Fraunhofer SIT, Germany*
- HERZBERG, AMIR, *Ba-Ilan University, Israel*
- 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*
- 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*
- MORENO AMBROSIN, *Intel Labs, US*
- 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*
- RAUL H. C. LOPES, *Brunel University, JISC & CMS/CERN, UK*
- ROMAN, RODRIGO, University of Malaga, Spain
- SABETTA, ANTONINO, *SAP, France*
- SENG-PHIL, HONG, *Sungshin Women's University, Korea*
- SKIANIS CHARALABOS, *University of Aegean, Greece*
- SPANOUDAKIS, GEORGE, *City University, UK*
- VILLE LEPPÄNENE, *University of Turku, Finland*
- WASHIZAKI, HIRONORI, *Waseda University, Japan*
- WEISONG SHI, *Wayne State University, USA*
- WESPI, ANDREAS, *IBM, Switzerland*
- YOSHIOKA, NOBUKAZU, *Nat. I. of Informatics, Japan*
- ZHANG, TAO, *Cisco, USA*
- ZIMMERMAN, OLAF. *Informatik IFS, Germany*

IWSECC 2019 Program

IWSECC I

Leveraging Kernel Security Mechanisms to Improve Container Security: a Survey
Maxime Bélair (Orange Labs, France), Sylvie Laniepce (Orange Labs, France) and Jean-Marc Menaud (IMT Atlantique, INRIA, LS2N, France)

A Misuse Pattern for Compromising VMs via Virtual Machine Escape in NFV
Abdulrahman Alnaim (Florida Atlantic University, United States), Ahmed Alwakeel (Florida Atlantic University, United States) and Eduardo B. Fernandez (Florida Atlantic University, United States)

IWSECC II

Preserving context security in AWS IoT Core
Luca Calderoni (University of Bologna, Italy)

DTE Access Control Model for Integrated ICS Systems
Khaoula Es-Salhi (IMT atlantique -LabSTICC, France), David Espes (Université de Bretagne Occidentale (UBO), France) and Nora Cuppens (IMT atlantique -LabSTICC, France)

The 2nd International Workshop on Cyber Threat Intelligence (WCTI 2019)

Welcome Message from the WCTI Workshop Organizers

Effective cyber defense requires information about the adversaries, their objective and modus operandi when attempting a compromise: cyber threat intelligence. If we don't have this information available, 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.

Despite its essential importance to effective and efficient cyber security, cyber threat intelligence as a discipline is still in its infancy. 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.

After an overwhelmingly successful workshop in 2018, we are proud to organize the second round of this event and provide a platform to present mature and early stage ideas, promote discussion and exchange, and build a community of researchers and practitioners in cyber threat intelligence.

Christian Doerr
TU Delft, Netherlands

Workshop Program Committee WCTI 2019

- 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 2019 Program

WCTI I

Zero Residual Attacks on Industrial Control Systems and Stateful Countermeasures
Hamid Reza Ghaeini (Singapore University of Technology and Design, Singapore), Nils Ole Tippenhauer (CISPA, Germany) and Jianying Zhou (Singapore University of Technology and Design, Singapore)

2nd International Workshop on Cyber Threat Intelligence Management (CyberTIM 2019)

Message from the CyberTIM Workshop Organizers

It is our great pleasure to welcome you to the second International Workshop on Cyber Threat Intelligence Management (CyberTIM), which takes place in conjunction with the ARES conference in Canterbury, United Kingdom from August 26th to 29th, 2019.

The increased sophistication of cyber-attacks has created a technology arm race between attackers and defenders. However, this arm race is not fought in equal terms. For example, defenders are somewhat disadvantaged due to lack of manpower coupled with an overwhelming number of sophisticated attacks, e.g. advanced persistent threats; thus, making cyber defense extremely difficult. There is also due to lack of collaboration among cyber and network security solutions, e.g., intrusion detection systems and honeypots.

In recent years, organizations like CERTs, NRENs, as well as industry organizations are moving towards proactive detection capabilities leveraging Cyber Threat Intelligence (CTI) platforms. These platforms include advanced alert aggregation, correlation, and prioritization, focusing on the asset criticality of organizations and the quality of shared threat intelligence. The goal of CyberTIM is to bring the industry practitioners, researchers, engineers, and academic researchers together from different domains, such as network security, network measurements, cyber incident monitoring, trust and risk management, cyber situational awareness, security analytics, and security visualization.

From the received submissions (14 papers) and after an in-depth review process, as well as discussions of the organizing committee, we accept six best papers for presentation in the workshop. In other words, the acceptance rate is 42%. We separate the talks into two main themes, namely: i) threat prediction, detection and mitigation and ii) threat intelligence sharing. Lastly, we are grateful to Dr. Panayiotis Kikiras for agreeing to give a keynote talk at the workshop.

The Workshop & Program Committee Chairs

Dr. Emmanouil Vasilomanolakis, *Aalborg University, Denmark*
Dr. Jassim Happa, *University of Oxford, UK*
Dr. Kim-Kwang Raymond Choo, *The University of Texas at San Antonio, USA*

Steering Committee

Dr. Brian Lee, *Athlone Institute of Technology, Ireland*
Dr. Fabio Martinelli, *IIT, C.N.R, Italy*
Dr. Sheikh Mahbub Habib, *Continental AG, Frankfurt, Germany*
Dr. Max Mühlhäuser, *Technische Universität Darmstadt, Germany*

Workshop Program Committee CyberTim 2019

- David Chadwick, *University of Kent, UK*
- Michal Choras, *ITTI Ltd., Poland*
- Theo Dimitrakos, *European Security Competence Center, Huawei Technologies, UK*
- Jason Nurse, *University of Kent, UK*
- Marcin Przybyszewski, *ITTI Ltd., Poland*
- Georgios Kambourakis, University of the Aegean, Grecce
- Andrea Tundis, TU Darmstadt, Germany
- Salvador Llopis, Universitat Politecnica de Valencia, Spain
- Jens Myrup Pedersen, Aalborg University, Denmark
- Abhijit Ambekar, Continental Teves AG & Co. oHG, Germany
- Xiaolu Zhang, University of Texas at San Antonio, USA
- Shankar Karuppayah, Universiti Sains Malaysia, Malaysia
- Reza M. Parizi, Kennesaw State University, USA
- Jörg Daubert, Philipps-Universität Marburg, Germany
- Andrea Saracino, Consiglio Nazionale delle Ricerche, Italy

External Reviewers

Gautam Srivastava
Sebastian Kauschke

CyberTIM 2019 Program

CyberTIM I – Keynote Session

CyberTIM II - Threat prediction, detection and mitigation

AIDA Framework: Real-Time Correlation and Prediction of Intrusion Detection Alerts,
Martin Husák (Masaryk University, Czechia) and Jaroslav Kašpar (Masaryk University, Czechia)

Automated Pattern Inference Based on Repeatedly Observed Malware Artifacts,
Christian Doll (Fraunhofer, Germany), Arnold Sykosch (University of Bonn, Fraunhofer FKIE, Germany), Marc Ohm (University of Bonn, Germany) and Michael Meier (University of Bonn, Fraunhofer FKIE, Germany)

A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources,
Thomas Schaberreiter (University of Vienna, Austria), Veronika Kupfersberger (University of Vienna, Austria), Konstantinos Rantos (Technological Educational Institute of Eastern Macedonia and Thrace, Greece), Arnolnt Spyros (Innovative Secure Technologies, Greece) , Alexandros Papanikolaou (Innovative Secure Technologies, Greece), Christos Ilioudis (Alexander Technological Educational Institute of Thessaloniki, Greece) and Gerald Quirchmayr (University of Vienna, Austria)

CyberTIM III - Threat Intelligence Sharing

NERD: Network Entity Reputation Database,
Václav Bartoš (CESNET, Czechia)

Cyber Threat Information Sharing: Perceived Benefits and Barriers,
Adam Zibak (University of Oxford, United Kingdom) and Andrew Simpson (University of Oxford, United Kingdom)

Automated Cyber Threat Sensing and Responding: Integrating Threat Intelligence into Security-Policy-Controlled Systems,
Peter Amthor (Technische Universität Ilmenau, Germany), Daniel Fischer (Technische Universität Ilmenau, Germany), Winfried Kühnhauser (Technische Universität Ilmenau, Germany) and Dirk Stelzer (Technische Universität Ilmenau, Germany)

2nd International Workshop on Behavioral Authentication for System Security (BASS 2019)

Message from the BASS Workshop Organizers

Behavioral features are getting in the last years an increasing attention from both IT research and industrial world. Human behavioral aspects are extremely valuable pieces of information, exploited by companies to profile current or potential customers, in order to anticipate their preferences and presenting custom offers. Runtime behavioral analysis is being applied with increasing success for continuous and silent user authentication, and is considered an enabler for the seamless authentication paradigm in several environment and devices. Furthermore, behavioral analysis is posing itself as a valuable alternative to signature-based approaches to identify anomalies, intrusions, security attacks and system malfunctioning. These approaches are in fact known to be flexible, self-learning and able to consider multi-level and multi-domain features, related to software execution, system status, user interaction and current context.

BASS aims at attracting innovative contributions from both industry and academia related to all aspects of human, system or software behavioral analysis for IT security.

The Workshop organizing committee

Andrea Saracino, *IIT-CNR, Italy*
Alessandro Aldini, *Università di Urbino, Italy*
Francesco Mercaldo*, IIT-CNR, Italy*

Workshop Program Committee BASS 2019

- Alberto Ferrante, *Università della Svizzera Italiana, Switzerland*
- Jelena Milosevic*, Institute of Telecommunications, TU Wien, Austria*
- Fabio di Troia, *San Jose University, United States*
- Martina Lindorfer, *University of California, Santa Barbara, United States*
- Antonella Santone, *University of Molise, Italy*
- Peter Kieseberg, *SBA Research, Austria*
- Daniele Sgandurra, *Royal Halloway University of London, UK*
- Vasileios Gkioulos, *Norwegian University of Technology and Science, Trondheim, Norway*
- Robert Künnemann, *Saarland Univ., Germany*
- Nicola Zannone, *TU/e, Eindhoven, Netherlands*
- Laura Genga, *TU/e, Eindhoven, Netherlands*
- Emiliano de Cristofaro, *UCL, UK*
- Menmeng Ge, *Deakin University, Australia*
- Kevin Allix, *Luxembourg Univ., Luxembourg*

BASS 2019 Program

BASS I – Privacy, Authentication, and Access Control

Privacy-Enhancing Context Authentication from Location-Sensitive Data
Pradip Mainali (OneSpan, Belgium), Carlton Shepherd (OneSpan, United Kingdom), and Fabien A. P. Petitcolas (OneSpan, Belgium)

Semantic Mediation for A Posteriori Log Analysis
Farah Dernaika (IMT Atlantique, France), Nora Cuppens-Boulahia (IMT Atlantique, France), Frédéric Cuppens (IMT Atlantique, France) and Olivier Raynaud (LIMOS, France)

Alexa's Voice Recording Behavior: A Survey of User Understanding and Awareness
Yousra Javed (Illinois State University, United States), Shashank Sethi (Illinois State University, United States) and Akshay Jadoun (Illinois State University, United States)

BASS II - Communication networks

Adversarial Communication Networks Modeling for Intrusion Detection Strengthened against Mimicry
Jorge Maestre Vidal (Universidad Complutense de Madrid, Spain) and Marco Antonio Sotelo Monge (Universidad Complutense de Madrid, Spain)

1st International Workshop on Information Security Methodology and Replication Studies (IWSMR 2019)

Message from the IWSMR Workshop Organizers

In recent years, research started to focus on the scientific fundamentals of information security. These fundamentals include several important aspects such as the unified description of attacks and countermeasures, the reproducibility of experiments, the sharing of research data and code, the discussion of quality criteria for experiments and the design and implementation of testbeds. The related academic publications contributed to the advancement of information security research, e.g. by making research contributions easier to compare. Moreover, work on terminology and taxonomy addressed redundancies and unified the understanding between different sub-domains of information security.

The First International Workshop on Information Security Methodology and Replication Studies (IWSMR 2019) was held in conjunction with ARES 2019 in Canterbury, UK. The workshop desired to foster the progress in research on the scientific methodology of information security, to improve the links between sub-domains of information security research and to advance the discussion on the scientific methodology in information security.

We like to thank the ARES organizers for their kind support. Moreover do we like to thank all authors who submitted a paper to IWSMR and all reviewers for their high-quality reviews.

The Workshop organizing committee

Steffen Wendzel, *Worms University of Applied Sciences, Germany*
Luca Caviglione, *Inst. Appl. Math. & Inf. Techn. (IMATI), National Research Council (CNR), Italy*
Alessandro Checco, *University of Sheffield, UK*
Aleksandra Mileva, *University Goce Delcev, Macedonia*
Jean-Francois Lalande, *CentraleSupélec, France*
Wojciech Mazurczyk, *Warsaw University of Technology, Poland*

Workshop Program Committee IWSMR 2019

- Krzysztof Cabaj, *Warsaw University of Technology, Poland*
- Bela Genge, *Petru Maior University of Tg Mures, Romania*
- Nils Gruschka, *University of Oslo, Norway*
- Karl Jonas, *Bonn Rhine-Sieg University, Germany*
- Jörg Keller, *University of Hagen, Germany*
- Thomas Kemmerich, *University of Bremen, Germany / NTNU, Norway*
- Hanno Langweg, *HTWG Konstanz, Germany*
- Michael Meier, *University of Bonn, Germany*
- Frederic Petit, *Argonne National Laboratory, USA*
- Slobodan Petrovic, *Gjøvik University College, Gjøvik, Norway*
- Michael Rademacher, *Bonn Rhine-Sieg University, Germany*
- Ruben Rios, *University of Malaga, Spain*
- Peter Schartner, *Klagenfurt University, Austria*
- Roland Varriale, *Argonne National Laboratory, USA*
- Simon Vrhovec, *University of Maribor, Slovenia*
- Christian Hummert, *ZITiS, Germany*
- Olaf Maennel, *Tallinn University of Technology, Estonia*

IWSMR 2019 Program

IWSMR I

Analysis of User Evaluations in Security Research
Peter Hamm (Goethe University Frankfurt, Germany), David Harborth (Goethe University Frankfurt, Germany) and Sebastian Pape (Goethe University Frankfurt, Germany)

The power of interpretation: Qualitative methods in cybersecurity research
Damjan Fujs (University of Maribor, Slovenia), Anže Mihelič (University of Maribor, Slovenia) and Simon Vrhovec (University of Maribor, Slovenia)

Examining and Constructing Attacker Categorisations - an Experimental Typology for Digital Banking
Moeckel Caroline (Royal Holloway, University of London, United Kingdom)

1st International Workshop on Location Privacy (LPW 2019)

Message from the LPW Workshop Organizers

Location and mobility data are highly sensitive, as they can be used to infer a number of other personal and sensitive data on an individual. However, human mobility is highly predictable, and location information is routinely collected by location-aware devices (e.g. smartphones), connected vehicles and smart transportation systems, e-tolling, and cameras with face recognition among others.

Location privacy is a rapidly developing research area, and the first Location Privacy Workshop (LPW) provides a platform for original research and discussion on all technical aspects of privacy and security of location-based services.

Among the received submissions, we have selected the 5 best for presentation, which have been arranged into 3 sessions.

The Workshop organizing committee

Paolo Palmieri, *University College Cork, Ireland* (co-chair)
Luca Calderoni, *University of Bologna, Italy* (co-chair)

Workshop Program Committee LPW 2019

- Antoine Boutet – *INSA de Lyon, France*
- Mauro Conti – *University of Padua, Italy*
- Chhagan Lal – *University of Padua, Italy*
- Zekeriya Erkin – *Delft University of Technology, The Netherlands*
- Sébastien Gambs – *Université du Québec à Montréal, Canada*
- Kimmo Järvinen – *University of Helsinki, Finland*
- Ioannis Krontiris – *Huawei European Research Center, Germany*
- Jelena Milosevic – *TU Vienna, Austria*
- Jun Pang – *University of Luxembourg, Luxembourg*
- Constantinos Patsakis – *University of Piraeus, Greece*
- Francesco Regazzoni – *University of Lugano, Switzerland*
- Simonas Šaltenis – *Aalborg University, Denmark*
- Michael Solomon – *University of Cumberlands, USA*
- Guillermo Suarez de Tangil – *King's College London, UK*

LPW 2019 Program

LPW I

eBook Readers, Location Surveillance and the Threat to Freedom of Association
Stephen Wicker (Cornell University, United States)

LPW II

Securing V2X Communications for the Future - Can PKI Systems offer the answer?
Thanassis Giannetsos (Technical University of Denmark, Denmark) and Ioannis Krontiris (European Research Center, Huawei Technologies, Germany)

Location Tracking Using Smartphone Accelerometer and Magnetometer Traces
Khuong An Nguyen (Department of Computer Science, Royal Holloway, University of London, United Kingdom), Raja Naeem Akram (ISG-Smart Card Centre, Royal Holloway, University of London, United Kingdom), Konstantinos Markantonakis (ISG-Smart Card Centre, Royal Holloway, University of London, United Kingdom), Zhiyuan Luo (Royal Holloway, University of London, United Kingdom) and Chris Watkins (Royal Holloway, University of London, United Kingdom

LPW III

A Location Privacy Analysis of Bluetooth Mesh
Matthias Caesar (Fraunhofer SIT, Fraunhofer Institute for Secure Information Technology SIT, Germany) and Jan Steffan (Fraunhofer SIT, Fraunhofer Institute for Secure Information Technology SIT, Germany)

DEMISe: Interpretable Deep Extraction and Mutual Information Selection Techniques for IoT Intrusion Detection
Paul Yoo (Birkbeck, University of London, United Kingdom), Luke Parker (Ministry of Defence, United Kingdom), Taufiq Asyhari (Coverntry University, United Kingdom, Yoonchan Jhi (Samsung Electronics, South Korea), Kamal Taha (Khalifa University, United Arab Emirates) and Lounis Chermak (Cranfield University, United Kingdom)

1st International Workshop on Industrial Security and IoT (WISI 2019)

Message from the WISI Workshop Organizers

The factory of the future requires an effective interconnection of machinery, robots, lines, products, sensors and operators to each other and to back-end systems. The industrial propagation environment may also be harsh and may suffer from man-made, impulsive interference. Industrial IoT priorities are security, low latency, reliability and low cost. However, smart factories are also looking for enhanced services for people and machines that create an added value that is beyond the limits of the production environment, such as indoor localization, smart logistic support, remote maintenance and access to machine data and advanced IT infrastructure, smart tracking of connected components and products. Workshop on Industrial Security and IoT (co-located with the ARES-conference) focuses on bringing together researchers from all over the world to share their experience and present recent research. In this workshop we discuss security demands of Industry 4.0, as well as specific security tools and methods, which enable interconnection of engineering activities at multiple levels of security and safety, in order to improve system resilience and to support security lifecycle management.

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

The Workshop organizing committee

Stefan Jaksic, *AIT Austrian Institute of Technology, Austria*

Julia Pammer, *SBA Research, Austria*

Workshop Program Committee WISI 2019

- Omar Veledar, *AVL List, Austria*
- Raphael Spreitzer, *SGS Digital Trust Services GmbH, Austria*
- Katharina Pfeffer, *SBA Research, Austria*
- Lukas Krammer, *Siemens AG , Austria*
- Mario Lamberger, *NXP Semiconductors*
- Ezio Bartocci, *TU Wien, Austria*
- Dejan Nickovic, *AIT Austrian Institute of Technology, Austria*
- Violeta Damjanovic-Behrendt, *Salzburg Research, Austria*
- Christoph Schmittner, *AIT Austrian Institute of Technology, Austria*
- Thomas Loruenser, *AIT Austrian Institute of Technology, Austria*
- Rupert Schlick, *AIT Austrian Institute of Technology, Austria*
- Christos Thomos, I*nfineon Austria, Austria*
- Edin Arnautovic, *TTTech, Austria*
- Rudolf Ramler, *Software Competence Center Hagenberg*
- Peter Priller, *AVL List GmbH, Austria*
- Sebastian Ramacher, *Graz University of Technology, Austria*
- Radu Grosu, *TU Wien, Austria*
- Christoph Striecks, *AIT Austrian Institute of Technology, Austria*
- Muhammad Shafique, *TU Wien, Austria*
- Willibald Krenn, *AIT Austrian Institute of Technology, Austria*
- Mario Drobics, *AIT Austrian Institute of Technology, Austria*

WISI 2019 Program

WISI I

Using Temporal and Topological Features for Intrusion Detection in Operational Networks
Simon Duque Anton (Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Germany), Daniel Fraunholz (Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Germany) and Hans Dieter Schotten (Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Germany)

Performance Evaluation of Elliptic-Curve Libraries on Automotive-Grade Microcontrollers
Lucian Popa (Politehnica University of Timisoara, Romania), Bogdan Groza (Politehnica University of Timisoara, Romania) and Pal-Stefan Murvay (Politehnica University of Timisoara, Romania)

WISI II

Applicability of the IEC 62443 standard in Industry 4.0 / IIoT
Björn Leander (Mälardalen University & ABB, Sweden), Aida Causevic (Mälardalen University, Sweden) and Hans Hansson (Mälardalen University, Sweden)

Requirements and Recommendations for IoT/IIoT Models to automate Security Assurance through Threat Modelling, Security Analysis and Penetration Testing
Ralph Ankele (JOANNEUM RESEARCH Forschungsgesellschaft mbH, Austria), Stefan Marksteiner (AVL List GmbH, Austria), Kai Nahrgang (JOANNEUM RESEARCH Forschungsgesellschaft mbH, Austria) and Heribert Vallant (JOANNEUM RESEARCH Forschungsgesellschaft mbH, Austria)

Federated Identity Management and Interoperability for Heterogeneous Cloud Platform Ecosystems
Nirojan Selvanathan (Salzburg Research, Austria), Dileepa Jayakody (Salzburg Research, Austria) and Violeta Damjanovic-Behrendt (Salzburg Research, Austria)

The 5th ARES 2019 EU Projects Symposium

Welcome to the ARES EU Projects Symposium!

The ARES EU Projects Symposium is held for the fifth 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, three workshops will be held within the ARES EU Projects Symposium:

- 2nd International Workshop on 5G Networks Security (5G-NS 2019)
- 2nd International Workshop on Physical and Cyber Security in Port Infrastructures (PCSCP 2019)
- 1st International Workshop on Next Generation Security Operations Centers (NG-SOC 2019)

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 2nd International Workshop on 5G Networks Security (5G-NS 2019)

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.

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 these issues and follow security-by-design approaches. Finally, since in 5G networks even more user data and network traffic will be transmitted, big data security solutions should be considered in order to address the magnitude of the data volume and ensure data security and privacy.

From this perspective, the 5G-NS 2019 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

Wojciech Mazurczyk, *Warsaw University of Technology, Poland (IoRL H2020 Project)*
Pascal Bisson, *Thales, France (5G-Ensure H2020 Project, 5G IA SEC WG Chair)*
Krzysztof Cabaj, *Warsaw University of Technology, Poland (IoRL H2020 Project)*
Edgardo Montes de Oca, *Montimage, France (Networld2020 steering board member)*

Workshop Program Committee 5G-NS 2019

- Gregory Blanc, *Télécom SudParis, Institut Mines-Télécom, France*
- Rolf Blom, *RISE SICS, Sweden Gino Carrozzo, Nextworks, Italy*
- Luca Caviglione, *IMATI CNR, Italy*
- Joo Cho, *Adva Optical, Germany*
- Michal Choraś, *ITTI Ltd., Poland*
- Jannik Dreier, *Université de Lorraine, France*
- Jin Hong, *University of Western Australia, Australia*
- Raimo Kantola, *Aalto University, Finland*
- Georgios Karopoulos, *National and Kapodistrian University of Athens, Greece*
- Zbigniew Kotulski, *Warsaw University of Technology, Poland*
- Poland Madhusanka Liyanage*, University of Oulu, Finland*
- Peter Schneider, *Nokia Bell Labs, Germany*
- Jani Suomalainen, *VTT, Finland*
- Hui Tian, *National Huaqiao University, China*

5G-NS 2019 Program

5G-NS I

6G Network Needs to Support Embedded Trust
Raimo Kantola (Aalto University, Finland)

Framework for Anticipatory Self-Protective 5G Environments
Marco Antonio Sotelo Monge (Universidad Complutense de Madrid, Spain) and Jorge Maestre Vidal (Universidad Complutense de Madrid, Spain)

5G-NS II

Securing Ethernet-based Optical Fronthaul for 5G Network
Joo Yeon Cho (ADVA Optical Networking SE, Germany), Andrew Sergeev (ADVA Optical Networking Israel Ltd., Israel) and Jim Zou (ADVA Optical Networking SE, Germany

Towards a Security Architecture for Hybrid WMNs
Markus Theil (Technische Universitaet Ilmenau, Germany), Martin Backhaus (Technische Universitaet Ilmenau, Germany), Michael Rossberg (Technische Universitaet Ilmenau, Germany) and Guenter Schaefer (Technische Universitaet Ilmenau, Germany)

Sniffing Detection within the Network: Revisiting Existing and Proposing Novel Approaches
Krzysztof Cabaj (Warsaw University of Technology, Poland), Marcin Gregorczyk (Warsaw University of Technology, Poland), Wojciech Mazurczyk (Warsaw University of Technology, Poland), Piotr Nowakowski (Warsaw University of Technology, Poland) and Piotr Żórawski (Warsaw University of Technology, Poland)

The 2nd International Workshop on Physical and Cyber Security in Port Infrastructures (PCSCP 2019)

Welcome Message from the PCSCP 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 protecting critical infrastructures, particularly port infrastructures, by enhancing threat modelling and situational awareness. The topics are coming from various current research projects, especially from H2020 SAURON as well as H2020 CyberSec4Europe and Ecsel. These approaches support not only port operators to increase the protection and resilience of their infrastructures against physical and cyber threats to an adequate level. The main focus lies on determining the potential consequences of any incident to identify potential cascading effects of a detected threat in the physical and the cyber domain.

In detail, the workshop provides a brief introduction into the SAURON project with an update on the current activities. Additionally, it covers an overview on a tool for structured threat modelling and how cascading effects can be modelled, identified and assessed, including an explicit exampled how the approach can be applied in a realistic scenario. Furthermore, use case scenarios from the SAURON project as well as from the CyberSec4Europe project are presented to sketch some of the problems critical (port) infrastructures are currently facing. Finally, the workshop also covers a description on how the ISPS code and an according risk management can be implemented within a port.

In particular, our special thanks are due to Bettina Jaber, Julia Pammer and Yvonne Poul for their kind assistance and help with the preparation of this workshop.

Stefan Schauer
PSCSP 2019 Workshop Chair
AIT Austrian Institute of Technology, Austria

Rafa Company
PSCSP 2019 Workshop Chair
Fundación Valenciaport, Spain

Federico Carvajal
PSCSP 2019 Workshop Chair
Universidad Politécnica de Valencia, Spain

Richard Chisnall
PSCSP 2019 Workshop Chair
Innovasec, UK

The 1st International Workshop on Next Generation Security Operations Centers (NG-SOC 2019)

Welcome Message from the NG-SOC Workshop Organizers

Globally, organisations face the difficult task of detecting and responding to increasing numbers of cyber-attacks and threats, given that their own ICT infrastructures are complex, constantly changing (e.g., through the introduction of new technologies) and there is a shortage of qualified cybersecurity experts. There is a great need to drastically reduce the time to detect and respond to cyber-attacks, and to enable organisations to structurally stay ahead of the threat. A key means for organizations to stay ahead of the threat is through the establishment of a Security Operations Center (SOC). The primary purpose of a SOC is to monitor, assess and defend the information assets of an enterprise, both on a technical and organizational level.

The aim of this workshop is to create a forum for researchers and practitioners to discuss the challenges associated with SOC operations and focus on research contributions that can be applied to address these challenges. The workshop will draw on expertise from a newly-awarded H2020 project, called SOCCRATES. Selected members of the SOCCRATES consortium will present their past and proposed project activities, along with experts from carefully-selected related initiatives. It is intended the workshop will foster discussion on this important topic and highlight the major operational challenges that enterprises and SOC operators face, and provide insights into promising research-based solutions.

The Workshop organizing committee

Ewa, Piatkowska, *AIT Austrian Institute of Technology, Austria*

Paul, Smith, *AIT Austrian Institute of Technology, Austria*

Reinder, Wolthuis, *TNO, Netherlands*

Frank, Fransen, *TNO, Netherlands*

ARES 2019 Table of Contents

ARES 2019 Program: Full Papers

ARES Full I - Dependability and resilience

ARES Full II - Best Paper Session

ARES Full III - Software security

ARES Full IV - Cryptographic mechanisms and applications I

A10_Practical Group-Signatures with Privacy-Friendly Openings

Stephan Krenn (AIT Austrian Institute of Technology GmbH, Austria), Kai Samelin (TÜV Rheinland i-sec GmbH, Germany) and Christoph Striecks (AIT Austria, Austria)

A11_E2E Verifiable Borda Count Voting System without Tallying Authorities

Samiran Bag (The University of Warwick, United Kingdom), Muhammad Ajmal Azad (University of Derby, United Kingdom) and Feng Hao ((The University of Warwick, United Kingdom)

ARES Full V - Cryptographic mechanisms and applications II

A12_SET-OT: A Secure Equality Testing Protocol Based on Oblivious Transfer

Ferhat Karakoç (Kuveyt Türk Participation Bank Research and Development Center, Turkey), Majid Nateghizad (Cyber Security Group, Department of Intelligent Systems, Delft University of Technology, Netherlands) and Zekeriya Erkin (Cyber Security Group, Department of Intelligent Systems, Delft University of Technology, Netherlands)

A13_Anonymous Identity Based Encryption with Traceable Identities

Olivier Blazy (Université de Limoges, France), Laura Brouilhet (Université de Limoges, France) and Duong-Hieu Phan (Université de Limoges, France)

ARES Full VI - Network Security I

A14_Towards Efficient Reconstruction of Attacker Lateral Movement

Florian Wilkens (University of Hamburg, Germany), Steffen Haas (University of Hamburg, Germany), Dominik Kaaser (University of Hamburg, Germany), Peter Kling (University of Hamburg, Germany) and Mathias Fischer (University of Hamburg, Germany)

A15_Strong Tenant Separation in Cloud Computing Platforms

Michael Pfeiffer (Technische Universität Ilmenau, Germany), Michael Rossberg (Technische Universität Ilmenau, Germany), Simon Buttgereit (Technische Universität Ilmenau, Germany) and Guenter Schaefer (Technische Universität Ilmenau, Germany)

A16_Blockchain Trilemma Solver Algorand has Dilemma over Undecidable Messages

Mauro Conti (University of Padua, Italy), Ankit Gangwal (University of Padova, Italy) and Michele Todero (University of Padova, Italy)

ARES Full VII – Web security and attacks

A17_PoliDOM: Mitigation of DOM-XSS by Detection and Prevention of Unauthorized DOM Tampering

Junaid Iqbal (University of New Brunswick, Canada), Ratinder Kaur (University of Saskatchewan, Canada) and Natalia Stakhanova (University of Saskatchewan, Canada)

A18_Towards a framework for detecting advanced Web bots

Christos Iliou (Information Technologies Institute, CERTH, Greece), Theodoros Kostoulas (Department of Computing and Informatics, Bournemouth University, United Kingdom), Theodora Tsikrika (Information Technologies Institute, CERTH, Greece), Vasilis Katos (Department of Computing and Informatics, Bournemouth University, United Kingdom), Stefanos Vrochidis (Information Technologies Institute, CERTH, Greece) and Yiannis Kompatsiaris (Information Technologies Institute, CERTH, Greece)

A19_Characterizing the Redundancy of DarkWeb .onion Services

Pavlo Burda (Eindhoven University of Technology, Netherlands), Coen Boot (Radboud University, Netherlands)and Luca Allodi (Eindhoven University of Technology, Netherlands)

ARES Full VIII - Network Security I

A20_Detecting DGA domains with recurrent neural networks and side information

Ryan Curtin (Symantec Corporation, United States), Andrew Gardner (Symantec Corporation, United States), Slawomir Grzonkowski (Symantec Corporation, Ireland), Alexey Kleymenov (Symantec Corporation, Ireland) and Alejandro Mosquera Lopez (Symantec Corporation, United States)

A21_Black Box Attacks on Deep Anomaly Detectors

Aditya Kuppa (Symantec Corporation and School of Computer Science University College, Dublin, Ireland), Slawomir Grzonkowski (Symantec Corporation, Ireland), Muhammad Rizwan Asghar (School of Computer Science The University of Auckland, New Zealand) and Nhien An Le Khac (School of Computer Science University College, Dublin, Ireland)

ARES 2019 Program: Short Papers

ARES Short I - Identity, authorization and privacy

A22_On the Exploitation of Online SMS Receiving Services to Forge ID Verification

Muhammad Hajian Berenjestanaki (University of Tehran, Iran), Mauro Conti (University of Padua, Italy) and Ankit Gangwal (University of Padova, Italy)

A23_Does “www.” Mean Better Transport Layer Security?

Eman Alashwali (University of Oxford, United Kingdom), Pawel Szalachowski (Singapore University of Technology and Design (SUTD), Singapore) and Andrew Martin (University of Oxford, United Kingdom)

A24_An Attribute-Based Privacy-Preserving Ethereum Solution for Service Delivery with Accountability Requirements

Francesco Buccafurri (DIIES – Universita’ Mediterranea di Reggio Calabria, Italy), Vincenzo De Angelis (DIIES – Universita’ Mediterranea di Reggio Calabria, Italy), Gianluca Lax (DIIES – Universita’ Mediterranea di Reggio Calabria, Italy), Lorenzo Musarella (DIIES – Universita’ Mediterranea di Reggio Calabria, Italy) and Antonia Russo (DIIES – Universita’ Mediterranea di Reggio Calabria, Italy)

ARES Short II - Threat detection and response

A25_STAMAD – a STAtic MAlware Detector

Khanh Huu The Dam (Nha Trang University, Viet Nam) and Tayssir Touili (LIPN, CNRS & University Paris 13, France)

A26_Enhancing credibility of digital evidence through provenance-based incident response handling

Ludwig Englbrecht (University of Regensburg, Germany), Gregor Langner (University of Vienna, Austria), Günther Pernul (University of Regensburg, Germany) and Gerald Quirchmayr (University of Vienna, Austria)

A27_Language-based Integration of Digital Forensics & Incident Response

Christopher Stelly (University of New Orleans, United States) and Vassil Roussev (University of New Orleans, United States)

ARES Short III -

A28_Post-Quantum UC-Secure Oblivious Transfer in the Standard Model with Adaptive Corruptions

Olivier Blazy (Université de Limoges, France), Céline Chevalier (ENS, France) and Quoc Huy Vu (DIENS, École normale supérieure, CNRS, INRIA, PSL University, Paris, France)

A29_On the Utility of Synthetic Data: An Empirical Evaluation on Machine Learning

Markus Hittmeir (SBA Research, Austria), Andreas Ekelhart (SBA Research, Austria) and Rudolf Mayer (SBA Research, Austria)

A30_Building Taxonomies based on Human-Machine Teaming: Cyber Security as an Example

Mohamad Imad Mahaini (The University of Kent, United Kingdom), Shujun Li (The University of Kent, United Kingdom) and Rahime Belen Sağlam (Ankara Yıldırım Beyazıt University, Turkey)

FARES 2019 Program

FARES I - Protection and Detection

A31_A Pattern for a Virtual Network Function (VNF)

Ahmed Alwakeel (Florida Atlantic University, United States), Abdulrahman Alnaim (Florida Atlantic University, United States) and Eduardo B. Fernandez (Florida Atlantic University, United States)

A32_Near-optimal Evasion of Randomized Convex-inducing Classifiers in Adversarial Environments

Pooria Madani (York University, Canada) and Natalija Vlajic (York University, Canada)

A33_AMON: an Automaton MONitor for Industrial Cyber-Physical Security

Giuseppe Bernieri (Department of Mathematics University of Padua, Italy), Mauro Conti (Department of Mathematics University of Padua, Italy) and Gabriele Pozzan (Department of Mathematics University of Padua, Italy)

A34_Decision Support for Mission-Centric Cyber Defence

Michal Javorník (Masaryk University, Czechia), Jana Komárková (Masaryk University, Czechia) and Martin Husák (Masaryk University, Czechia)

FARES II - Measurement and Robust Design

A35_Managing the over-estimation of resilience

Thomas Clédel (IMT Atlantique, France), Frédéric Cuppens (TELECOM Bretagne, France) and Nora Cuppens-Boulahia (IMT Atlantique, France)

A36_GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform

Martin Horák (Masaryk University, Czechia), Václav Stupka (Masaryk University, Czechia) and Martin Husák (Masaryk University, Czechia)

A37_Cyber Security Skill Set Analysis for Common Curricula Development

Muhammad Mudassar Yamin (Norwagian University of Science and Technology, Norway) and Basel Katt (Norwagian University of Science and Technology, Norway)

WSDF 2019 Program

WSDF I

A38_Assessing the Applicability of Authorship Verification Methods

Oren Halvani (The Fraunhofer Institute for Secure Information Technology SIT, Germany), Christian Winter (The Fraunhofer Institute for Secure Information Technology SIT, Germany) and Lukas Graner (The Fraunhofer Institute for Secure Information Technology SIT, Germany)

A39_Improved Manipulation Detection with Convolutional Neural Network for JPEG Images

Huajian Liu (Fraunhofer, Germany), Martin Steinebach (Fraunhofer, Germany) and Kathrin Schölei (Fraunhofer, Germany)

A40_Deep Learning-based Facial Detection and Recognition in Still Images for Digital Forensics

Patricio Domingues (ESTG – Leiria, Portugal) and Alexandre Frazão Rosário (IT, Portugal)

WSDF II

A41_Revisiting Data Hiding Techniques for Apple File System

Thomas Göbel (University of Applied Sciences Darmstadt, Germany), Jan Türr (University of Applied Sciences Darmstadt, Germany) and Harald Baier (University of Applied Sciences Darmstadt, Germany)

A42_Map My Murder! A Digital Forensic Study of Mobile Health and Fitness Applications

Courtney Hassenfeldt (University of New Haven, United States), Shabana Baig (University of New Haven, United States), Ibrahim Baggili (University of New Haven, United States) and Xiaolu Zhang (University of Texas at San Antonio, United States)

A43_Methodology for the Automated Metadata-Based Classification of Incriminating Digital Forensic Artefacts

Xiaoyu Du (University College Dublin, Ireland) and Mark Scanlon (University College Dublin, Ireland)

WSDF III

A44_A Study of Network Forensic Investigation in Docker Environments

Daniel Spiekermann (FernUniversität in Hagen, Germany), Tobias Eggendorfer (HS Weingarten, Germany) and Jörg Keller (FernUniversität in Hagen, Germany)

A45_IO-Trust: An out-of-band trusted memory acquisition for intrusion detection and Forensics investigations in cloud IOMMU based systems

Ahmad Atamli (Alan Turing Institute, University of Cambridge, United Kingdom) and Jon Crowcroft (Alan Turing Institute, University of Cambridge, United Kingdom)

A46_IoT Ignorance is Digital Forensics Research Bliss: A Survey to Understand IoT Forensics Definitions, Challenges and Future Research Directions

Tina Wu (University of Oxford, United Kingdom), Frank Breitinger (University of New Haven, United States) and Ibrahim Baggili (University of New Haven, United States)

IWSMA 2019 Program

IWSMA I

A47_Analyzing Android's File-Based Encryption: Information Leakage through Unencrypted Metadata

Tobias Groß (Friedrich-Alexander University, Germany), Matanat Ahmadova (University of Bonn, Germany) and Tilo Müller (Friedrich-Alexander University, Germany)

A48_Post-Quantum Cryptography in Embedded Systems

Soundes Marzougui (TU Darmstadt, Germany) and Juliane Krämer (TU Darmstadt, Germany)

A49_The Internet Banking [in]Security Spiral: Past, Present, and Future of Online Banking Protection Mechanisms based on a Brazilian case study

Marcus Botacin (Federal University of Brazil, Brazil), Anatoli Kalysch (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany), Tilo Mueller (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany) and Andre Gregio (UFPR, Brazil)

IWCC 2019 Program

IWCC I

A50_An Analysis Framework for Product Prices and Supplies in Darknet Marketplaces
York Yannikos (Fraunhofer, Germany), Julian Heeger (Fraunhofer, Germany) and Maria Brockmeyer (TU Darmstadt, Germany)

A51_Limits in the data for detecting crimincals on social media
Andrea Tundis (TU Darmstadt, Germany), Leon Böck (Technische Universität Darmstadt (TUDA), Germany), Victoria Stanilescu (Siemens AG, Germany) and Max Mühlhäuser (TU Darmstadt, Germany)

IWCC II

A52_Ontology of Metrics for Cyber Security Assessment
Elena Doynikova (St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Russia), Andrey Fedorchenko (St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Russia) and Igor Kotenko (St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Russia)

A53_Large-Scale Analysis of Pop-Up Scam on Typosquatting URLs
Tobias Dam (FHSTP UAS, Austria), Lukas Daniel Klausner (FHSTP UAS, Austria), Damjan Buhov (Josef Ressel Center TARGET, Austria) and Sebastian Schrittwieser (SBA Research, Austria)

A54_Realistically Fingerprinting Social Media Webpages in HTTPS Traffic
Mariano Di Martino (Hasselt University / Expertise Center For Digital Media, Belgium), Peter Quax (Hasselt University / Expertise Center For Digital Media, Belgium) and Wim Lamotte (Hasselt University / Expertise Center For Digital Media, Belgium)

IWCC III

A55_Fake News Detection by Image Montage Recognition
Martin Steinebach (Fraunhofer, Germany), Huajian Liu (Fraunhofer, Germany) and Karol Gotkowski (Fraunhofer, Germany)

A56_HEHLKAPPE: Utilizing Deep Learning to Manipulate Surveillance Camera Footage in Real-Tim
Alexander Aigner (University of Applied Sciences Upper Austria, Austria) and Rene Zeller (University of Applied Sciences Upper Austria, Austria)

A57_Improving Borderline Adulthood Facial Age Estimation through Ensemble Learning
Felix Anda (University College Dublin, Ireland), David Lillis (University College Dublin, Ireland), Aikaterini Kanta (University College Dublin, Ireland), Brett Becker (University College Dublin, Ireland), Elias Bou-Harb (Cyber Threat Intelligence Lab, Florida Atlantic University, United States), Nhien An Le Khac (University College Dublin, Ireland) and Mark Scanlon (University College Dublin, Ireland)

SSE 2019 Program

SSE I - Secure Software Development

A58_Learning Software Security in Context: An Evaluation in Open Source Software Development Environment
Shao-Fang Wen (Norwegian University of Science and Technology, Norway) and Basel Katt (Norwegian University of Science and Technology, Norway)

A59_The Security Intention Meeting Series as a way to increase visibility of software security decisions in agile development projects
Inger Anne Tøndel (Norwegian University of Science and Technology, Norway), Daniela S. Cruzes (SINTEF Digital, Norway), Martin Gilje Jaatun (SINTEF Digital, Norway) and Kalle Rindell (SINTEF Digital, Norway)

SSE II - Managing security on applications

A60_Managing Security in Software Or: How I Learned to Stop Worrying and Manage the Security Technical Debt
Kalle Rindell (SINTEF Digital, Norway), Martin Gilje Jaatun (SINTEF Digital, Norway) and Karin Bernsmed (SINTEF Digital, Norway)

A61_Applying Security Testing Techniques to Automotive Engineering
Irdin Pekaric (University of Innsbruck, Austria), Clemens Sauerwein (University of Innsbruck, Austria) and Michael Felderer (University of Innsbruck, Austria)

A62_Model Driven Security in a Mobile Banking Application Context
Serafettin Senturk (Gebze Technical University, Turkey), Hasan Yasar (Software Engineering Institute, Carnegie Mellon University, United States) and Ibrahim Sogukpinar (Gebze Technical University, Turkey)

CUING 2019 Program

CUING I – Keynote Session

CUING II

A63_Protocol-independent Detection of `Messaging Ordering' Network Covert Channels
Steffen Wendzel (Worms University of Applied Sciences and Fraunhofer FKIE, Germany)

A64_Introducing Dead Drops to Network Steganography using ARP-Caches and SNMP-Walks
Tobias Schmidbauer (University of Hagen, Germany), Steffen Wendzel (Worms University of Applied Sciences and Fraunhofer FKIE, Germany), Aleksandra Mileva (University Goce Delcev, Macedonia) and Wojciech Mazurczyk (Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications, Poland)

A65_Fine-tuning of Distributed Network Covert Channels Parameters and Their Impact on Undetectability
Krzysztof Cabaj (Warsaw University of Technology, Poland), Wojciech Mazurczyk (Warsaw University of Technology, Poland), Piotr Nowakowski (Warsaw University of Technology, Poland) and Piotr Żórawski (Warsaw University of Technology, Poland)

CUING III

A66_Detection and Analysis of Tor Onion Services
Martin Steinebach (Fraunhofer, Germany), Marcel Schäfer (Fraunhofer CESE, United States) and York Yannikos (Fraunhofer, Germany)

A67_Productivity and Patterns of Activity in Bug Bounty Programs: Analysis of HackerOne and Google Vulnerability Research
Donatello Luna (Tribunale di Busto Arsizio, Italy), Luca Allodi (Eindhoven University of Technology, Netherlands) and Marco Cremonini (University of Milan, Italy)

A68_SocialTruth Project Approach to Online Disinformation (Fake News) Detection and Mitigation
Michal Choras (UTP Bydgoszcz, Poland), Marek Pawlicki (Uniwersytet Technologiczno-Przyrodniczy, Poland) and Rafal Kozik (Institute of Telecommunications, UTP Bydgoszcz, Poland)

CUING IV

A69_Towards Reversible Storage Network Covert Channels
Wojciech Mazurczyk (Warsaw University of Technology, Poland), Przemysław Szary (Warsaw University of Technology, Poland), Steffen Wendzel (Worms University of Applied Sciences and Fraunhofer FKIE, Germany) and Luca Caviglione (CNR – IMATI, Italy)

A70_Privacy and Robust Hashes
Martin Steinebach (Fraunhofer, Germany), Sebastian Lutz (Fraunhofer, Germany) and Huajian Liu (Fraunhofer, Germany)

IoT-SECFOR 2019 Program

IoT-SECFOR I

A71_Securing the Device Drivers of Your Embedded Systems: Framework and Prototype
Zhuohua Li (The Chinese University of Hong Kong, Hong Kong), Jincheng Wang (The Chinese University of Hong Kong, Hong Kong), Mingshen Sun (Baidu X-Lab, United States) and John C.S. Lui (The Chinese University of Hong Kong, Hong Kong)

A72_IoT-HarPSecA: A Framework for Facilitating the Design and Development of Secure IoT Devices
Musa Samaila (Universidade da Beira Interior and Instituto de Telecomunicações, Covilhã, Portugal), Moser José (Universidade da Beira Interior and Instituto de Telecomunicações, Covilhã, Portugal), João Bernardo Sequeiros (Universidade da Beira Interior and Instituto de Telecomunicações, Covilhã, Portugal), Mario Freire (Universidade da Beira Interior and Instituto de Telecomunicações, Covilhã, Portugal) and Pedro Inácio (Universidade da Beira Interior and Instituto de Telecomunicações, Covilhã, Portugal)

IoT-SECFOR II

A73_Privacy-Enhancing Fall Detection from Remote Sensor Data Using Multi-Party Computation
Pradip Mainali (OneSpan, Belgium) and Carlton Shepherd (OneSpan, United Kingdom)

A74_Energy Attack in LoRaWAN: Experimental Validation
Konstantin Mikhaylov (University of Oulu, Finland), Radek Fujdiak (Brno University of Technology, Czechia), Miroslav Voznak (Technical University of Ostrava, Czechia), Ari Pouttu (University of Oulu, Finland) and Petr Mlynek (Brno University of Technology, Czechia)

A75_A Secure Publish/Subscribe Protocol for Internet of Things
Lukas Malina (Brno University of Technology, Czechia), Gautam Srivastava (Brandon University, Canada), Petr Dzurenda (Brno University of Technology, Czechia) and Jan Hajny (Brno University of Technology, Czechia)

IWSECC 2019 Program

IWSECC I

A76_Leveraging Kernel Security Mechanisms to Improve Container Security: a Survey
Maxime Bélair (Orange Labs, France), Sylvie Laniepce (Orange Labs, France) and Jean-Marc Menaud (IMT Atlantique, INRIA, LS2N, France)

A77_A Misuse Pattern for Compromising VMs via Virtual Machine Escape in NFV
Abdulrahman Alnaim (Florida Atlantic University, United States), Ahmed Alwakeel (Florida Atlantic University, United States) and Eduardo B. Fernandez (Florida Atlantic University, United States)

IWSECC II

A78_Preserving context security in AWS IoT Core
Luca Calderoni (University of Bologna, Italy)

A79_DTE Access Control Model for Integrated ICS Systems
Khaoula Es-Salhi (IMT atlantique -LabSTICC, France), David Espes (Université de Bretagne Occidentale (UBO), France) and Nora Cuppens (IMT atlantique -LabSTICC, France)

WCTI 2019 Program

WCTI I

A80_Zero Residual Attacks on Industrial Control Systems and Stateful Countermeasures
Hamid Reza Ghaeini (Singapore University of Technology and Design, Singapore), Nils Ole Tippenhauer (CISPA, Germany) and Jianying Zhou (Singapore University of Technology and Design, Singapore)

CyberTIM 2019 Program

CyberTIM I – Keynote Session

CyberTIM II - Threat prediction, detection and mitigation

A81_AIDA Framework: Real-Time Correlation and Prediction of Intrusion Detection Alerts,
Martin Husák (Masaryk University, Czechia) and Jaroslav Kašpar (Masaryk University, Czechia)

A82_Automated Pattern Inference Based on Repeatedly Observed Malware Artifacts,
Christian Doll (Fraunhofer, Germany), Arnold Sykosch (University of Bonn, Fraunhofer FKIE, Germany), Marc Ohm (University of Bonn, Germany) and Michael Meier (University of Bonn, Fraunhofer FKIE, Germany)

A83_A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources,
Thomas Schaberreiter (University of Vienna, Austria), Veronika Kupfersberger (University of Vienna, Austria), Konstantinos Rantos (Technological Educational Institute of Eastern Macedonia and Thrace, Greece), Arnolnt Spyros (Innovative Secure Technologies, Greece) , Alexandros Papanikolaou (Innovative Secure Technologies, Greece), Christos Ilioudis (Alexander Technological Educational Institute of Thessaloniki, Greece) and Gerald Quirchmayr (University of Vienna, Austria)

CyberTIM III - Threat Intelligence Sharing

A84_NERD: Network Entity Reputation Database,
Václav Bartoš (CESNET, Czechia)

A85_Cyber Threat Information Sharing: Perceived Benefits and Barriers,
Adam Zibak (University of Oxford, United Kingdom) and Andrew Simpson (University of Oxford, United Kingdom)

A86_Automated Cyber Threat Sensing and Responding: Integrating Threat Intelligence into Security-Policy-Controlled Systems,
Peter Amthor (Technische Universität Ilmenau, Germany), Daniel Fischer (Technische Universität Ilmenau, Germany), Winfried Kühnhauser (Technische Universität Ilmenau, Germany) and Dirk Stelzer (Technische Universität Ilmenau, Germany)

BASS 2019 Program

BASS I – Privacy, Authentication, and Access Control

A87_Privacy-Enhancing Context Authentication from Location-Sensitive Data
Pradip Mainali (OneSpan, Belgium), Carlton Shepherd (OneSpan, United Kingdom), and Fabien A. P. Petitcolas (OneSpan, Belgium),

A88_Semantic Mediation for A Posteriori Log Analysis
Farah Dernaika (IMT Atlantique, France), Nora Cuppens-Boulahia (IMT Atlantique, France), Frédéric Cuppens (IMT Atlantique, France) and Olivier Raynaud (LIMOS, France)

A89_Alexa's Voice Recording Behavior: A Survey of User Understanding and Awareness
Yousra Javed (Illinois State University, United States), Shashank Sethi (Illinois State University, United States) and Akshay Jadoun (Illinois State University, United States)

BASS II - Communication networks

A90_Adversarial Communication Networks Modeling for Intrusion Detection Strengthened against Mimicry
Jorge Maestre Vidal (Universidad Complutense de Madrid, Spain) and Marco Antonio Sotelo Monge (Universidad Complutense de Madrid, Spain)

IWSMR 2019 Program

IWSMR I

A91_Analysis of User Evaluations in Security Research
Peter Hamm (Goethe University Frankfurt, Germany), David Harborth (Goethe University Frankfurt, Germany) and Sebastian Pape (Goethe University Frankfurt, Germany)

A92_The power of interpretation: Qualitative methods in cybersecurity research
Damjan Fujs (University of Maribor, Slovenia), Anže Mihelič (University of Maribor, Slovenia) and Simon Vrhovec (University of Maribor, Slovenia)

A93_Examining and Constructing Attacker Categorisations - an Experimental Typology for Digital Banking
Moeckel Caroline (Royal Holloway, University of London, United Kingdom)

LPW 2019 Program

LPW I

A94_eBook Readers, Location Surveillance and the Threat to Freedom of Association
Stephen Wicker (Cornell University, United States)

LPW II

A95_Securing V2X Communications for the Future - Can PKI Systems offer the answer?
Thanassis Giannetsos (Technical University of Denmark, Denmark) and Ioannis Krontiris (European Research Center, Huawei Technologies, Germany)

A96_Location Tracking Using Smartphone Accelerometer and Magnetometer Traces
Khuong An Nguyen (Department of Computer Science, Royal Holloway, University of London, United Kingdom), Raja Naeem Akram (ISG-Smart Card Centre, Royal Holloway, University of London, United Kingdom), Konstantinos Markantonakis (ISG-Smart Card Centre, Royal Holloway, University of London, United Kingdom), Zhiyuan Luo (Royal Holloway, University of London, United Kingdom) and Chris Watkins (Royal Holloway, University of London, United Kingdom

LPW III

A97_A Location Privacy Analysis of Bluetooth Mesh
Matthias Caesar (Fraunhofer SIT, Fraunhofer Institute for Secure Information Technology SIT, Germany) and Jan Steffan (Fraunhofer SIT, Fraunhofer Institute for Secure Information Technology SIT, Germany)

A98_DEMISe: Interpretable Deep Extraction and Mutual Information Selection Techniques for IoT Intrusion Detection
Paul Yoo (Birkbeck, University of London, United Kingdom), Luke Parker (Ministry of Defence, United Kingdom), Taufiq Asyhari (Coverntry University, United Kingdom, Yoonchan Jhi (Samsung Electronics, South Korea), Kamal Taha (Khalifa University, United Arab Emirates) and Lounis Chermak (Cranfield University, United Kingdom)

WISI 2019 Program

WISI I

A99_Using Temporal and Topological Features for Intrusion Detection in Operational Networks
Simon Duque Anton (Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Germany), Daniel Fraunholz (Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Germany) and Hans Dieter Schotten (Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Germany)

A100_Performance Evaluation of Elliptic-Curve Libraries on Automotive-Grade Microcontrollers
Lucian Popa (Politehnica University of Timisoara, Romania), Bogdan Groza (Politehnica University of Timisoara, Romania) and Pal-Stefan Murvay (Politehnica University of Timisoara, Romania)

WISI II

A101_Applicability of the IEC 62443 standard in Industry 4.0 / IIoT
Björn Leander (Mälardalen University & ABB, Sweden), Aida Causevic (Mälardalen University, Sweden) and Hans Hansson (Mälardalen University, Sweden)

A102_Requirements and Recommendations for IoT/IIoT Models to automate Security Assurance through Threat Modelling, Security Analysis and Penetration Testing
Ralph Ankele (JOANNEUM RESEARCH Forschungsgesellschaft mbH, Austria), Stefan Marksteiner (AVL List GmbH, Austria), Kai Nahrgang (JOANNEUM RESEARCH Forschungsgesellschaft mbH, Austria) and Heribert Vallant (JOANNEUM RESEARCH Forschungsgesellschaft mbH, Austria)

A103_Federated Identity Management and Interoperability for Heterogeneous Cloud Platform Ecosystems

Nirojan Selvanathan (Salzburg Research, Austria), Dileepa Jayakody (Salzburg Research, Austria) and Violeta Damjanovic-Behrendt (Salzburg Research, Austria)

5G-NS 2019 Program

5G-NS I

A104_6G Network Needs to Support Embedded Trust

Raimo Kantola (Aalto University, Finland)

A105_Framework for Anticipatory Self-Protective 5G Environments

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

5G-NS II

A106_Securing Ethernet-based Optical Fronthaul for 5G Network

Joo Yeon Cho (ADVA Optical Networking SE, Germany), Andrew Sergeev (ADVA Optical Networking Israel Ltd., Israel) and Jim Zou (ADVA Optical Networking SE, Germany

A107_Towards a Security Architecture for Hybrid WMNs

Markus Theil (Technische Universitaet Ilmenau, Germany), Martin Backhaus (Technische Universitaet Ilmenau, Germany), Michael Rossberg (Technische Universitaet Ilmenau, Germany) and Guenter Schaefer (Technische Universitaet Ilmenau, Germany)

A108_Sniffing Detection within the Network: Revisiting Existing and Proposing Novel Approaches

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