ARES Conference
International Conference on Availability, Reliability and Security

ARES 2018

13th International Conference on Availability, Reliability and Security

August 27 – August 30, 2018
Hamburg, Germany

ARES 2018
13th International Conference on Availability, Reliability and Security
August 27 - 30, 2018
University of Hamburg, Hamburg, Germany

Organized by….

SBA Research

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Table of Content

Welcome to ARES 2018

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

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

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

Hamburg calls itself the German gate to the world. With ARES the world is coming to Hamburg.
We would like to thank the University of Hamburg for hosting ARES 2018!

Enjoy ARES 2018 and Hamburg!

Sebastian Doerr
TU Delft, Netherlands

Mathias Fischer
Universität Hamburg, Germany

Sebastian Schrittwieser
FH St. Pölten, Austria

Dominik Herrmann
Otto-Friedrich-Universität Bamberg, Germany

Welcome to CD-MAKE 2018

The International Cross Domain Conference for Machine Learning & Knowledge Extraction CD-MAKE is a joint effort of IFIP TC 5, IFIP WG 8.4, IFIP WG 8.9 and IFIP WG 12.9 and is held in conjunction with the International Conference on Availability, Reliability and Security (ARES).

IFIP – the International Federation for Information Processing is the leading multi-national, non-governmental, apolitical organization in Information & Communications Technologies and Computer Sciences, is recognized by the United Nations (UN) and was established in the year 1960 under the auspices of the UNESCO as an outcome of the first World Computer Congress held in Paris in 1959.

IFIP brings together more than 3500 scientists without boundaries form both academia and industry, organized in more than 100 Working Groups (WG) and 13 Technical Committees (TC).

CD stands for Cross-Domain and means the integration and appraisal of different fields and application domains (e.g. Health, Industry 4.0, etc.) to provide an atmosphere to foster different perspectives and opinions. The conference is dedicated to offer an international platform for novel ideas and a fresh look on the methodologies to put crazy ideas into Business for the benefit of the human. Serendipity is a desired effect, and shall cross-fertilize methodologies and transfer of algorithmic developments.

MAKE stands for MAchine Learning & Knowledge Extraction. Machine learning studies algorithms which can learn from data to gain knowledge from experience and to make decisions and predictions. A grand goal is in understanding intelligence for the design and development of algorithms that work autonomously (ideally without a human-in-the-loop) and can improve their learning behaviour over time. The challenge is to discover relevant structural and/or temporal patterns ("knowledge") in data, which is often hidden in arbitrarily high dimensional spaces, which is simply not accessible to humans. Machine learning as a branch of Artificial Intelligence currently undergoes kind of Cambrian explosion and is the fastest growing field in computer science today. There are many application domains, e.g., smart health, smart factory (Industry 4.0), etc. with many use cases from our daily life, e.g., recommender systems, speech recognition, autonomous driving, etc. The grand challenges are in sense making, in context understanding, and in decision making under uncertainty. Our real-world is full of uncertainties and probabilistic inference enormously influenced Artificial Intelligence generally and statistical learning specifically. The inverse probability allows to infer unknowns, to learn from data and to make predictions to support decision making. Whether in social networks, recommender systems, health or Industry 4.0 applications, the increasingly complex data sets require efficient, useful and useable solutions for knowledge discovery and knowledge extraction.

To acknowledge here all those who contributed to the efforts and stimulating discussions would be impossible. Many people contributed to the development of this Volume, either directly or indirectly, so it would be sheer impossible to list all of them. We herewith thank all colleagues and friends for all their positive and supportive encouragement. Last but not least, we thank the Springer management team and the Springer production team for their smooth support.

Thank you to all! Let's make it!

Andreas Holzinger, Peter Kieseberg, Edgar Weippl, A Min Tjoa
CD-MAKE 2018 Chairpersons

Welcome to the ARES EU Projects Symposium 2018

The ARES EU Projects Symposium is held for the fourth time in conjunction with the ARES Conference.
The goal is to disseminate the results of EU research projects, meet potential project partners and exchange ideas within the scientific community.

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

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

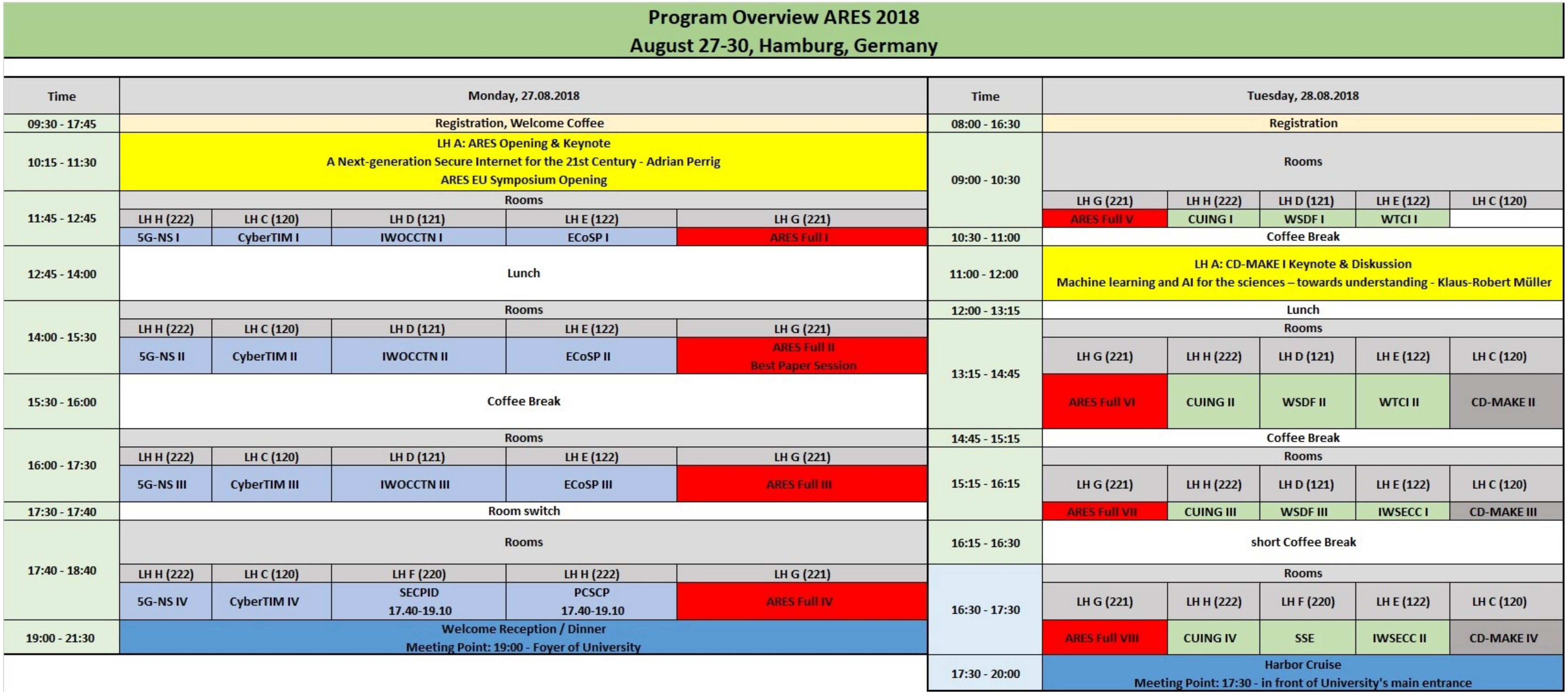
We would like to thank the workshop organizers for their great efforts and hard work in proposing the workshop, selecting the papers, the interesting programs and for the arrangements of the workshops during the conference days.

We hope you enjoy the ARES EU Projects Symposium!

This year the following projects will be represented:

DPSP
CLUSTER
Data Protection, Security and Privacy in cloud.
prisma cloud
CREDENTIAL
LIGHTest
ANASTACIA
Aries
YAKSHA
SAINT
CYBECO
FORTIKA
CIPSEC
SPECIAL
CS-AWARE
CYBERSECURITY
REDALERT

Program Overview



Program Overview ARES 2018
August 27-30, Hamburg, Germany

Time	Monday, 27.08.2018				
09:30 - 17:45	Registration, Welcome Coffee				
10:15 - 11:30	LH A: ARES Opening & Keynote A Next-generation Secure Internet for the 21st Century - Adrian Perrig ARES EU Symposium Opening				
11:45 - 12:45	Rooms				
	LH H (222)	LH C (120)	LH D (121)	LH E (122)	LH G (221)
	5G-NS I	CyberTIM I	IWOCCTN I	ECoSP I	ARES Full I
12:45 - 14:00	Lunch				
14:00 - 15:30	Rooms				
	LH H (222)	LH C (120)	LH D (121)	LH E (122)	LH G (221)
	5G-NS II	CyberTIM II	IWOCCTN II	ECoSP II	ARES Full II Best Paper Session
15:30 - 16:00	Coffee Break				
16:00 - 17:30	Rooms				
	LH H (222)	LH C (120)	LH D (121)	LH E (122)	LH G (221)
	5G-NS III	CyberTIM III	IWOCCTN III	ECoSP III	ARES Full III
17:30 - 17:40	Room switch				
17:40 - 18:40	Rooms				
	LH H (222)	LH C (120)	LH F (220)	LH H (222)	LH G (221)
	5G-NS IV	CyberTIM IV	SECPID 17.40-19.10	PCSCP 17.40-19.10	ARES Full IV
19:00 - 21:30	Welcome Reception / Dinner Meeting Point: 19:00 - Foyer of University				

Time	Tuesday, 28.08.2018				
08:00 - 16:30	Registration				
09:00 - 10:30	Rooms				
	LH G (221)	LH H (222)	LH D (121)	LH E (122)	LH C (120)
	ARES Full V	CUING I	WSDF I	WTCI I	
10:30 - 11:00	Coffee Break				
11:00 - 12:00	LH A: CD-MAKE I Keynote & Diskussion Machine learning and AI for the sciences – towards understanding - Klaus-Robert Müller				
12:00 - 13:15	Lunch				
13:15 - 14:45	Rooms				
	LH G (221)	LH H (222)	LH D (121)	LH E (122)	LH C (120)
	ARES Full VI	CUING II	WSDF II	WTCI II	CD-MAKE II
14:45 - 15:15	Coffee Break				
15:15 - 16:15	Rooms				
	LH G (221)	LH H (222)	LH D (121)	LH E (122)	LH C (120)
	ARES Full VII	CUING III	WSDF III	IWSECC I	CD-MAKE III
16:15 - 16:30	short Coffee Break				
16:30 - 17:30	Rooms				
	LH G (221)	LH H (222)	LH F (220)	LH E (122)	LH C (120)
	ARES Full VIII	CUING IV	SSE	IWSECC II	CD-MAKE IV
17:30 - 20:00	Harbor Cruise Meeting Point: 17:30 - in front of University's main entrance				

Time	Wednesday, 29.08.2018					ICS-CSR +only for registered participants
08:30 - 16:00	Registration					08:30 - 09:15 Registration
09:30 - 10:30	LH A: Keynote Session ARES Innovations in permutation-based crypto - Joan Daemen					LH G (221) 09:15 - 09:30 Welcome 09:30 - 10:30 Keynote
10:30 - 11:00	Coffee Break					
11:00 - 12:30	Rooms					
	LH D (121)	LH H (222)	LH E (122)	LH F (220)	LH C (120)	LH G (221)
	ARES Full IX	IoT-SECFOR I	IWCC I	IWSMA I	CD-MAKE V	11:15 - 12:15 Paper 1 & 2
12:30 - 14:00	Lunch					12:15-13:30 Lunch
14:00 - 15:30	Rooms					
	LH D (121)	LH H (222)	LH E (122)	LH F (220)	LH C (120)	LH G (221)
	ARES Short I	IoT-SECFOR II	IWCC II	IWSMA II	MAKE-TEXT	13:30 - 15:00 Paper 3, 4 & 5
15:30 - 16:00	Coffe Break					15:00 - 15:45 Coffee Break
16:00 - 17:30	Rooms					
	LH D (121)	LH H (222)	LH E (122)	LH F (220)	LH C (120)	LH G (221)
	ARES Full X	IoT-SECFOR III	SPEBD		MAKE-Smart Factory	15:45 - 17:00 Paper 6 & 7, Day Closing
17:30 - 23:00	Conference Dinner Meeting Point: 17:30 - in front of University's main entrance					

Time	Thursday, 30.08.2018					ICS-CSR +only for registered participants
08:30 - 14:00	Registration					
09:30 - 11:00	Rooms					
	LH D (121)	LH H (222)	LH E (122)	LH F (220)	LH C (120)	LH G (221)
	ARES Short II	FARES I	SAW I	iPAT I220	MAKE-Explainable AI I	09:00 - 10:00 Morning Coffee 10:00 - 11:00 Industrial Talk
11:00-11:30	Coffee Break					
11:30-13:00	Rooms					
	LH D (121)	LH H (222)	LH E (122)	LH F (220)	LH C (120)	LH G (221)
	ARES Short III	FARES II	SAW II	iPAT II	MAKE-Explainable AI II	Paper 8, 9 & 10
13:00-14:00	Lunch				Room 221 Ost MAKE Journal Editorial Board Meeting	Lunch
14:00-15:30	Rooms					
	LH D (121)				LH C (120)	LH G (221)
	ARES Short IV				MAKE-Topology	14:00 - 15:45 Paper 11, 12 & 13; Conference Closing
15:45 - 16:00						short Coffee Break
						Rooms
						LH G (221)
						16:00 - 17:30 Limes-Cyber-Game

Detailed Program

Time	Monday, August 27th, 2018				
	Track 1: ARES EU Projects Symposium **Lecture Hall F (220)**	**Track 2: ARES EU Projects Symposium** **Lecture Hall C (120)**	**Track 3: ARES EU Projects Symposium** **Lecture Hall D (121)**	**Track 4: ARES EU Projects Symposium** **Lecture Hall E (122)**	**Track 5: ARES** **Lecture Hall G (221)**
09:30 – 17:45	**Registration** **Foyer**				
10:30 – 11:30	**ARES & ARES EU Projects Symposium Opening** Welcome: Hannes Federrath, Universität Hamburg, Germany Mathias Fischer, Universität Hamburg, Germany & Christian Doerr, TU Delft, Germany Session Chair: Edgar Weippl, SBA Research, Austria **Keynote: A Next-generation Secure Internet for the 21st Century** *Adrian Perrig,* *ETH Zürich* Lecture Hall A				
	Abstract: The Internet has been successful beyond even the most optimistic expectations. It permeates and intertwines with almost all aspects of our society and economy. The success of the Internet has created a dependency on communication as many of the processes underpinning the foundations of modern society would grind to a halt should communication become unavailable. However, much to our dismay, the current state of safety and availability of the Internet is far from commensurate given its importance. Although we cannot conclusively determine what the impact of a 1-day, or 1-week outage of Internet connectivity on our society would be, anecdotal evidence indicates that even short outages have a profound negative impact on society, businesses, and government. Unfortunately, the Internet has not been designed for high availability in the face of malicious actions by adversaries. Recent patches to improve Internet security and availability have been constrained by the current Internet architecture, business models, and legal aspects. Moreover, there are fundamental design decisions of the current Internet that inherently complicate secure operation. Given the diverse nature of constituents in today’s Internet, another important challenge is how to scale authentication of entities (e.g., AS ownership for routing, name servers for DNS, or domains for TLS) to a global environment. Currently prevalent PKI models (monopoly and oligarchy) do not scale globally because mutually distrusting entities cannot agree on a single trust root, and because everyday users cannot evaluate the trustworthiness of each of the many root CAs in their browsers. To address these issues, we propose SCION, a next-generation Internet architecture that is secure, available, and offers privacy by design; that provides incentives for a transition to the new architecture; and that considers economic and policy issues at the design stage. We have implemented SCION and deployed it in the production networks of several ISPs.				

	5G-NS I **Welcome & Keynote** **Session Chair: Wojciech Mazurczyk & Krzysztof Cabaj, Warsaw University of Technology, Poland and Pascal Bisson, Thales, France** **Lecture Hall F (220)**	**CyberTIM I** **Opening** **Session Chair: Dr. Sheikh Mahbub Habib, Continental AG, Germany** **Lecture Hall C (120)**	**IWOCCTN I** **Session Chair: Andrea Tundis, Technische Universität Darmstadt (TUDA), Germany & Matteo Bonfanti, ETH Center for Security Studies, Switzerland** **Lecture Hall D(121)**	**ECoSP I** **Session Chair: tba** **Lecture Hall E (122)**	**ARES Full I** **Machine Learning** **Session Chair: Sebastian Schrittwieser, FH St. Pölten, Austria** **Lecture Hall G (221)**
11:45 – 12:45	**Welcome Message** Keynote: Peter Schneider, *(Nokia Bell Lab, Germany)*	**Keynote I: Cyber Security Threat Intelligence: Challenges and Research Opportunities"** Prof. Dr. Kim-Kwang Raymond Choo (*The University of Texas at San Antonio, USA)*	**Introductory talk: An Overview on the H2020 TAKEDOWN Project** Florian Huber *(SYNYO GmbH, Austria)*	**ANASTACIA - Advanced Networked Agents for Security and Trust Assessment in CPS / iOT Architectures** Jorge Bernal, (*University of Murcia Spain)* **SAINT - Cyber Threat Risk and Cost Assessment: Tangible and Intangible Factors** Edgardo Montes de Oca, (*Montimage, France)* **YAKSHA - Automating Honeypot Deployment and Malware Analytics** Nikolaos Mantas, (*University of Piraeus, Greece;)* **FORTIKA - The FORTIKA Paradigm: Cyber Security Accelerator for trusted SMEs IT Ecosystem** Evangelos Markakis, (*TEI Crete, Greece)*	**Modular Convolutional Neural Network for Discriminating between Computer-Generated Images and Photographic Images** Hong-Huy Nguyen,Ngoc-Dung Tieu-Thi *(SOKENDAI (The Graduate University for Advanced Studies), Japan)*, Hoang-Quoc Nguyen-Son *(National Institute of Informatics, Japan)*, Vincent Nozick *(Japanese-French Laboratory for Informatics (JFLI) (UMI 3527), Japan)*, Junichi Yamagishi and Isao Echizen *National Institute of Informatics, Japan)* **FALKE-MC: A Neural Network Based Approach to Locate Cryptographic Functions in Machine Code** Alexander Aigner *(University of Applied Sciences Upper Austria, Austria)*
12:45 – 14:00	**Lunch**				

	5G-NS II Session Chair: Pascal Bisson, Thales, France Lecture Hall F (220)	CyberTIM II Attack Detection and Mitigation Session Chair: Dr. Emmanouil Vasilomanolakis, TU Darmstadt, Germany Lecture Hall C (120)	IWOCCTN II Cyber Organized Crime and Terrorism Session Chair: Matteo Bonfanti, ETH Center for Security Studies Switzerland Lecture Hall D (121)	ECoSP II Session Chair: tba Lecture Hall E (122)	ARES Full II Best Paper Session Session Chair: Christian Doerr, TU Delft, Germany Lecture Hall G (221)
14:00 – 15:30	**To Trust or Not to Trust: Data Origin Authentication for Group Communication in 5G Networks** Robert Annessi, Joachim Fabini and Tanja Zseby *(Vienna University of Technology, Austria)* **Universal Trusted Execution Environments for Securing SDN/NFV Operations** Vincent Lefebvre (*tages sas, France)*, Gianni Santinelli (tages sas, Italy), Tilo MÜller *(FAU Erlangen-Nürnberg, Germany)* and Johannes Götzfried *(FAU Erlangen-Nürnberg, Germany)* **Enhancing NFV Orchestration with Security Policies** Christian Banse and Florian Wendland *(Fraunhofer, Germany)*	**Evaluation of Apache Spot's machine learning capabilities in an SDN/NFV enabled environment** Christos M. Mathas (*University of Peloponnese, Greece)*, Olga E. Segou, Georgios Xylouris (Orion Innovations PC, Greece), Dimitris Christinakis (*Orion Innovations PC, Greece)*, Michail -Alexandros Kourtis *(Institute of Informatics and Telecommunications National Centre for Scientific Research "Demokritos", Greece)*, Costas Vassilakis *(University of Peloponnese, Greece)* and Anastasios Kourtis *(Institute of Informatics and Telecommunications National Centre for Scientific Research "Demokritos", Greece)* **Towards an Automated Recognition System for Chat-based Social Engineering Attacks in Enterprise Environments** Nikolaos Tsinganos, George Sakellariou, Panagiotis Fouliras and Ioannis Mavridis *(University of Macedonia, Greece)*	**Conceptualizing the Digital TAKEDOWN Platforms for Supporting First-Line-Practitioners and Law Enforcement Agencies** Florian Huber, *(SYNYO GmbH, Austria)* **Cybercrime and Organized Crime** Václav Jirovský and Andrej Pastorek *(Czech Technical University, Czech Republic)* **The AWID and TAKEDOWN Prevention Approach. The Generation of a Holistic Good Practice Model for Prevention of Radicalization in Youth Work** Karin Rainer, Mario Springnagel and Diana Silvestru *(Agency for European Integration and Economic Development, Austria)*	**CYBECO - Supporting Cyber Insurance from a Behavioural Choice Perspective** Aitor Couce Vieira, (*ICMAT Spain)* **SISSDEN - Avoiding Cyber-Threat Detection Evasion Techniques** Edgardo Montes de Oca, (Montimage, France) **CIPSEC - Enhancing Critical Infrastructure Protection with Innovative SECurity Framework** Christian Schlehuber, (Deutsche Bahn AG, Germany) **CS-AWARE - Cybersecurity Situational Awareness and Information Sharing Solution** Juha Röning, (*OULU, Finland)*	**Secure Equality Testing Protocols in the Two-Party Setting** Majid Nateghizad *(Delft University of Technology, Netherlands)*, Thijs Veugen *(TNO, Netherlands)*, Zekeriya Erkin and Reginald L. Lagendijk (*Delft University of Technology, Netherlands)* **Android Authorship Attribution Through String Analysis** Vaibhavi Kalgutkar, Natalia Stakhanova, Paul Cook and Alina Matyukhina *(University of New Brunswick, Canada)* **Flashlight: A Novel Monitoring Path Identification Schema for Securing Cloud Services** Heng Zhang *(DEEDS Group, Department of Computer Science, TU Darmstadt, Germany)*, Ruben Trapero *(Atos Research & Innovation, Spain)*, Jesus Luna Garcia *(TU Darmstadt, Germany)* and Neeraj Suri *(TU Darmstadt, Germany)*

	Identity and Access Control for micro-services based 5G NFV platforms Daniel Guija and Muhammad Shuaib Siddiqui (*i2CAT, Spain*)	**Augmented DDoS Mitigation with Reputation Scores** Tomáš Jánský, Tomáš Čejka *(Faculty of Information Technology, CTU in Prague, Czech Republic),* Martin Žádník and Václav Bartoš *(CESNET a.l.e., Czech Republic)* **The Challenge of Detecting Sophisticated Attacks: Insights from SOC Analysts** Olusola Akinrolabu, Ioannis Agrafiotis and Arnau Erola *(University of Oxford, United Kingdom)*		**RED-Alert - Use of Social Media Forensics in the Early Detection of Terrorist Activities - European Project RED-Alert Approach** Syed Naqvi, (Birmingham City University, UK*)* **Truessec.eu - Privacy and Cybersecurity Trust-Enhancing Labels** Manel Medina, (*UPC, Spain)*	
15:30 – 16:00	**Coffee Break**				

	5G-NS III Session Chair: Wojciech Mazurczyk, Warsaw University of Technology, Poland Lecture Hall F (220)	CyberTIM III Threat Intelligence Sharing Session Chair: Marcin Przybyszewski, ITTI, Poland Lecture Hall C (120)	IWOCCTN III Cyber Security Session Chair: Andrea Tundis, Technische Universität Darmstadt (TUDA), Germany Lecture Hall D (121)	ECoSP III Session Chair: tba Lecture Hall E (122)	ARES Full III Software Security Session Chair: Alexander Aigner, University of Applied Sciences Upper Austria, Austria Lecture Hall G (221)
16:00 – 17:30	**Towards a 5G Security Architecture: Articulating Software-Defined Security and Security as a Service** Gregory Blanc *(Institut Mines-Télécom, Télécom SudParis, France)*, Nizar Kheir *(Thales Group, France)*, Dhouha Ayed *(Thales Group, France)*, Vincent Lefebvre *(Tages SAS, France)*, Edgardo Montes de Oca *(Montimage, France)* and Pascal Bisson *(Thales Group, France)* **A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation** Marco Antonio Sotelo Monge, Jorge Maestre Vidal and Luis Javier García Villalba *(Universidad Complutense de Madrid, Spain)*	**Mission-Centric Risk Assessment to Improve Cyber Situational Awareness** Franklin Silva and Paul Jacob *(Athlone IT, Ireland)* **The Mouseworld, a Security Traffic Analysis Lab Based on NFV/SDN** Antonio Pastor *(Telefonica I+D, Spain)*, Alberto Mozo Velasco *(Universidad Politécnica de Madrid, Spain)*, Diego R. Lopez, Jesús Luis Folgueira *(Telefonica I+D, Spain)* and Georgios Gardikis (*Space Hellas S.A., Greece)* **Risks of Sharing Cyber Incident Information** Adham Albakri *(University of Kent, UK)*, Eerke Boiten (*De Montfort University, UK)* and Rogério de Lemos *(University of Kent, UK)*	**Challenges of Cryptocurrencies Forensics – A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals** Syed Naqvi *(Birmingham City University, UK)* **Enhancing Cyber-Security by Safeguarding Information Privacy: the European Union and the Implementation of the "Data Protection by Design" Approach** Matteo E. Bonfanti *(ETH Center for Security Studies, Switzerland)* **A Review of Network Vulnerabilities Scanning Tools: Types, Capabilities and Functioning** Andrea Tundis *(TU Darmstadt, Germany)*, Wojciech Mazurczyk *(Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications, Poland)* and Max Mühlhäuser *(TU Darmstadt, Germany)*	**ARIES - Architecture for a Reliable European Identity Ecosystem** Jorge Bernal, (University of Murcia, Spain) **LIGHTest - LIGHTest Automated Trust Verification** Jon Shamah, (*EEMEA, UK)* **CREDENTIAL - Design and Implementation of Privacy-Friendly Web-Based Authentication in CREDENTIAL** Krenn Stephan, Austrian Institute of Technology *(AIT)* **FutureTrust - FutureTrust Extending the eIDAS Reach** Jon Shamah, (*EEMEA, UK)* **SPECIAL - New Ways for Informed Consent and Transparency Under the GDPR with Technical Specifications** Harald Zwingelberg, (*ULD, Germany)* **LEPS**	**Discovering Software Vulnerabilities Using Data-flow Analysis and Machine Learning** Jorrit Kronjee, Arjen Hommersom and Harald Vranken *(Open University of the Netherlands, Netherlands)* **Speeding Up Bug Finding using Focused Fuzzing** Ulf Kargén and Nahid Shahmehri *(Linköping University, Sweden)* **HYDRA- Hypothesis Driven Repair Automation** Partha Pal, Brett Benyo, Shane Clark and Aaron Paulos *(Raytheon BBN, USA)*

	SDN-based Mitigation of Scanning Attacks for the 5G Internet of Radio Light System Krzysztof Cabaj, Marcin Gregorczyk, Wojciech Mazurczyk, Piotr Nowakowski and Piotr Żórawski *(Warsaw University of Technology, Poland)*	**Hunting Observable Objects for Indication of Compromise** *Arnold Sykosch, Michael Meier and Marc Ohm (University of Bonn, Germany)*			
17:30 – 17:40	**Room switch**				

	5G-NS IV **Session Chair:** **Krzysztof Cabaj,** **Warsaw University of Technology,** **Poland** **Lecture Hall F (220)**	**CyberTIM IV** **Session Chair:** **Dr. Sheikh Mahbub Habib,** **Continental AG,** **Germany** **Lecture Hall C (120)**	**SECPID** **Session Chair:** **Stephan Krenn,** **AIT Austrian Institute of Technology,** **Austria** **17:40-19:10** **Lecture Hall D (221)**	**PCSCP** **Session Chair:** **Stefan Schauer,** **AIT Austrian Institute of Technology,** **Austria** **17:30-19:10** **Lecture Hall H (222)**	**ARES Full IV - Network Security and Monitoring I** **Session Chair:** **Paul Smith,** **AIT Austrian Institute of Technology,** **Austria** **Lecture Hall G (221)**
17:40 **–** **18:40**	**Detecting Workload-based and Instantiation-based Economic Denial of Sustainability on 5G environments** Jorge Maestre Vidal, Marco Antonio Sotelo Monge and Luis Javier García Villalba *(Universidad Complutense de Madrid, Spain)* **Framework for Security Event Management in 5G** Iris Adam *(Nokia Bell Labs, Germany)* and Jing Ping *(Nokia Software, China)*	**Keynote II**: Prof. Dr. Hervé Debar *(Telecom SudParis, France)* **Reasoning About Alert Formats: a Comparative Study** **Closing of CyberTIM**	**Fingerprint Recognition on Mobile Devices: Widely Deployed, Rarely Understood** Farzaneh Karegar, John Sören Pettersson and Simone Fischer-Hübner *(Karlstad University, Sweden)* **Keys in the Clouds: Auditable Multi-Device Access to Cryptographic Credentials** Arseny Kurnikov, Andrew Paverd *(Aalto University, Finland)*, Mohammad Mannan *(Concordia University, Canada)* and N. Asokan *(Aalto University, Finland)* **Definitions for Plaintext-Existence Hiding in Cloud Storage** Colin Boyd, Gareth T. Davies, Kristian Gjøsteen *(Norwegian University of Science and Technology, Norway)*, Håvard Raddum *(Simula Research Laboratories, Norway)* and Mohsen Toorani *(University of Bergen, Norway)*	**An Overview of the SAURON Project** Stefan Schauer(*AIT Austrian Institute of Technology, Austria)* **An Event Correlation Engine for Cyber-Physical Infrastructures** Nicolas Museux, (Thales, France) **Threat Propagation for Identifying Cascading Effects** Sandra König, (*AIT Austrian Institute of Technology, Austria)* **SAURON Case Study of Port of Piraeus** Christos Douligeris, (*University of Piraeus, Greece)* **Legal Aspects of Situational Awareness under GDPR and the NIS Directive** Plixavra Vogiatzoglou, (*KU Leuven, Belgium)*	**A Framework for Monitoring Net Neutrality** Wilfried Mayer *(SBA Research, Austria)*, Thomas Schreiber *(TU Wien, Austria)* and Edgar Weippl *(SBA Research, Austria)* **The Other Side of the Coin: A Framework for Detecting and Analyzing Web-based Cryptocurrency Mining Campaigns** Julian Rauchberger, Sebastian Schrittwieser, Tobias Dam, Robert Luh, Damjan Buhov, Gerhard Pötzelsberger *(St. Pölten UAS, Austria)* and Hyoungshick Kim *(Sungkyunkwan University, South Korea)*

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

	Welcome Reception/Dinner
19:00 – 21:30	Get a taste of Hamburg´s cuisine and culture at this year´s ARES reception. Fish buns, local craft beer and the performance of a shanty-choir will get you in the mood for a great conference. Meeting point: 19:00 in the foyer of the University **Meeting point:** 19:00 in the foyer of the University 19:15: Opening, Anja Diek (chief officer in the Hamburg Ministry of Science, Research and Equalities) 19:30: Shanty Choir 20:00: DJane

Tuesday, August 28th, 2018

Time	Track 1: ARES Lecture Hall G (221)	Track 2: Workshops Lecture Hall H (222)	Track 3: Workshops Lecture Hall D (121)	Track 4: Workshops Lecture Hall E (122)	Track 5: CD-MAKE Lecture Hall C (120)
08:00 – 16:30	Registration Foyer				
09:00 – 10:30	ARES Full V - Cryptography Session Chair: Edgar Weippl, SBA Research, Austria Lecture Hall G (221)		CUING I - Introduction & Keynote Session Chair: Wojciech Mazurczyk, Warsaw University of Technology, Poland & Joerg Keller, FernUniversitaet in Hagen, Germany Lecture Hall H (222)	WSDF I Session Chair: Richard Overill, King's College London, UK Lecture Hall D (121)	WTCI I Session Chair: Christian Dörr, TU Delft, Netherlands Lecture Hall E (122)
	Finally Johnny Can Encrypt. But Does This Make Him Feel More Secure? Nina Gerber *(KIT, Germany)*, Verena Zimmermann, Birgit Henhapl, Sinem Emeröz *(TU Darmstadt, Germany)* and Melanie Volkamer *(KIT, Germany)* **An Efficient Cryptography-Based Access Control Using Inner-Product Proxy Re-Encryption Scheme** Masoomeh Sepehri, Maryam Sepehri *(University of Milan, Italy)*, Alberto Trombetta *(Università degli Studi dell'Insubria, Italy)* and Ernesto Damiani *(Khalifa University of Science and Technology, United Arab Emirates)* **Non-Interactive Key Exchange from Identity-Based Encryption** Olivier Blazy *(Université de Limoges, France)* and Céline Chevalier *(ENS, France)*		**Welcome Message** **Introductory Talk I: Criminal Use of Information Hiding Initiative – An Update** Wojciech Mazurczyk, *(Warsaw University of Technology)* **Introductory Talk II: CUING and CTI (Cyber Threat Intelligence)** Jart Armin (*Stichting CUlng Foundation, The Netherlands)* **Keynote: Europol's European Cybercrime Centre - a Networked Approach** Philipp Amann, (*Europol EC3, Netherlands)*	**Keynote: Structured Argumentation in Digital Forensic Practice: Opportunity or Burden?** Virginia N. L. Franqueira, (*University of Derby, UK)* **Digital Forensics in the Next Five Years** Laoise Luciano, Mateusz Topor, Ibrahim Baggili and Frank Breitinger *(University of New Haven, USA)*	**Data Model for Cyber Situation Awareness** Jana Komárková, Martin Husák, Martin Laštovička and Daniel Tovarňák *(Masaryk University, Czech Republic).* **Integrating Threat Intelligence to Enhance an Organization's Information Security Management** Mathias Gschwandtner *(Leopold-Franzens University Innsbruck, Austria)*, Lukas Demetz *(University of Applied Sciences Kufstein, Austria)*, Matthias Gander *(Leopold-Franzens University Innsbruck, Austria)* and Ronald Maier *(Department of Information Systems, Production and Logistics Management, Austria)* **MAL (the Meta Attack Language): A Language for Domain-Specific Probabilistic Threat Modeling and Attack Simulation** Pontus Johnson, Robert Lagerström and Mathias Ekstedt *(KTH Royal Institute of Technology, Sweden)*

10:30 – 11:00	**Coffee Break**
11:00 – 12:00	**CD-MAKE I** **Keynote & Discussion** Session Chair: Andreas Holzinger, Medical University Graz, Austria **Keynote: Machine Learning and AI for the Sciences – Towards Understanding** *Klaus-Robert Müller,* *Machine Learning Group TU Berlin, MPI for Informatics, Saarbrücken, and Korea University, Seoul* Lecture Hall A
	Abstract: In recent years, machine learning (ML) and artificial intelligence (AI) methods have begun to play a more and more enabling role in the sciences and in industry. In particular, the advent of large and/or complex data corpora has given rise to new technological challenges and possibilities. In his talk, Müller will touch upon the topic of ML applications in the sciences, in particular in neuroscience, medicine and physics. He will also discuss possibilities for extracting information from machine learning models to further our understanding by explaining nonlinear ML models. E.g. Machine Learning Models for Quantum Chemistry can, by applying interpretable ML, contribute to furthering chemical understanding. Finally, Müller will briefly outline perspectives and limitations.
12:00 – 13:15	**Lunch**

	ARES Full VI Anomaly Detection Session Chair: Csilla Farkas, University of South Carolina, USA Lecture Hall G (221)	CUING II Session Chair: Angelo Consoli, Scuola Universitaria Professionale Della Svizzera Italiana, Switzerland Lecture Hall H (222)	WSDF II Session Chair: Richard Overill, King's College London, UK Lecture Hall D (121)	WTCI II Session Chair: Christian Dörr, TU Delft, Netherlands Lecture Hall E (122)	CD-MAKE II Session Chair: tba Lecture Hall C (120)
13:15 – 14:45	**Behavioural Comparison of Systems for Anomaly Detection** Martin Pirker, Patrick Kochberger and Stefan Schwandter *(St. Pölten UAS, Austria)* **Converting Unstructured System Logs into Structured Event List for Anomaly Detection** Zongze Li, Song Fu, Matthew Davidson *(University of north Texas, United States)*, Sean Blanchard and Michael Lang *(Los Alamos National Laboratory, United States)* **Stealthy Attacks on Smart Grid PMU State Estimation** Sarita Paudel *(AIT Austrian Institute of Technology, Austria)*, Tanja Zseby *(Vienna University of Technology, Austria)* and Paul Smith (*AIT Austrian Institute of Technology, Austria)*	**Channel Steganalysis** Martin Steinebach *(Fraunhofer, Germany)* **Towards Deriving Insights into Data Hiding Methods Using Pattern-based Approach** Wojciech Mazurczyk *(Warsaw University of Technology, Poland)*, Steffen Wendzel *(Worms University of Applied Sciences and Fraunhofer FKIE, Germany)* and Krzysztof Cabaj *(Warsaw University of Technology, Poland)* **Steganography by Synthesis - Can Commonplace Image Manipulations like Face Morphing Create Plausible Steganographic Channels?** Christian Kraetzer and Jana Dittmann *(Dept. of Computer Science, Otto-von-Guericke University Magdeburg, Germany)*	**Forensic APFS File Recovery** Jonas Plum *(Siemens AG, Germany)* and Andreas Dewald *(ERNW Research GmbH, Germany)* **Volatile Memory Forensics Acquisition Efficacy: A Comparative Study Towards Analysing FirmwareBased Rootkits** Jacob Taylor, Benjamin Turnbull and Gideon Creech *(The University of New South Wales, Australia)* **I Know What You Did Last Summer: Your Smart Home Internet of Things and Your iPhone Forensically Ratting You Out** Gokila Dorai *(Florida State University, United States)*, Shiva Houshmand *(Southern Illinois University, United States)* and Ibrahim Baggili *(University of New Haven, United States)*	**Keynote** Kas Clark *(National Cyber Security Center, Netherlands)* **CRUSOE: Data Model for Cyber Situation Awareness** **Jana Komárková, Martin Husák, Martin** Laštovička and Daniel Tovarňák *(Masaryk University, Czech Republic)* **Integrating Threat Intelligence to Enhance an Organization's Information Security Management**Mathias Gschwandtner *(Leopold-Franzens University Innsbruck, Austria)*, Lukas Demetz *(University of Applied Sciences Kufstein, Austria)*, Matthias Gander *(Leopold-Franzens University Innsbruck, Austria)* and Ronald Maier *(Department of Information Systems, Production and Logistics Management, Austria)* **MAL (the Meta Attack Language): A Language for Domain-Specific Probabilistic Threat Modeling and Attack Simulation** Pontus Johnson, Robert Lagerström and Mathias Ekstedt *(KTH Royal Institute of Technology, Sweden)*	**A Modified Particle Swarm Optimization Algorithm for Community Detection in Complex Networks** Alireza Abdollahpouri, Shadi *Rahimi (University of Kurdistan, Iran)*, Shahnaz Mohammadi Majd *(Islamic Azad University, Sanandaj, Iran)* and Chiman Salavati *(University of Kurdistan, Iran)* **Mouse Tracking Measures and Movement Patterns with Application for Online Surveys** Catia Cepeda, Joao Rodrigues Maria Camila Dias, Diogo Oliveira *(Faculdade de Ciências e Tecnologia, Universidade Nova de Lisboa, Caparica, Portugal)*, Dina Rindlisbacher, Marcus Cheetham (*University Hospital Zurich, Zurich, Switzerland)* and Hugo Gamboa *(Faculdade de Ciências e Tecnologia, Universidade Nova de Lisboa, Caparica, Portugal)*

14:45 – 15:15	Coffee Break				
15:15 – 16:15	**ARES Full VII** **Security and the User** **Session Chair:** **Melanie Volkamer,** **Karlsruhe Institute of Technology** **Germany** **Lecture Hall G (221)**	**CUING III** **Session Chair:** **Joerg Keller,** **FernUniversitaet in Hagen,** **Germany** **Lecture Hall H (222)**	**WSDF III** **Session Chair:** **Richard Overill,** **King's College London,** **UK** **Lecture Hall D (121)**	**IWSECC I** **Security Implementations for Cloud Computing** **Session Chair:** **Dr. Antonio Muñoz,** **University of Málaga,** **Spain** **Lecture Hall E (122)**	**CD-MAKE III** **Session Chair:** **Svetla Boytcheva,** **Bulgarian Academy of Sciences,** **Bulgaria** **Lecture Hall C (120)**
	Protecting Patients' Data: An Efficient Method for Health Data Privacy Mark Daniels, John Rose and Csilla Farkas *(University of South Carolina, USA)* **Influence Factors on the Quality of User Experience in OS Reliability: A Qualitative Experimental Study** Daniela Yabe, Caio Augusto Rodrigues Dos Santos,Lucas Miranda and Rivalino Matias *(Federal University of Uberlandia, Brazil)*	**Towards Distributed Network Covert Channels Detection Using Data Mining-based Approach** Krzysztof Cabaj, Wojciech Mazurczyk, Piotr Nowakowski and Piotr Żórawski *(Warsaw University of Technology, Poland)* **Get Me Cited, Scotty! Analysis of Academic Publications in Covert Channel Research** Steffen Wendzel *(Fraunhofer FKIE / Worms University of Applied Sciences, Germany)*	**Breaking Down Violence: A Deep-learning Strategy to Model and Classify Violence in Videos** Bruno Malveira Peixoto, Sandra Avila, Zanoni Dias and Anderson Rocha *(Universidade Estadual de Campinas – Unicamp, Brazil)* **Digitally Signed and Permission Restricted PDF Files: a Case Study on Digital Forensics** Patricio Domingues and Miguel Frade *(Instituto Politécnico de Leiria, Portugal)* **Investigating the Use of Online Open Source Information as Evidence in European Courts** Yi-Ching Liao *(Noroff University College, Norway)*	**A Process Framework for Stakeholder-specific Visualization of Security Metrics** Tanja Hanauer *(Leibniz-Rechenzentrum der BAdW, Germany),* Wolfgang Hommel *(Universität der Bundeswehr München, Germany),* Stefan Metzger *(Leibniz-Rechenzentrum der BAdW, Germany*) and Daniela Pöhn *(Fraunhofer-Institut für Angewandte und Integrierte Sicherheit, Germany*) **Security Wrapper Orchestration in Cloud** Aapo Kalliola *(Nokia Bell Labs, Finland),* Shankar Lal *(Aalto University,Finland),* Kimmo Ahola (*VTT Technical Research Centre of Finland, Finland),* Ian Oliver *(Nokia Bell Labs, Finland),* Yoan Miche *(Nokia Bell Labs, Finland)* and Tuomas Aura (*Aalto University, Finland)* **A Simulation Tool for Cascading Effects in Interdependent Critical Infrastructures** Stefan Rass, Thomas Grafenauer *(Universitaet Klagenfurt, Austria),* Sandra König and Stefan Schauer *(Austrian Institute of Technology, Austria)*	**Knowledge compilation techniques for model-based diagnosis of complex active systems** *Gianfranco Lamperti (University of Brescia, Italy), Marina Zanella (University of Brescia, Italy) and Xiangfu Zhao (Zhejiang Normal University, China)* **Recognition of Handwritten Characters Using Google Fonts and Freeman Chain Codes** *Alexiei Dingli, Mark Bugeja and Dylan Seychell (University of Malta, Malta)*

16:15 – 16:30	**short Coffee Break**				
	ARES Full VIII Network Security and Monitoring II **Session Chair: Chibuike Ugwuoke, TU Delft, Netherlands** **Lecture Hall G (221)**	**CUING IV** **Session Chair: Klaus Kieseberg, SBA Research Austria** **Lecture Hall H (222)**	**SSE Secure software development and DevOps** **Session Chair: Juha Röning, University of Oulu, Finland** **Lecture Hall F (220)**	**IWSECC II Security Engineering Solutions for Cloud Computing** **Session Chair: Eduardo B. Fernandez, Florida Atlantic University, USA** **Lecture Hall E (122)**	**CD-MAKE IV** **Session Chair: Panagiotis Germanakos, SAP SE & University of Cyprus, Cyprus** **Lecture Hall C (120)**
16:30 – 17:30	**A Pyramidal-based Model to Compute the Impact of Cyber Security Events** Gustavo Gonzalez *(Atos, Spain)*, Jose Manuel Rubio Hernan and Joaquin Garcia-Alfaro *(Télécom SudParis, CNRS UMR 5157 SAMOVAR, Université Paris-Saclay, France)* **ToGather: Towards Automatic Investigation of Android Malware Cyber-Infrastructures** Elmouatez Billah Karbab Karbab and Mourad Debbabi *(Concordia University, Canada)*	**Towards Utilization of Covert Channels as a Green Networking Technique** Daniel Geisler *(FernUniversitaet in Hagen, Germany)*, Wojciech Mazurczyk *(Warsaw University of Technology, Poland)* and Joerg Keller *(FernUniversitaet in Hagen, Germany)* **Enhanced Electromagnetic Side-channel Eavesdropping Attacks on Computer Monitors** Asanka Sayakkara, Nhien An Le Khac and Mark Scanlon *(University College Dublin, Ireland)*	**Surveying Secure Software Development Practices in Finland** Kalle Rindell, Jukka Ruohonen *(University of Turku, Finland)* and Sami Hyrynsalmi (*Tampere University of Technology, Finland)* **Challenges and Mitigation Approaches for Getting Secured Applications in a Big Company** Pawel Rajba *(University of Wroclaw, Poland)* **Software Security Activities that Support Incident Management in Secure DevOps** Martin Gilje Jaatun *(SINTEF Digital, Norway)*	**A Reference Architecture for the Container Ecosystem** Madiha Syed and Eduardo B. Fernandez *(Florida Atlantic University, United States)* **Evolution Oriented Monitoring oriented to Security Properties for Cloud Applications** Jamal Toutouh, Antonio Muñoz *(University of Malaga, Spain)* and Sergio Nesmachnow *(Universidad de la República – Engineering Faculty, Uruguay)* **IWSECC Interactive Forum Discussion,** Track Dr. Antonio Muñoz, *(University of Málaga, Spain)*	**An Efficient Approach for Extraction Positive and Negative Association Rules in Big Data** Bemarisika Parfait, Ramanantsoa Harrimann and Totohasina André *(Laboratoire de Mathématiques et d'Informatique, ENSET, Université d'Antsiranana, Madagascar)* **Field-Reliability Predictions based on Statistical System Life Cycle Models** Lukas Felsberger (CERN, LMU Munich, Austria), Dieter Kranzlmüller (Ludwig Maximilian University of Munich, Austria) and Benjamin Todd (CERN, Switzerland)

	Harbor Cruise
17:30 – 20:00	We will take you on an evening Harbour Cruise. Experience the multifaceted Port of Hamburg, see and learn about its most interesting places. Our cruise will take us through Hafencity, Speicherstadt (depending on the tide), watergates and canals. **Meeting point:** 17:30 in front of the University, buses leave at 17:40

Wednesday, August 29th, 2018

Time	Track 1: ARES Lecture Hall D (121)	Track 2: Workshops Lecture Hall H (222)	Track 3: Workshops Lecture Hall E (122)	Track 4: Workshops Lecture Hall F (220)	Track 6: CD-MAKE Lecture Hall C 8(120)
08:00 – 16:30	**Registration** **Foyer**				
09:30 – 10:30	**ARES Keynote Session** Session Chair: Edgar Weippl, SBA-Research, Austria **Keynote: Innovations in Permutation-Based Crypto** Dr. Joan Daemen, *Radboud University, Security Architect at ST Microelectronics* Lecture Hall A				
	Abstract: Imagine there's no block ciphers, it's easy if you try:-) A (cryptographic) permutation can be thought of as a block cipher (like AES or DES) without a key (or with a fixed key if you prefer). During the SHA-3 competition it became clear that permutation-based hashing, e.g., by using the sponge construction, is superior to block-cipher based hashing (as in MD5, SHA-1 and SHA-2). By including a key in the sponge input, it can readily be used for message authentication (MAC) and by exploiting the arbitrarily long sponge output even for stream encryption. The duplex variant of sponge widens the spectrum to, among other, authenticated encryption and reseedable pseudorandom generation and was adopted by a dozen submissions to the CAESAR competition for authenticated ciphers. The disadvantage of the sponge and duplex constructions is that they are inherently serial. To address this, we introduced a fully parallel counterpart of the sponge, called Farfalle. Clearly, there is a lot going on in permutation-based crypto and this talk will get you up to date.				
10:30 – 11:00	**Coffee Break**				

	ARES Full IX - Automotive Session Chair: Jose Manuel Rubio Hernán, Télécom SudParis, CNRS UMR 5157 SAMOVAR, Université Paris-Saclay, France Lecture Hall D (121)	IoT-SECFOR I Session Chair: Virginia Franqueira, University of Derby, UK Lecture Hall H (222)	IWCC I Session Chair: Wojciech Mazurczyk, Warsaw University of Technology, Poland Lecture Hall E (122)	IWSMA I Session Chair: tba Lecture Hall F (220)	CD-MAKE V Session Chair: Constantions Mourlas, National & Kapodistrian University of Athens, Greece Lecture Hall C (120)
11:00 – 12:30	**Attack Graph-Based Assessment of Exploitability Risks in Automotive On-Board Networks** Martin Salfer and Claudia Eckert *(Technical University of Munich, Germany)* **Anonymous Charging and Billing of Electric Vehicles** Daniel Zelle, Markus Springer, Maria Zhdanova and Christoph Krauß *(Fraunhofer, Germany)* **Comparison of Data Flow Error Detection Techniques in Embedded Systems: an Empirical Study** Venu Babu Thati *(Katholieke Universiteit Leuven, Belgium)*, Jens Vankeirsbilck *(Katholieke Universiteit Leuven, Belgium)*, Niels Penneman *(Televic Healthcare, Belgium)*, Davy Pissoort *(Katholieke Universiteit Leuven, Belgium)* and Jeroen Boydens *(Katholieke Universiteit Leuven, Belgium)*	**Keynote: Steganography in the World of IoT** Aleksandra Mileva, *(University of Goce Delcev, MK)* **Security Threats and Possible Countermeasures in Applications Covering Different Industry Domains** Musa Samaila, João Sequeiros, Mário Freire and Pedro Inácio *(Instituto de Telecomunicações and Department of Computer Science, Universidade da Beira Interior, Covilhã, Portugal)*	**Keynote: Reality of Malware Author Attribution** Natalia Stakhanova, *(University of New Brunswick, Canada)* **Monitoring Product Sales in Darknet Shops** York Yannikos *(Fraunhofer, Germany)*, Annika Schäfer *(TU Darmstadt, Germany)* and Martin Steinebach *(Fraunhofer, Germany)* **IoT Forensic: Identification and Classification of Evidence in Criminal Investigations** François Bouchaud, Gilles Grimaud and Thomas Vantroys *(IRCICA – CRIStAL, France)*	**Toward a Distributed Trust Management scheme for VANET** Amira Kchaou, Ryma Abassi *(SUPCOM, Tunisia)* and Sihem Guemara El Fatmi *(High School of Communication, Sup'Com, Tunisia)* **There Goes Your PIN: Exploiting Smartphone Sensor Fusion Under Single and Cross User Setting** David Berend *(Nanyang Technological University, Singapore, University of Applied Sciences Wiesbaden, Rüsselsheim, Germany)*, Bernhard Jungk (*Temasek Laboratories at Nanyang Technological University, Singapore)* and Shivam Bhasin *(Temasek Labs@NTU, Singapore)* **Towards a Privacy Preserving and Flexible Scheme for Assessing the Credibility and the Accuracy of Safety Messages Exchanged in VANETs** Ons Chikhaoui, Aida Ben Chehida Douss, Ryma Abassi and Sihem Guemara El Fatmi *(Higher School of Communication, Sup'Com, Tunisia)*	**Building a Knowledge Based Summarization System for Text Data Mining** Andrey Timofeyev and Ben Choi *(Louisiana Tech University, USA)* **Spanish Twitter Data Used As A Source Of Information About Consumer Food Choice** Luis Gabriel Moreno Sandoval, Carolina Sanchez Barriga, Katherine Espindola Buitrago, Alexandra Pomares Quimbaya and Juan Carlos García Días *(Pontificia Universidad Javeriana, Colombia)* **Feedback Matters! Predicting the Appreciation of Online Articles: A Data-Driven Approach** Catherine Sotirakou *(National & Kapodistrian University of Athens, Greece)*, Panagiotis Germanakos *(SAP SE &amp; University of Cyprus, Germany)*, Andreas Holzinger *(Medical University Graz, Austria)* and Constantinos Mourlas *(National & Kapodistrian University of Athens, Greece)*

12:30 – 14:00	Lunch				
14:00 – 15:30	**ARES Short I Malware Session Chair: Johannes Blömer, University of Paderborn, Germany Lecture Hall D (121)**	**IoT-SECFOR II Security Attacks & Solutions Session Chair: Virginia Franqueira, University of Derby, UK Lecture Hall H (222)**	**IWCC II Session Chair: Krzysztof Cabaj, Warsaw University of Technology, Poland Lecture Hall E (122)**	**IWSMA II Session Chair: tba Lecture Hall F (220)**	**MAKE-Text Session Chair: Philipp Cimiano, Universität Bielefeld, Germany Lecture Hall C (120)**
	An Investigation of a Deep Learning Based Malware Detection System Mohit Sewak, Sanjay Sahay and Hemant Rathore *(BITS, Pilani, Department of CS & IS, Goa Campus, India)* **Towards the Automatic Generation of Low-Interaction Web Application Honeypots** Marius Musch, Martin Johns *(TU Braunschweig, Germany*) and Martin Härterich *(SAP Security Research, Germany)* **Learning Malware Using Generalized Graph Kernels** Khanh Huu The Dam *(LIPN and University Paris Diderot, France)* and Tayssir Touili *(LIPN, CNRS & University Paris 13, France)*	**Denial-of-Service Attacks on LoRaWAN** Eef van Es, Harald Vranken and Arjen Hommersom *(Open University of the Netherlands, Netherlands)* **Towards In-Network Security for Smart Homes** Martin Serror, Martin Henze *(RWTH Aachen University, Germany)*, Sacha Hack, Marko Schuba *(FH Aachen University of Applied Sciences, Germany)* and Klaus Wehrle *(RWTH Aachen University, Germany)* **On Track of Sigfox Confidentiality with End-to-End Encryption** Radek Fujdiak, Petr Petr *(Brno University of Technology, Czech Republic)*, Konstantin Mikhaylov *(University of Oulu, Finland)*, Lukas Malina, Petr Mlynek, Jiri Misurec and Vojtech Blazek *(Brno University of Technology, Czech Republic)* **Improved RNS-Based PRNGs** Alan Michaels *(Virginia Tech, United States)*	**Recent Granular Computing Implementations and its Feasibility in Cybersecurity Domain** Marek Pawlicki *(UTP Bydgoszcz, Poland)*, Michal Choras *(ITTI Ltd., Poland)* and Rafal Kozik *(Institute of Telecommunications, UTP Bydgoszcz, Poland)* **Determination of Security Threat Classes on the basis of Vulnerability Analysis for Automated Countermeasure Selection** Elena Doynikova, Andrey Fedorchenko and Igor Kotenko *(St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Russia)* **A New Classification of Attacks against the Cyber-Physical Security of Smart Grids** Ghada Elbez, Hubert B. Keller and Veit Hagenmeyer *(Karlsruhe Institute of Technology, Germany)*	**Practical Precise Taint-flow Static Analysis for Android App Sets** William Klieber, Lori Flynn, William Snavely and Michael Zheng *(Carnegie Mellon Univ, Software Engineering Institute, United States)* **Detection of Obfuscation Techniques in Android Applications** Alessandro Bacci, Alberto Bartoli *(Dipartimento di Ingegneria e Architettura – Università degli Studi di Trieste, Italy)*, Fabio Martinelli *(Istituto di Informatica e Telematica – Consiglio Nazionale delle Ricerche, Pisa, Italy)*, Eric Medvet *(Dipartimento di Ingegneria e Architettura – Università degli Studi di Trieste, Italy)* and Francesco Mercaldo *(Istituto di Informatica e Telematica – Consiglio Nazionale delle Ricerche, Pisa, Italy)* **Tackling Android's Native Library Malware with Robust, Efficient and Accurate Similarity Measures** Anatoli Kalysch, Mykolai Protsenko, Oskar Milisterfer and Tilo Müller *(Friedrich-Alexander-Universität ErlangenNürnberg (FAU), Germany)*	**A Combined CNN and LSTM Model for Arabic Sentiment Analysis** Abdulaziz Alayba, Vasile Palade, Matthew England and Rahat Iqbal *(Coventry University, UK)* **Between the Lines: Machine Learning for Prediction of Psychological Traits - a Survey** Dirk Johannßen and Chris Biemann *(University of Hamburg, Germany)* **LawStats -- Large-scale German Court Decision Evaluation using Web Service Classifiers** Eugen Ruppert *(University of Hamburg, Germany)*, Dirk Hartung *(Bucerius Law School, Germany)*, Phillip Sittig, Tjorben Gschwander, Lennart Rönneburg, Tobias Killing and Chris Biemann *(University of Hamburg, Germany)*

15:30 – 16:00	**Coffee Break**			
	ARES Full X - Cloud Security **Session Chair: Sebastian Schrittwieser, FH St. Pölten, Austria** **Lecture Hall D (121)**	**IoT-SECFOR III - Security Assessment & Analysis** **Session Chair: Virginia Franqueira, University of Derby, UK** **Lecture Hall H (222)**	**SPEBD** **Session Chair: tba** **Lecture Hall H (222)**	**MAKE-Smart Factory** **Session Chair: Mario Heinz. Ostwestfalen-Lippe University of Applied Sciences, Germany** **Lecture Hall C (120)**
16:00 – 17:20	**Distributed and Cooperative Firewall/Controller in Cloud Environments** Ferdaous Kamoun-Abid, Amel Meddeb-Makhlouf, Faouzi Zarai *(NTS'COM, ENET'COM, Tunisia)* and Mohsen Guizani *(ECE Department, University of Idaho, USA)* **Cloud Architectures for Searchable Encryption** Johannes Blömer and Nils Löken *(University of Paderborn, Germany)*	**Correlation Power Analysis on the PRESENT Block Cipher on an Embedded Device** Owen Lo, Bill Buchanan *(Edinburgh Napier University, UK)* and Douglas Carson *(Keysight Technologies, UK)* **Adding Salt to Pepper: A Structured Security Assessment over a Humanoid Robot** Alberto Giaretta *(Örebro Universitet, Sweden)*, Michele De Donno and Nicola Dragoni (*Technical University of Denmark, Denmark)* **Towards Wireless Secret key Agreement with LoRa Physical Layer** Henri Ruotsalainen *(St. Pölten University of Applied Sciences, Austria)* and Stepan Grebeniuk *(VACE Systemtechnik GmbH, Austria)*	**Secure Fixed-point Division for Homomorphically Encrypted Operands** Chibuike Ugwuoke, Zekeriya Erkin and Reginald Lagendijk *(Delft University of Technology, Netherlands)* **Attribute Based Content Security and Caching in Information Centric IoT** Nurefsan Sertbas, Samet Aytac, Orhan Ermis *(Bogazici University, Turkey)*, Gurkan Gur *(ZHAW Zurich University of Applied Sciences, Swtiherlands) and* Fatih Alagoz *(Bogazici University, Turkey)* **Evidence Identification in Heterogenous Data Using Clustering** Hussam Mohammed, Nathan Clarke and Fudong Li *(University of Plymouth, UK)*	**A Multi-Device Assistive System for Industrial Maintenance Operations** Mario Heinz, Hitesh Dhiman and Carsten Röcker *(University of Applied Sciences Ostwestfalen-Lippe – Institute Industrial IT, Germany)* **Feedback Presentation for Workers in Industrial Environments – Challenges and Opportunities** Mario Heinz and Carsten Röcker *(University of Applied Sciences Ostwestfalen-Lippe – Institute Industrial IT, Germany)*
17:30 – 23:00	**Conference Dinner & Miniature Wonderland**			
	Our Conference Dinner – a highlight at ARES 2018 – will take place right at the heart of Hamburg´s historical port area. Located at the centre of the Speicherstadt, the Experience Warehouse combines comfort with the flair of ancient merchant tradition. After an aperitif you will get the chance to experience Hamburg´s most popular tourist attraction, the Miniature Wonderland. The biggest model railway exhibition impresses through lifelike scenery of European countries, the US, replica of Hamburg Airport and much more. **Meeting point:** 17:30 in front of the University, buses leave at 17:40 			

Thursday, August 30th, 2018					
Time	Track 1: ARES Lecture Hall D (121)	Track 2: Workshops Lecture Hall H (222)	Track 3: Workshops Lecture Hall E(122)	Track 4: Workshops Lecture Hall F (220)	Track 6: CD-MAKE Lecture Hall (120)
08:30 – 14:00	**Registration** **Foyer**				
09:30 – 11:00	ARES Short II Monitoring Session Chair: Christian Doerr, TU Delft, Netherlands Lecture Hall D (121)	FARES I Protection and Detection Session Chair:Eduardo B. Fernandez, Florida Atlantic University, USA Lecture Hall H (222)	SAW I Session Chair:Jungwoo Ryoo, Pennsylvania State University, USA Lecture Hall E (122)	iPAT I Session Chair: Max Maaß, TU-Darmstadt, Germany Lecture Hall F (220)	MAKE-Explainable AI I Session Chair: Andreas Holzinger, Medical University of Graz, Austria Lecture Hall C (120)
	Assessing Internet-wide Cyber Situational Awareness of Critical Sectors Martin Husák *(Masaryk University, Czech Republic),* Nataliia Neshenko, Morteza Safaei Pour, Elias Bou-Harb *(Florida Atlantic University, United States)* and Pavel Čeleda *(Masaryk University, Czech Republic)* **Spreading Alerts Quietly: New Insights from Theory and Practice** Olivier Blazy *(Université de Limoges, France)* and Céline Chevalier *(ENS, France)*	**Recovery of Encrypted Mobile Device Backups from Partially Trusted Cloud Servers** Omid Mir, Rene Mayrhofer, Michael Hölzl and Thanh-Binh Nguyen *(Institute of Networks and Security, Johannes Kepler University, Austria)* **Reputation-Based Security System For Edge Computing** Francis Nwebonyi, Rolando Martins *(University of Porto, Portugal)* and Manuel E. Correia *(CRACS/INESC TEC; DCC/FCUP, Portugal)* **New Authentication Concept Using Certificates for Big Data Analytic Tools** Paul Velthuis *(Fraunhofer -SIT, Netherlands),* Marcel Schäfer and Martin Steinebach *(Fraunhofer SIT, Germany)*	**Mission-Centric Automated Cyber Red Teaming** Suneel Randhawa *(Defence Science and Technology, Department of Defence, Australia),* Benjamin Turnbull, Joseph Yuen *(The University of New South Wales, Australia)* and Jonathan Dean *(Defence Science and Technology, Department of Defence, Australia)* **Ransomware's Early Mitigation Mechanisms** Ruta Mussaileb, Nora Cuppens *(IMT-Atlantique, France),* Jean Louis Lanet *(INRIA, France),* Helene Bouder *(IMT-Atlantique, France),* Benjamin Bouget *(DGA, France)* and Aurelien Palisse *(INRIA, France)*	***Keynote - Usable Privacy&Security Preserving Services in the Cloud*** *Simone Fischer-Hübner, (Karlstad University, Sweden)* **The User-centered Privacy-aware Control System PRICON: An Interdisciplinary Evaluation** Jonas Walter, Bettina Abendroth *(TU Darmstadt, Germany),* Thilo von Pape *(Université de Franche-Comté, France),* Christian Plappert Daniel Zelle, Christoph Krauß *(Fraunhofer, Germany),* Gundula Gagzow *(Unabhängiges Landeszentrum für Datenschutz, Germany)* and Hendrik Decke *(Volkswagen, Germany)*	**Keynote Randy Goebel** *(University of Alberta, Canada)* **Explainable AI: the New 42?** Andreas Hozinger *(Medical University,Austria)* and Peter Kieseberg *(SBA Research, Austria)* **A Rule Extraction Study Based on a Convolutional Neural Network** Guido Bologna (*University of Applied Science and Arts of Western Switzerland, Switzerland)*

	A Reactive Defense Against Bandwidth Attacks Using Learning Automata Nafiseh Kahani *(Queen's Univeristy, Canada)* and Mehran Fallah *(Amirkabir University of Technology, Iran)*	**Evaluation of Machine Learning-based Anomaly Detection Algorithms on an Industrial Modbus/TCP Data Set** Simon Duque Anton, Suneetha Kanoor, Daniel Fraunholz and Hans Dieter Schotten *(Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Germany)*	**A GDPR Compliance Module for Supporting the Exchange of Information between CERTs** Otto Hellwig *(SBA-Research, Austria),* Gerald Quirchmayr (*University of Vienna, Austria),* Walter Hötzendorfer *(Research Institute AG & Co KG, Austria),* Christof Tschohl *(Research Institute AG & Co KG, Austria),* Edith Huber (*Danube University Krems, Austria),* Franz Vock *(Federal Chancellery, Austria),* Florian Nentwich (*IKARUS Security Software, Austria),* Bettina Pospisil *(Danube University Krems, Austria),* Matthias Gusenbauer (*SBA-Research, Austria)* and Gregor Langner (*University of Vienna, Austria)*		
11:00 – 11:30	**Coffee Break**				

	ARES Short III Attacks and Mitigation Session Chair: Jose Manuel Rubio Hernán, CNRS UMR 5157 SAMOVAR, Université Paris-Saclay, France Lecture Hall D (121)	FARES II Session Chair: Aaron Visaggio, University of Sannio, Italy Lecture Hall H (222)	SAW II Session Chair: Simon Tjoa, St. Pölten University of Applied Sciences, Austria Lecture Hall E (122)	iPAT II Session Chair: Dr. Jörg Daubert, TU-Darmstadt, Germany Lecture Hall F (220)	MAKE-Explainable AI II Session Chair: Andreas Holzinger, Medical University of Graz, Austria Lecture Hall C (120)
11:30 – 13:00	**ATG: An Attack Traffic Generation Tool for Security Testing of In-vehicle CAN Bus** Tianxiang Huang *(Chongqing University of Posts and Telecommunications, China)*, Jianying Zhou (Singapore University of Information Systems Technology and Design) **Technology and Design, Singapore) and Andrei** Bytes *(Singapore University of Technology and Design, Singapore)* **Let's Shock our IoT's Heart: ARMv7-M Under (fault) Attacks** Sebanjila K. Bukasa, Ronan Lashermes, Jean-Louis Lanet and Axel Legay *(TAMIS INRIA-RBA, France)* **Enterprise WLAN Security Flaws: Current Attacks and Relative Mitigations** Mohamed Abo-Soliman and Marianne Azer *(Nile University, Egypt)*	**X.509 Certificate Error Testing** David Mcluskie and Xavier Bellekens *(Abertay University, UK)* **Evaluating the Degree of Security of a System Built Using Security Patterns** Eduardo B. Fernandez *(Florida Atlantic University, USA)*, Nobukazu Yoshioka *(National Institute of Informatics, Japan)* and Hironori Washizaki *(Waseda, Japan)* **Attack Difficulty Metric for Assessment of Network Security Preetam Mukherjee and** Chandan Mazumdar (*Jadavpur University, India)* **Robustness Estimation of Infrastructure Networks: On the Usage of Degree Centrality** Sebastian Wandelt and Xiaoqian Sun *(Beihand University, China)*	**CryptSDLC: Embedding Cryptographic Engineering into Secure Software Development Lifecycle** Thomas Lorünser *(AIT Austrian Institute of Technology, Austria)*, Thomas Länger *(University of Lausanne, Austria)*, Henrich C. Pöhls and Leon Sell *(University of Passau, Germany)* **Architectural Solutions to Mitigate Security Vulnerabilities in Software Systems** Priya Anand and Jungwoo Ryoo *(The Pennsylvania State University, USA)*	**User Privacy Attitudes Regarding Proximity Sensing** Håkan Jonsson *(Lund University, Sweden)* and Carl Magnus Olsson (*Malmö University, Sweden)* **Critical Analysis of LPL according to Articles 12 - 14 of the GDPR** **Armin Gerl and Dirk Pohl** *(Universität Passau, Germany)* **Privacy and DRM Requirements for Collaborative Development of AI Applications** Vida Ahmadi Mehri, Dragos Ilie and Kurt Tutschku *(Blekinge Institute of Technology, Sweden)*	**Evaluating Explanations by Cognitive Value** Ajay Chander and Ramya Srinivasan *(Fujitsu Labs of America, USA)* **Measures of Model Interpretability for Model Selection** André M. Carrington, Paul Fieguth and Helen Chen *(University of Waterloo, Canada)* **Regular Inference on Artificial Neural Networks** Franz Mayr and Sergio Yovine *(Universidad ORT, Uruguay)* **Creative Intelligence – Automating Car Design Studio with Generative Adversarial Networks (GAN)** Sreedhar Radhakrishnan, Varun Bharadwaj, Varun Manjunath and Ramamoorthy Srinath *(PES University, India)*
13:00 – 14:00			**Lunch**		CD-MAKE Journal Editorial Board meeting (221, East Wing)

	ARES Short IV **Security Practices** **Session Chair:** **Martin Husák,** **Masaryk University,** **Czech Republic** **Lecture Hall D (121)**	**CD-MAKE Topology** **Session Chair:** **Massimo Ferri,** **University of Bologna,** **Italy** **Lecture Hall C (120)**
14:00 – 15:30	**What are Security Patterns? A Formal Model for Security and Design of Software** Anika Behrens *(University of Bremen, Germany)* **A Nlp-based Solution to Prevent from Privacy Leaks in Social Network Posts** **G**erardo Canfora, Andrea Di Sorbo, Enrico Emanuele, Sara Forootani and Corrado A. Visaggio *(University of Sannio, Italy)* **In Secure Configuration Practices of WPA2 Enterprise Supplicants** Alberto Bartoli (*Università degli Studi di Trieste – DEEI, Italy),* Eric Medvet *(DI3 – University of Trieste, Italy),* Fabiano Tarlao *(Department of Engineering and Architecture, University of Trieste, It)* and Andrea De Lorenzo *(University of Trieste – DIA, Italy)*	**Topological Characteristics of Digital Models of Geological Core** Rustem Gilmanov *(OOO "Gazpromneft NTC", Russia),* Iskander Taymanov (*St. Petersburg State University, Russia),* Alexander *Kalyuzhnyuk (Peter the Great St.Petersburg Polytechnic University, Russia)* and Andrey Yakovlev *(OOO "Gazpromneft NTC", Russia)* **On a New Method to Build Group Equivariant Operators by Means of Permutants** Francesco Camporesi, Patrizio Frosini and Nicola Quercioli *(University of Bologna, Italy)* **Shortened Persistent Homology for a Biomedical Retrieval System with Relevance Feedback** Alessia Angeli, Massimo Ferri, *Eleonora (University of Bologna, Italy),* and Ivan Tomba *(Ca-Mi srl, Italy)*
15:30 – 15:45	**Short coffee break**	

Keynotes

ARES Keynote Speaker

Adrian Perrig

ETH Zürich, Switzerland

Keynote: A Next-generation Secure Internet for the 21st Century

Monday, August 27, 2018, 10.30 – 11.30; LH A

Abstract: *The Internet has been successful beyond even the most optimistic expectations. It permeates and intertwines with almost all aspects of our society and economy. The success of the Internet has created a dependency on communication as many of the processes underpinning the foundations of modern society would grind to a halt should communication become unavailable. However, much to our dismay, the current state of safety and availability of the Internet is far from commensurate given its importance.*

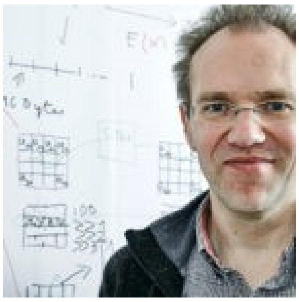
Although we cannot conclusively determine what the impact of a 1-day, or 1-week outage of Internet connectivity on our society would be, anecdotal evidence indicates that even short outages have a profound negative impact on society, businesses, and government. Unfortunately, the Internet has not been designed for high availability in the face of malicious actions by adversaries. Recent patches to improve Internet security and availability have been constrained by the current Internet architecture, business models, and legal aspects. Moreover, there are fundamental design decisions of the current Internet that inherently complicate secure operation.

Given the diverse nature of constituents in today's Internet, another important challenge is how to scale authentication of entities (e.g., AS ownership for routing, name servers for DNS, or domains for TLS) to a global environment. Currently prevalent PKI models (monopoly and oligarchy) do not scale globally because mutually distrusting entities cannot agree on a single trust root, and because everyday users cannot evaluate the trustworthiness of each of the many root CAs in their browsers.

To address these issues, we propose SCION, a next-generation Internet architecture that is secure, available, and offers privacy by design; that provides incentives for a transition to the new architecture; and that considers economic and policy issues at the design stage. We have implemented SCION and deployed it in the production networks of several ISPs.

Adrian Perrig is a Professor at the Department of Computer Science at ETH Zürich, Switzerland, where he leads the network security group. He is also a Distinguished Fellow at CyLab, and an Adjunct Professor of Electrical and Computer Engineering, and Engineering and Public Policy at Carnegie Mellon University. From 2002 to 2012, he was a Professor of Electrical and Computer Engineering, Engineering and Public Policy, and Computer Science (courtesy) at Carnegie Mellon University, becoming Full Professor in 2009. From 2007 to 2012, he served as the technical director for Carnegie Mellon's Cybersecurity Laboratory (CyLab). He earned his MS and PhD degrees in Computer Science from Carnegie Mellon University, and spent three years during his PhD at the University of California at Berkeley. He received his BSc degree in Computer Engineering from EPFL. Adrian's research revolves around building secure systems -- in particular his group is working on the SCION secure Internet architecture.

He is a recipient of the NSF CAREER award in 2004, IBM faculty fellowships in 2004 and 2005, the Sloan research fellowship in 2006, the Security 7 award in the category of education by the Information Security Magazine in 2009, the Benjamin Richard Teare teaching award in 2011, the ACM SIGSAC Outstanding Innovation Award in 2013. He is an IEEE senior member and became an ACM Fellow in 2017.



Dr. Joan Daemen,

Radboud University, Security Architect at ST Microelectronics

Keynote: Innovations in permutation-based crypto

Wednesday, August 29, 2018, 09.30 – 10.30, LH A

Abstract: *Imagine there's no block ciphers, it's easy if you try:-) A (cryptographic) permutation can be thought of as a block cipher (like AES or DES) without a key (or with a fixed key if you prefer). During the SHA-3 competition it became clear that permutation-based hashing, e.g., by using the sponge construction, is superior to block-cipher based hashing (as in MD5, SHA-1 and SHA-2). By including a key in the sponge input, it can readily be used for message authentication (MAC) and by exploiting the arbitrarily long sponge output even for stream encryption. The duplex variant of sponge widens the spectrum to, among other, authenticated encryption and reseedable pseudorandom generation and was adopted by a dozen submissions to the CAESAR competition for authenticated ciphers. The disadvantage of the sponge and duplex constructions is that they are inherently serial. To address this, we introduced a fully parallel counterpart of the sponge, called Farfalle. Clearly, there is a lot going on in permutation-based crypto and this talk will get you up to date.*

Joan Daemen is professor at Radboud University as well as cryptographer and security architect at ST Microelectronics, and in his work as a symmetric cryptography expert he has designed a variety of block ciphers over the past 25 years. Dr. Daemen is probably best known for his work on the Rijndael cipher, which was selected as the Advanced Encryption Standard (AES) in 2001. He also co-invented Sponge functions and specifically the Keccak hash, which in 2012 has been chosen to become the new SHA-3 hash function. Joan Daemen's work is thus at the core of much of the cryptography and network security protocols in use today, and in 2017 he was recognized for his contribution with the Levchin Prize for Real World Cryptography.

CD-MAKE Keynote Speaker

Prof. Dr. Klaus-Robert MÜLLER

Machine Learning Group TU Berlin, MPI for Informatics, Saarbrücken, and Korea University, Seoul

Keynote: Machine learning and AI for the sciences - towards understanding

Tuesday, August 28, 2018, 11.00 – 12.00, LH A

Abstract: *In recent years, machine learning (ML) and artificial intelligence (AI) methods have begun to play a more and more enabling role in the sciences and in industry. In particular, the advent of large and/or complex data corpora has given rise to new technological challenges and possibilities. In his talk, Müller will touch upon the topic of ML applications in the sciences, in particular in neuroscience, medicine and physics. He will also discuss possibilities for extracting information from machine learning models to further our understanding by explaining nonlinear ML models. E.g. Machine Learning Models for Quantum Chemistry can, by applying interpretable ML, contribute to furthering chemical understanding. Finally, Müller will briefly outline perspectives and limitations.*

Klaus-Robert Müller studied physics (Master-1989) and computer science (PhD-1992) in Karlsruhe, did a Postdoc at GMD FIRST (1992-1994) and at the University of Tokyo (1994/95), then founded the Intelligent Data Analysis group at GMD FIRST (1995) and became Professor at the University of Potsdam (1999). Since 2006 he is Machine Learning Professor at TU Berlin; directing the Bernstein Center for Neurotechnology Berlin (-2014) and from 2014 co-directing the Berlin Big Data Center. He was awarded the Olympus Prize for Pattern Recognition (1999), the SEL Alcatel Communication Award (2006), the Science Prize of Berlin by the Governing Mayor of Berlin (2014), the Vodafone Innovations Award (2017). In 2012, he was elected member of the German National Academy of Sciences-Leopoldina, in 2017 of the Berlin Brandenburg Academy of Sciences and also in 2017 external scientific member of the Max Planck Society. His research interests are intelligent data analysis and Machine Learning in the sciences (Neuroscience, Physics, Chemistry).

Randy Goebel

University of Alberta, Canada

Keynote: Integrating abduction, visualization, and explanation as a data architecture for Artificial Intelligence

Thursday, August 30, 2018, 9.30 – 11.00, LH C

Abstract: *The integration of abduction, visualization, and explanation provides a fundamental data architecture for artificial intelligence (AI). Abduction has been described as constrained induction, which provides the basis for using what is already known to focus the synthesis — both creation and adjustment — of scientific theories. Visualization is inherently about how to appropriately present information for drawing inferences by the human visual system. And explanation is at the heart of the scientific process, which, in all its forms, is about connecting theories and evidence across a spectrum from exposing relationships between observation and theory, all the way to exposing causality. We will attempt to create coherence around these three foundational ideas, show how they can be related in both theory and practice, by use of examples of multi-level representations that can exploit AI and machine learning for both humans and machines.*

R.G. (Randy) Goebel is Professor of Computing Science at the University of Alberta, in Edmonton, Alberta, Canada, and concurrently holds the positions of Associate Vice President Research, and Associate Vice President Academic. He is also co-founder and principle investigator in the Alberta Innovates Centre for Machine Learning. He holds B.Sc., M.Sc. and Ph.D. degrees in computer science from the University of Regina, Alberta, and British Columbia, and has held faculty appointments at the University of Waterloo, University of Tokyo, Multimedia University (Malaysia), Hokkaido University, and has worked at a variety of research institutes around the world, including DFKI (Germany), NICTA (Australia), and NII (Tokyo), was most recently Chief Scientist at Alberta Innovates Technology Futures. His research interests include applications of machine learning to systems biology, visualization, and web mining, as well as work on natural language processing, web semantics, and belief revision. He has experience working on industrial research projects in scheduling, optimization, and natural language technology applications.

ARES EU Symposium Workshop Keynotes

Peter Schneider

Nokia Bell Labs, Germany

Keynote: Where we are in 5G Security - from early requirements until today

Workshop 5G-NS 2018, Monday, August 27, 2018, 11.45 – 12.45, LH B

Abstract: *5G mobile networks will have to support a variety of services, including control of critical infrastructures, Industry 4.0 factory communication or vehicular communication. There is no doubt that supreme, built-in security is required for maintaining the availability and integrity of the communication network and ensure the dependability that is essential for such mission critical services. Accordingly, demanding security requirements have been raised in early stages of the conceptual work. Since then, various research projects investigated 5G security aspects, and standardization is well on the way, with the first release of the 3GPP 5G System mostly frozen in June 2018. This talk will briefly revisit 5G security requirements, give an overview of what has been achieved until now, and point out some areas for future 5G security research.*

After receiving his diploma in mathematics, Peter started his professional career at Siemens, as a researcher on new software architectures. For several years, he worked on the research and prototyping of innovative communication solutions. Later, he became a system engineer for the IP based mobile core network, working on various aspects of the IP technology, in particular on IP security, deep packet inspection and IP network reliability. Since 2007, he is focusing on network security research. Currently, he is a senior expert for mobile network security in the Security Research Team at Nokia Bell Labs. In this position, he has been involved in various security research projects including publicly funded international projects. He has published his research results at various conferences and has given many invited talks and tutorials on network security topics. His research interests include all aspects of mobile network security, in particular security for programmable, cloud-based networks and the overall security architecture of future 5G networks.

Kim-Kwang Raymond Choo

The University of Texas at San Antonio, USA

Keynote: Cyber Security Threat Intelligence: Challenges and Research Opportunities

Workshop CyberT IM 2018, Monday, August 27, 2018, 11.45 – 12.45, LH C

Abstract: *Cyber threat intelligence and analytic is among one of the fastest growing interdisciplinary fields of research bringing together researchers from different fields such as digital forensics, political and security studies, criminology, cyber security, big data analytics, machine learning, etc. to detect, contain and mitigate advanced persistent threats and fight against organized cybercrimes. In this presentation, we will discuss some of the challenges underpinning this inter- / trans- /multi-disciplinary field as well as research opportunities (e.g. how can we leverage advances in deep learning to better predict cyber attacks?).*

Bio: Kim-Kwang Raymond Choo received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA), and has a courtesy appointment at the University of South Australia. In 2016, he was named the Cybersecurity Educator of the Year – APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn), and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, ESORICS 2015 Best Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is also a Fellow of the Australian Computer Society, an IEEE Senior Member, and an Honorary Commander of the 502nd Air Base Wing, Joint Base San Antonio-Fort Sam Houston.

Hervé Debar

Telecom SudParis, France

Keynote: Reasoning about alert formats: a comparative study

Workshop CyberT IM 2018, Monday, August 27, 2018, 17.40 – 18.40, LH C

Abstract: *Intrusion detection sensors and SIEM platforms have been available for over a decade now. While significant efforts have been realized to ensure communication between detection tools and management platforms, one needs to acknowledge that no standard has prevailed at this time for expressing alert information. In this presentation, we will analyze several relevant alert formats, describe their advantages and drawbacks, and provide hints for future situational awareness platforms.*

Bio: I am a professor at Telecom SudParis, head of the Networks and Telecommunication Services department. My activity is related to the area of Information and Communication Technology (ICT) security, including network and information systems security. While I have been heavily involved in intrusion detection research in the past and am still conducting research in the area, I am today focusing on Security Information and Event Management (SIEM), with an emphasis on automated threat mitigation.

Workshop Keynotes:

Philipp Amann

Europol European Cyber Crime Centre (EC3)

Keynote: Europol EC3 - Europol's European Cybercrime Centre - a networked approach

Workshop CUING 2018, Tuesday, August 28, 2018, 09.00 – 10.30, LH B

Abstract: *There is a service-based underground industry that fuels cybercrime, turning it into a growth business in terms of scope and volume of attacks, number of victims and economic damage. This calls for a networked, intelligence-led, adaptive and pro-active response that includes law enforcement. Prioritised and coordinated joint actions against the key cyber threats supported by adequate legislation can change the rules of the game by increasing the risks for cybercriminals and imposing real consequences. Effective prevention and disruption activities can further tip the scales to the detriment of criminals. The multi-stakeholder model and networked approach used by Europol's European Cybercrime Centre is a successful example of how this can be put in practice by leveraging the power of the network.*

Philipp Amann is the Head of Strategy of the European Cybercrime Centre (EC3). EC3 Strategy is responsible for the delivery of strategic, situational and tactical cyber-related products such as the Internet Organised Crime Threat Assessment (IOCTA). Other key areas of responsibility include prevention and awareness, outreach, stakeholder management, training management and internet governance.

Prior to joining the EC3, he held management positions with the Organization for Security and Co-operation in Europe, the Organisation for the Prohibition of Chemical Weapons and the International Criminal Court. Philipp has more than 17 years of relevant working experience and hands-on skills in information and cyber security management, policy development, combatting cybercrime, electronic evidence management and the analysis and management of intelligence. He has worked in various fields, including the financial sector, global disarmament and arms control, CBRNe, law enforcement and international law. He is also a member of ENISA’s Permanent Stakeholder Group and the program advisory board of the Cyber Akademie. Philipp’s professional experience is complemented by a PhD degree and a Master’s degree in business informatics from the University of Vienna. He also holds an MSc in Forensic Computing and Cybercrime Investigation from the University College Dublin.

Hasan Yasar

Secure Lifecycle Solutions group Software Engineering Institute, Carnegie Mellon University

Keynote: DevOps is the key for Continuous Security: RMF, ATO and beyond

Workshop SSE 2018, Tuesday, August 28, 2018, 16.00 – 17.30, LH F

Abstract: *Risk Management Framework (RMF) or Authority to Operate (ATO) is the bottleneck for continuous deployment when it is not addressed automatically. The only solution is being agile with DevOps principles. Such as communication and collaboration between all stakeholders via automated and integrated platform enables to address lengthy RMF/ATO process, so new features can be deployed into production faster with high degree on security. To do, the team must identify a continuous monitoring approach to the security controls with automated ways of performing assessments throughout DevOps pipeline. This talk will describe how to overlays RMF onto DevOps pipeline and taking an advantage of core DevOps core principles (CI, CD, IaC, automation and beyond) based on lesson learned examples on SEI/CERT engagement with various clients who operates at Highly Regulated Environments*

Hasan Yasar is the technical manager of the Secure Lifecycle Solutions group Software Engineering Institute, Carnegie Mellon University. Hasan leads an engineering group on software development processes and methodologies, specifically on DevOps practices, cloud technologies and big data problems while providing expertise and guidance to SEI's clients. Hasan has more than 25 years' experience as senior security engineer, software engineer, software architect and manager in all phases of secure software development and information modeling processes. He is specialized on secure software solutions design and development experience in the cybersecurity domain including data-driven investigation and collaborative incident management, network security assessment, automated and large-scale malware triage/analysis. He is also Adjunct Faculty member in CMU Heinz Collage and Institute of Software Research where he currently teaches "Software and Security" and "DevOps: Engineering for Deployment and Operations".

Aleskandra Mileva

University of Goce Delcev, Macedonia

Keynote: Steganography in the World of IoT

Workshop IoT-SECFOR 2018, Wednesday, August 29, 2018, 11.00 – 12.30, LH B

Abstract*: Steganography, as a subfield of information hiding, is an art of hiding a message in a legitimate carrier, so that no one suspects it exists. When the carrier is some transmission in communication networks, we speak about network steganography. And when we have a communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy, we speak about the covert channel. In this talk, a recent trends and achievements of network steganography and covert channels in the world of Internet of Things and Cyber Physical Systems will be presented.*

Aleksandra Mileva is an associate professor and a vice dean at the Faculty of Computer Science, University "Goce Delčev" in Štip, Republic of Macedonia and Head of the Laboratory of computer security and digital forensics. She received her PhD degree in Computer Science from the Faculty of Natural Sciences and Mathematics Skopje, "Ss. Cyril and Methodius" University in Skopje in 2010. Her research interests include: cryptography, network steganography, computer and network security, IoT protocols and security, and digital forensics. She is a member of the Criminal Use of Information Hiding (CUing) initiative.

Natalia Stakhanova

University of New Brunswick, Canada

Keynote: Reality of malware author attribution

Workshop IWCC 2018, Wednesday, August 29, 2018, 11.00 – 12.30, LH E

Abstract: *Since the first computer virus hit the DARPA network in the early 1970s, the security community interest revolved around ways to expose identities of malware writers. Knowledge of the adversary's identity promised additional leverage to security experts in their ongoing battle against perpetrators. At the dawn of computing era, when malware writers and malicious software were characterized by the lack of experience and relative simplicity, the task of uncovering the identities of virus writers was more or less straightforward. Manual analysis of source code often revealed personal, identifiable information embedded by authors themselves. But these times have long gone. Modern days' malware writers extensively use numerous malware code generators to mass produce new malware variants and employ advanced obfuscation techniques to hide their identities. As a result the work of security experts trying to uncover the identities of malware writers became significantly more challenging and time consuming. With introduction of more and more advanced obfuscation techniques and malware writing kits, we face the challenging questions: Is it even feasible to reveal adversary's identity? In this talk, we will explore this question in the context of authorship attribution research. Well-established in social science, authorship attribution offers a broad spectrum of techniques that allow author's characterization based on the analysis of the textual features of documents and an author's writing style. Drawing analogy between literature and software domain, in this talk we investigate our ability to attribute malware code.*

Natalia Stakhanova is the New Brunswick Innovation Research Chair in Cyber Security at the University of New Brunswick, Canada. Her work revolves around building secure systems and includes mobile security, IoT security, software obfuscation & reverse engineering, and malicious software. Working closely with industry on a variety of R&D projects, she developed a number of technologies that resulted in 3 patents in the field of computer security. Natalia Stakhanova is the recipient of the UNB Merit Award, the McCain Young Scholar Award and the Anita Borg Institute Faculty Award. She is a strong advocate of Women in IT and co-founder of CyberLaunch Academy, an initiative that aims to promote science and technology among children.

Virginia N. L. Franqueira

University of Derby, UK

Keynote: Structured Argumentation in Digital Forensic Practice: Opportunity or Burden?

Workshop WSDF 2018, Tuesday, August 28, 2018, 09:00 – 10:30, LH D

Abstract: *Digital Forensic (DF) practitioners have to gather massive amounts of data from a diversity of seized devices, online forums and/or cloud storage for the investigation of cyber-enabled or cyber-dependent crimes. This exponentially growing volume, and increasing variety and complexity of data involved in single cases, known as a "big data problem in DF", imposes numerous challenges. For example, such data typically contains numerous pieces of evidence of different types collected using a variety of forensic tools and techniques, such as hard drive evidence, mobile phone evidence, social media evidence, evidence from the crime scene, and evidence from interviews. It mostly remains up to DF investigators to systematically reason about how evidence of different types can be logically connected and how they fit together in the case's "big picture". This talk explores this problematic phenomenon and discusses ways in which structured argumentation could potentially be helpful for interpretation, reconstruction and reporting of forensic arguments to the Court of Law.*

Virginia Franqueira received a Ph.D. in Computer Science (focused on Security) from the University of Twente (Netherlands) in 2009, and a M.Sc. in Computer Science (focused on Optimization) from the Federal University of Espirito Santo (Brazil). Since June 2014, she holds a senior lecturer position in Computer Security and Digital Forensics at the University of Derby, UK. She has around 40 publications related to Security or Digital Forensics. Her research interests include cybercrime investigation, image processing and reconstruction. She is a member of the British Computer Society and fellow of The Higher Education Academy.

Simone Fischer-Hübner

Karlstad University, Sweden

Keynote: Usable Privacy&Security Preserving Services in the Cloud

Workshop iPAT 2018, Thursday 30, 2018, 09:30 – 11:00, LH F

Abstract: *This presentation will present end user perspective and HCI requirements for Privacy-enhancing services that have been developed for the Cloud context within the H2020 project PRISMACLOUD. The focus will be on a Selective Authentic Exchange Service based on malleable signatures in an eHealth use case, which allows patients to selectively disclose authentic medical data from a private cloud platform to different parties, as well as the configuration management of the ARCHISTAR service based on secret sharing for securely archiving data in the Cloud. User studies with different types of stakeholders and their results will be presented, which show in particular that even technically-skilled users require special HCI guidance. Moreover, also support for meeting legal and organizational requirements is needed.*

Simone Fischer-Hübner has been a Full Professor at Karlstad University since June 2000, where is the head of the Privacy& Security (PriSec) research group. She received a Diploma Degree in Computer Science with a minor in Law (1988), and a PhD (1992) and Habilitation (1999) Degrees in Computer Science from Hamburg University. She has been conducting research in privacy and privacy-enhancing technologies for more than 30 years. She is the chair of IFIP WG 11.6 on "Identity Management", the Swedish IFIP TC 11 representative, member of MSB's Information Security Advisory Board (MSB:s informationssäkerhetsråd), member of the Scientific Advisory Board of Science Europe, Vice Chair of IEEE Sweden and has been an expert for ENISA (European Network and Information Security Agency). She is partner in several European privacy-related research projects including the EU H2020 projects PAPAYA, CREDENTIAL PRISMACLOUD, and the EU H2020 Marie Curie ITN Privacy&Us, for which she is also the scientific coordinator. Moreover, she coordinates the Swedish IT Security Network SWITS.

Kas Clark

National Cyber Security Centre

Keynote: Building CTI at the national level

Workshop WCTI, Tuesday, August 28, 2018, 13:15 – 14:45, LH E

Abstract: *Cyber Threat intelligence (CTI) is not a single product, but rather a wide spectrum of tools, processes, knowledge and, above all, close collaboration with trusted partners. In the Netherlands, the National Cyber Security Centre (NCSC) is working hard to build and improve its CTI capabilities. As the Computer Emergency Response Team (CERT) for the Dutch national government and critical infrastructure, we are responsible for the increasing the resilience of our digital society. As threats increase and malicious actors improve their skills, so too must we continue to grow our defensive capabilities. One aspect of this is significant investment to harness the benefits of CTI by turning limited information into actionable intelligence. This presentation describes our role in this field, the types of questions our CTI needs to answer, as well as the growth of our capabilities and research in this area.*

Kas Clark lives and works in The Hague as a senior researcher for the National Cyber Security Centre (NCSC), a division of the Dutch Ministry of Justice and Security. The NCSC works together with academia and the private sector to align efforts around high priority areas of research. His current work focusses on improving the effectiveness of security teams through multidisciplinary research that includes both technical and social aspects. After completing his bachelor's and master's degrees in computer science, he received a Ph.D. in computer science with a specialization in distributed computing from the Delft University of Technology. In addition, he has served on the editorial boards of the IEEE Security & Privacy and Platform for Information Security magazines.

Social Events

This year we have planned a truly diverse social program for ARES and CD-MAKE 2018. We hope to see you all there!

If you want to come directly to a social event (and you are not using the organized transport) please contact us at the registration desk to find an appropriate meeting point.

Monday, August 27, 2018 – Welcome Reception

Meeting point: 19:00 in the foyer of the University

Get a taste of Hamburg´s cuisine and culture at this year´s ARES reception. Fish buns, local craft beer and the performance of a shanty-choir will get you in the mood for a great conference.

Shanty-Choir HHLA Hamburg (Source: Norbert Müller)

Tuesday, August 28, 2018 – Harbor Cruise

Meeting point: 17:30 in front of the University, buses leave at 17:40

On August 28, 2018, we will take you on an evening Harbor Cruise. Experience the multifaceted Port of Hamburg, see and learn about its most interesting places. Our cruise will take us through Hafencity, Speicherstadt (depending on the tide), watergates and canals.

Harbor Cruise (Resource: http://www.abicht.de/fleet/mb-iris-abicht)

Wednesday, August 29, 2018 – Conference Dinner and Miniature Wonderland

Meeting point: **17:30 in front of the University**, buses leave at 17:40

Our Conference Dinner – a highlight at ARES 2018 – will take place right at the heart of Hamburg´s historical port area. Located at the center of the Speicherstadt, the Experience Warehouse combines comfort with the flair of ancient merchant tradition. After an aperitif you will get the chance to experience Hamburg´s most popular tourist attraction, the Miniature Wonderland. The biggest model railway exhibition impresses through lifelike scenery of European countries, the US, replica of Hamburg Airport and much more.

Experience Warehouse

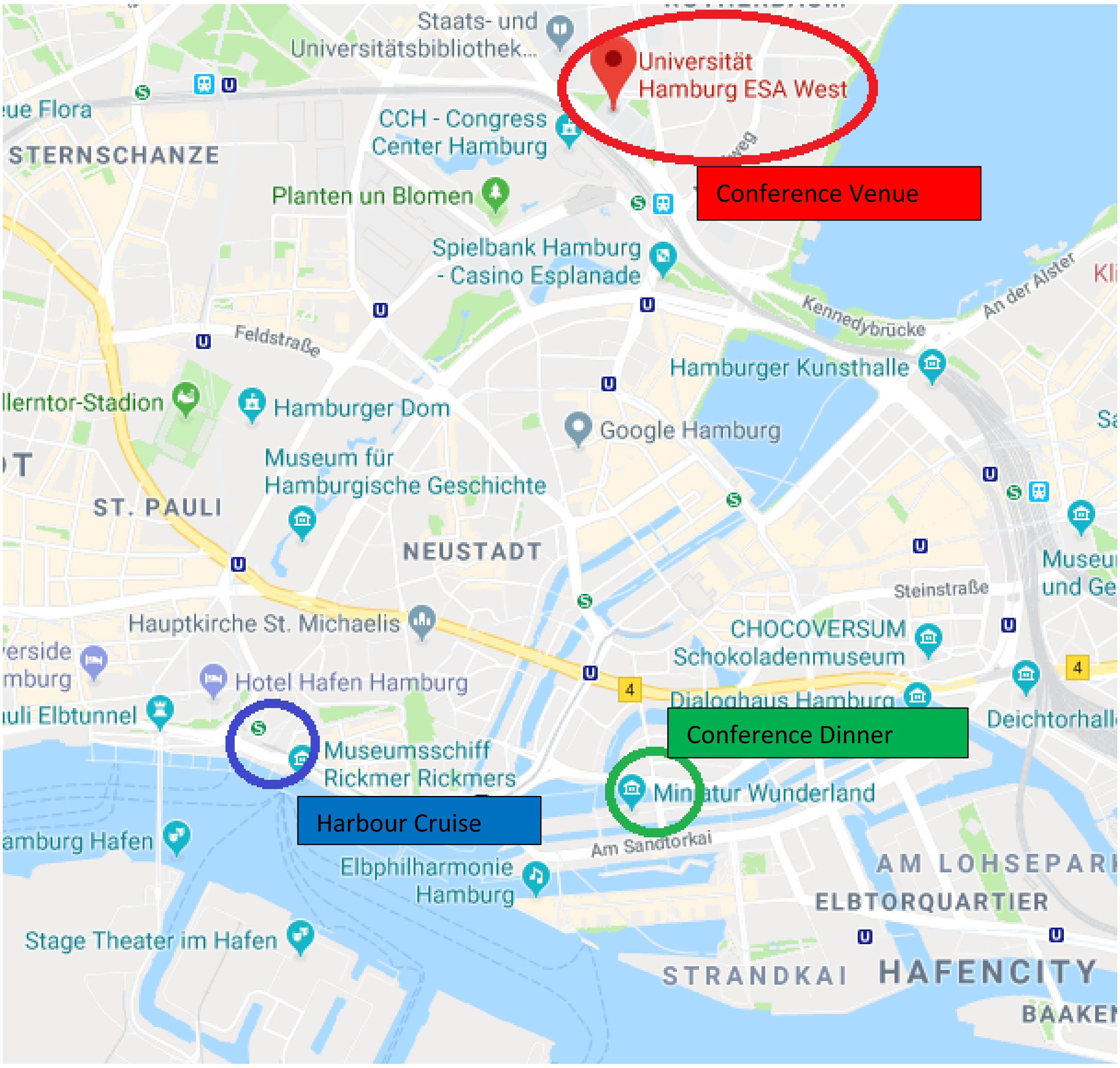
(Resource: Nord Event GmbH)

Miniature Wonderland

(Resource: https://presse.miniatur-wunderland.de/download/)

Venue Overview

Coordinates:
https://www.google.at/maps/place/Universit%C3%A4t+Hamburg+ESA+West/@53.5509586,9.9716015,14z/data=!4m5!3m4!1s0x47b18f3cbe82f20d:0x3aa594a8a534d678!8m2!3d53.5631951!4d9.9877377



Venue Overview

Conference Venue

Address of the ARES 2018 Conference Venue
University of Hamburg, Main Building
Edmund-Siemers-Allee 1
20146 Hamburg
Germany

ARES 2018 and all collocated events will take place in the buildings of the ESA campus of University of Hamburg, which is located at Edmund-Siemers-Allee.

The venue is right in the heart of the city of Hamburg and in close walking distance (10 minutes) to beautiful Binnenalster, a water basin surrounded by parks that is very popular with locals and visitors alike.

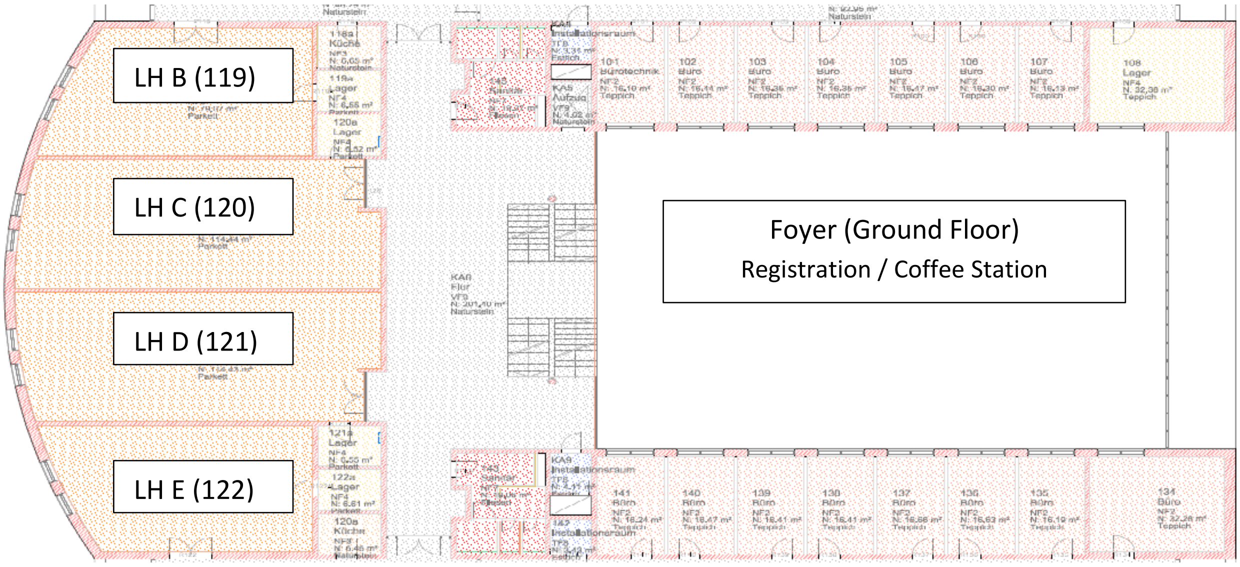
The ESA campus is well-connected to public transport: **Dammtor railway station**, which is served by local as well as long-distance trains, is located right in front of the building (5 minutes walking distance). **Hamburg Airport** can be reached within 30 minutes by city trains (departing every 10 minutes).

Room Plans

ROOM CHANGE:
WS 5G-NS from LH B (119) to LH F (220) – all day
WS SECPID from LH F (220) to LH D (121) – last session

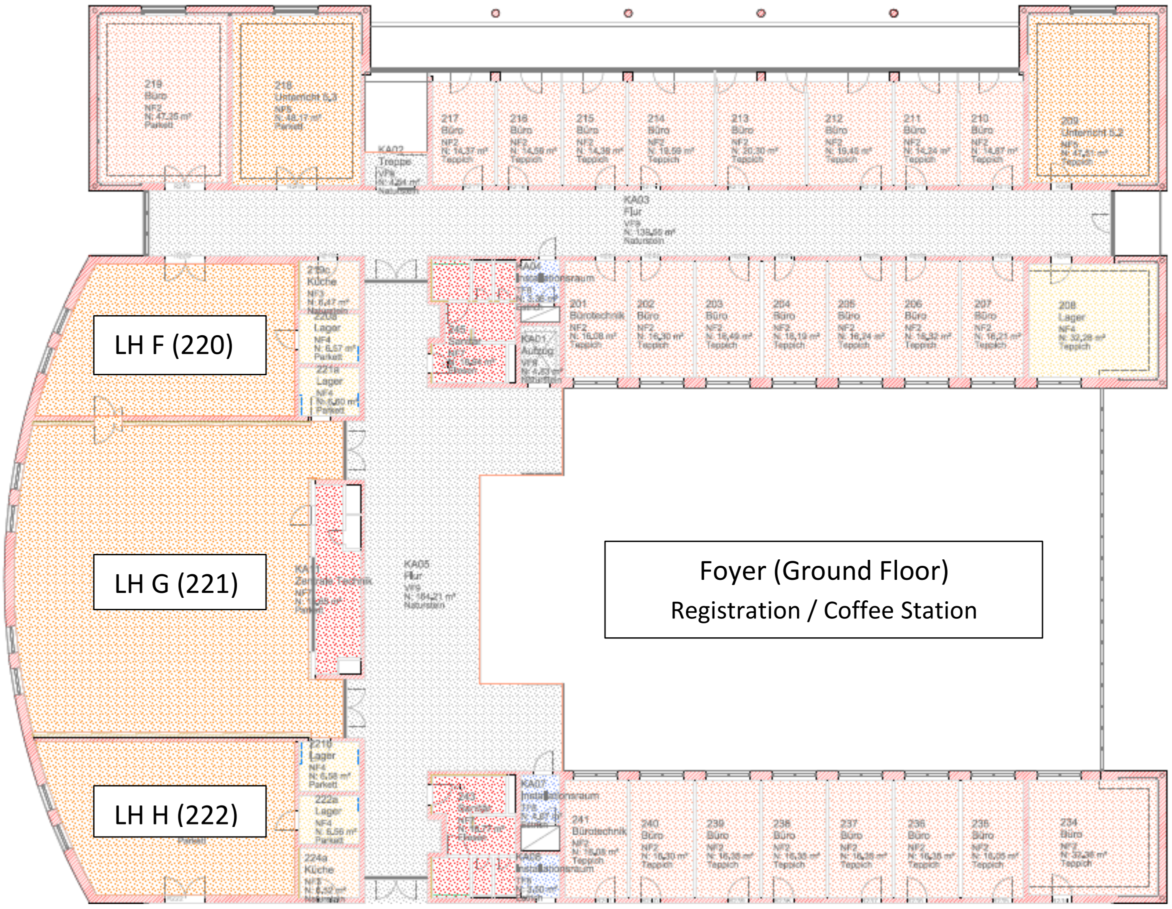
Lecture Halls

West Wing, First Floor



Lecture Halls

West Wing, Second Floor



Lunch Information & Menu

We will provide you with a catered lunch directly at the conference venue. There will be a lunch and coffee break area on site.

Please find the menu below:

Monday, August 27, 2018
Main Course - Shredded chicken, chickpea curry with mince yoghurt sauce, rice with herbs
Side Dishes - Mixed salad (lettuce, vegetables)
Dessert – Mango mousse with mango puree, coconut rice pudding with rhubarb sauce

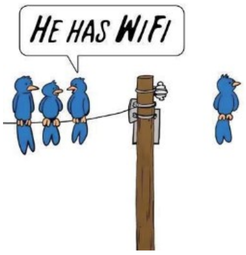
Tuesday, August 28, 2018
Main Course – Chicken vegetable mix with green asparagus, ratatouille with basil sauce, gnocchi
Side Dishes - Mixed salad (lettuce, vegetables)
Dessert – Chocolate mince mousse, panna cotta with strawberry puree

Wednesday, August 29, 2018
Main Course – Corn poulard with rosemary jus, pointed cabbage with nut potatoes, beetroot pilaf with pea dip
Side Dishes - Mixed salad (lettuce, vegetables)
Dessert – Curd cream with red fruit pudding, stracciatella mousse with forest berries

Thursday, August 30, 2018
Starters – Superfood salads (bulgur with almonds, soya, couscous mince with fried shrimp, quinoa)
Main Course – Shredded chicken with vegetables and spaetzle, vegetable lasagna
Dessert – Vanilla soya pudding with berries, fruit skewers

WIFI Information

There is WIFI available at the venue of ARES 2018: GUEST
As for this year's conference WIFI, we have a personalized access for each participant at Hamburg University. The code to connect to the WIFI can be found on your badge.



Eduroam is also available.

WIFI in the city

Throughout the city there are various public spots that offer free wifi services such as for instance the passage Hanseviertel in the city center, the shopping mall Hamburger Hof and many more. Additionally, there are free wifi services offered in the railways. If you are curious about all the places around you that offer free wifi services, you can check them out by downloading the wiman app in your Appstore.

More information can be found here: https://www.wiman.me/germany/free-wifi-hamburg

Directions

Address of the Conference Venue:
Universität Hamburg
Edmund-Siemers-Allee 1
20146 Hamburg

How to get from the Conference Venue to the City Center

Dammtor Railway Station

From Dammtor Railway Station to Hamburg Hauptbahnhof (Central Railway Station)

Take

- **S1** in direction of Hamburg Airport to Hamburg Hauptbahnhof (2 minutes).
- **S3** in direction of Hamburg-Neugraben/Stade to Hamburg Hauiptbahnhof (2 minutes).
- **S21** in direction of Hamburg Bergedorf to Hamburg Hauptbahmhof (2 minutes).

From Dammtor Railway Station to Rathausmarkt (City Hall)

Take

- **Bus Line 4** in direction of Rathausmarkt/Brandstwiete to Rathausmarkt (7 minutes).
- **Bus Line 5** in direction of Hauptbahnhof/ZOB to Rathausmarkt (7minutes).

How to get from the Conference Venue to the City Center

From Dammtor Railway Station to the Harbor Area (St. Pauli Landungsbrücken)

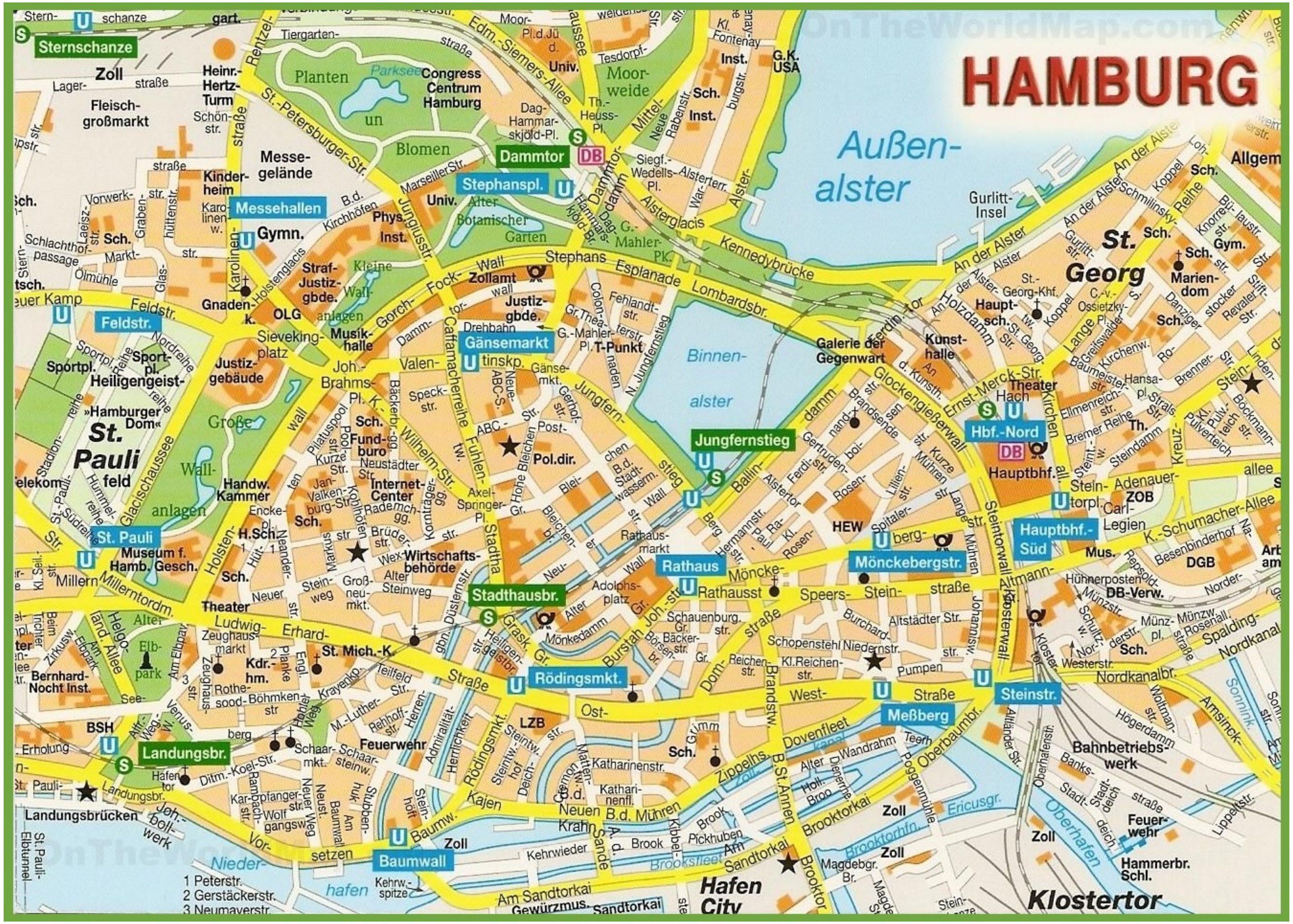
Hamburg Harbour Area, St. Pauli Landungsbrücken

Take

- **Bus Line 4** in direction of Rathausmarkt to Rathausmarkt (7 minutes).
  Change to the metro and take U3 from Rathaus in direction of Barmbek(2) to Landungsbrücken (5 minutes).
- **Bus Liner 5** in direction of Hauptbahnhof/ZOB to Rathausmarkt (7minutes).
  Change to the metro and take U3 from Rathaus in direction of Barmbek(2) to Landungsbrücken (5 minutes).
- **S21** in direction of Elbgaustraße to Sternschanze (2 minutes).
  Change to the metro and take U3 from Sternschanze (Messe) in the direction of Wandsbeck Gartenstadt to Landungsbrücken (5 minutes).

Sternschanze Metro Station
https://www.google.at/search?q=sternschanze+station&rlz=1C1GCEA_enAT765AT765&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjFpMG4sfvcAhXrsaQKHe2-B5gQ_AUICygC&biw=1366&bih=631#imgrc=k4NlSxGceFmeDM:

City Map Hamburg



City Map Hamburg

Source: http://ontheworldmap.com/germany/city/hamburg/hamburg-city-centre-map.html

Welcome to Hamburg!

Picture Source: Shutterstock

Useful Information

Tourist Information
Hauptbahnhof Hamburg Kirchenallee 20095 Hamburg +49 40 30051707

Emergency Numbers	
Fire service	112
Police	110
Ambulance/ rescue	112
European emergency	112

Drinking Water

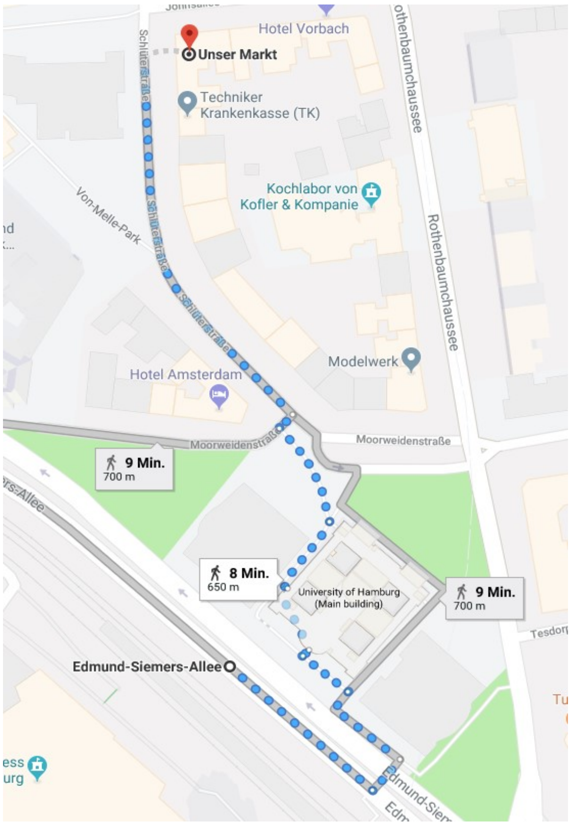
It is officially safe to drink tap water.

Opening Hours of Shops in Hamburg

Shop opening hours may depend indicatively. Generally, shopping centers, and smaller shops tend to have opening hours from 9:00 – 19:00 from Monday to Saturday. Apart from small markets, gas station and pharmacies (emergency service 24/7) everything tends to be closed on Sundays.

There is a supermarket not far from the conference venue called *Unser Markt.*

Tipping: Tipping in restaurants in Germany is not obligatory. However, if you are happy with the service you can leave a 10% tip of the bill or simply round up to a convenient number.



Unser Markt Supermarket

About Hamburg

Hamburg is the second-largest city of Germany with a population of roughly 1.8 million people. The city lies at the core of the Hamburg Metropolitan Region which spreads across four German federal states and is home to more than 5 million people. The official name reflects Hamburg's history as a member of the medieval Hanseatic League, a free imperial city of the Holy Roman Empire, a city-state and one of the 16 states of Germany. Situated on the river Elbe, Hamburg is home to Europe's second-largest port and a broad corporate base.

Hamburg Port
Picture Source: www.cruisemapper.com

The city of Hamburg was once built on trade, survived Danish, Prussian, French and Nazi rule, endured fires, floods and diseases. Hamburg is one of the greenest cities in Europe with a number of parks, botanical gardens, nature reserves and deep forests. From Romanic churches & Jugendstil mansions to sleep modern office buildings. Thank Hamburg, think harbour! Hamburg´s main waterway, the Elbe connects the city to the North Sea. Piers feature spectacular views and must-see historic waterfront buildings. Some of the must sees are: City Hall, Speicherstadt, Fischmarkt, Landungsbrücken and the Elbphilharmonie.

Fischmarkt
Source: https://hamburgtourist.info

Elbphilharmonie
Source: www.stern.de

Hamburg has an oceanic climate, influenced by its proximity to the coast and marine air masses that originate over the Atlantic Ocean. The warmest moths are June, July and August, with average highs of 23 °C. Rain falls throughout the year in Hamburg. The most rain falls during the 31 days centered around June 30th, with an average total accumulation of 2 inches or 5cm.

The Culinary Side of Hamburg

Due to its location on the Elbe river and its proximity to the sea the regional cuisine does feature a lot of fish dishes. Beside of different herring dishes like Matjes or Bismarckhering, Green Herring ('green' meaning fresh, hence not marinated, fried or cured) is also very common. A main dish of Hamburg cuisine which originates in the burgois cuisine owes its development to the intensive trade with Portugal. It features oxtail in Madeira wine and is nowadays rather used as soup course instead of the main dish.

Like in any larger city, Hamburg offers a great variety of snacks with a local or regional tradition. Next to the popular fish sandwiches which are called Fischbrötchen, toasted white bread with small, brown shrimps from the North Sea called Krabbentoast is very popular either for breakfast or as a snack at lunch time. Other popular snacks are Currywurst which comes in different styles made with different kind of sausages, or Knackwurst.

Typical sweet dishes of the cuisine of Hamburg are Rote Grütze with milk, vanilla sauce, vanilla ice cream or liquid cream, elderberry soup or Großer Hans (a flour dumpling eaten with cherry compote) and bread pudding with lemon sauce.

Fischbrötchen
Source: www.bento.de

Curry Wurst
Source: www.hamburg.mitvergnuegen.com

Rote Grütze with milk
Source: www.stellarash.com

Tourism Information Hamburg

Here are some websites that provide further information and suggestions for your stay in Hamburg:

Hamburg Tourism: https://www.hamburg.com/
Hamburg Travel: http://www.hamburg-travel.com/info/out-and-about-in-hamburg/tourist-info-hotlines/
TripAdvisor: https://www.tripadvisor.com.au/Tourism-g187331-Hamburg-Vacations.html

Survive in Hamburg… ☺

Hello!	Hallo!	*Ha-low*
Goodbye!	Auf Wiedersehen!	*Aouf-we-der-zehen*
How are you?	Wie geht´s?	*Vee gits?*
Do you speak English? (informal)	Sprechen Sie Englisch?	*Shprexh-en zee eng-lish?*
Can you help me?	Können Sie mir helfen?	*Kuh-nen zee mir hel-fen?*
You're welcome.	Bitte gerne.	*Bitt-er*
Please.	Bitte.	*Bi-te*
Yes.	Ja.	*Ya*
No.	Nein.	*Niyn*
I don't know	Ich weiß nicht.	*Ikh wise nikht*
I (don't) understand.	Ich verstehe nicht.	*Sorry, ah-ber ikh ver-shte-he-nikht*
Okay.	Okay	*Okay*
Help!	Hilfe!	*Heel-fe!*
Thank you	Danke.	*Dan-ker*
Thank you very much	Vielen Dank!	*Vee-len dank*
Excuse me? (When walking through a crowd)	Entschuldigen Sie?	*Ent-schul-dig´n zee*
Excuse me.	Entschuldigung.	*Ent-schul-dig´ung*
I'm sorry.	Es tut mir leid.	*Es toot mir lied*
Good morning!	Guten Morgen!	*Goot-en mor-gen/targ*
Good evening!	Guten Abend!	*Goot-en-ar-bent*
Good night!	Gute Nacht!	*Goot-er naxht*
See you later!	Bis später!	*Biz spater*
Where is / Where are... ?	Wo ist / Wo sind …?	*Voe ist / voe sind …?*
The Train station	Zug Station	*Zoog station*
Restroom	Toilette/WC	*To-lett*
The Airport	Flughafen	*Floog-ha-fen*
Post	Post	*Post*
What?	Was?	*Vas*
When?	Wann?	*Van*
How much?	Wie viel?	Vee feel?

Conference Office / Contact

If you need any support, please do not hesitate to contact us.

Julia Pammer
jpammer@sba-research.org
Tel: +43 664 88 198 489

Yvonne Poul
ypoul@sba-research.org
Tel: +43 699 100 41066

Program Overview ARES 2018
August 27-30, Hamburg, Germany

Time	Monday, 27.08.2018				
09:30 - 17:45	Registration, Welcome Coffee				
10:15 - 11:30	LH A: ARES Opening & Keynote A Next-generation Secure Internet for the 21st Century - Adrian Perrig ARES EU Symposium Opening				
11:45 - 12:45	Rooms				
	LH H (222)	LH C (120)	LH D (121)	LH E (122)	LH G (221)
	5G-NS I	CyberTIM I	IWOCCTN I	ECoSP I	ARES Full I
12:45 - 14:00	Lunch				
14:00 - 15:30	Rooms				
	LH H (222)	LH C (120)	LH D (121)	LH E (122)	LH G (221)
	5G-NS II	CyberTIM II	IWOCCTN II	ECoSP II	ARES Full II Best Paper Session
15:30 - 16:00	Coffee Break				
16:00 - 17:30	Rooms				
	LH H (222)	LH C (120)	LH D (121)	LH E (122)	LH G (221)
	5G-NS III	CyberTIM III	IWOCCTN III	ECoSP III	ARES Full III
17:30 - 17:40	Room switch				
17:40 - 18:40	Rooms				
	LH H (222)	LH C (120)	LH F (220)	LH H (222)	LH G (221)
	5G-NS IV	CyberTIM IV	SECPID 17.40-19.10	PCSCP 17.40-19.10	ARES Full IV
19:00 - 21:30	Welcome Reception / Dinner Meeting Point: 19:00 - Foyer of University				

Time	Tuesday, 28.08.2018				
08:00 - 16:30	Registration				
09:00 - 10:30	Rooms				
	LH G (221)	LH H (222)	LH D (121)	LH E (122)	LH C (120)
	ARES Full V	CUING I	WSDF I	WTCI I	
10:30 - 11:00	Coffee Break				
11:00 - 12:00	LH A: CD-MAKE I Keynote & Diskussion Machine learning and AI for the sciences – towards understanding - Klaus-Robert Müller				
12:00 - 13:15	Lunch				
13:15 - 14:45	Rooms				
	LH G (221)	LH H (222)	LH D (121)	LH E (122)	LH C (120)
	ARES Full VI	CUING II	WSDF II	WTCI II	CD-MAKE II
14:45 - 15:15	Coffee Break				
15:15 - 16:15	Rooms				
	LH G (221)	LH H (222)	LH D (121)	LH E (122)	LH C (120)
	ARES Full VII	CUING III	WSDF III	IWSECC I	CD-MAKE III
16:15 - 16:30	short Coffee Break				
16:30 - 17:30	Rooms				
	LH G (221)	LH H (222)	LH F (220)	LH E (122)	LH C (120)
	ARES Full VIII	CUING IV	SSE	IWSECC II	CD-MAKE IV
17:30 - 20:00	Harbor Cruise Meeting Point: 17:30 - in front of University's main entrance				

Time	Wednesday, 29.08.2018					ICS-CSR +only for registered participants
08:30 - 16:00	Registration					08:30 - 09:15 Registration
09:30 - 10:30	LH A: Keynote Session ARES Innovations in permutation-based crypto - Joan Daemen					LH G (221) 09:15 - 09:30 Welcome 09:30 - 10:30 Keynote
10:30 - 11:00	Coffee Break					
11:00 - 12:30	Rooms					
	LH D (121)	LH H (222)	LH E (122)	LH F (220)	LH C (120)	LH G (221)
	ARES Full IX	IoT-SECFOR I	IWCC I	IWSMA I	CD-MAKE V	11:15 - 12:15 Paper 1 & 2
12:30 - 14:00	Lunch					12:15-13:30 Lunch
14:00 - 15:30	Rooms					
	LH D (121)	LH H (222)	LH E (122)	LH F (220)	LH C (120)	LH G (221)
	ARES Short I	IoT-SECFOR II	IWCC II	IWSMA II	MAKE-TEXT	13:30 - 15:00 Paper 3, 4 & 5
15:30 - 16:00	Coffe Break					15:00 - 15:45 Coffee Break
16:00 - 17:30	Rooms					
	LH D (121)	LH H (222)	LH E (122)	LH F (220)	LH C (120)	LH G (221)
	ARES Full X	IoT-SECFOR III	SPEBD		MAKE-Smart Factory	15:45 - 17:00 Paper 6 & 7, Day Closing
17:30 - 23:00	Conference Dinner Meeting Point: 17:30 - in front of University's main entrance					

Time	Thursday, 30.08.2018					ICS-CSR +only for registered participants
08:30 - 14:00	Registration					
09:30 - 11:00	Rooms					
	LH D (121)	LH H (222)	LH E (122)	LH F (220)	LH C (120)	LH G (221)
	ARES Short II	FARES I	SAW I	iPAT I220	MAKE-Explainable AI I	09:00 - 10:00 Morning Coffee 10:00 - 11:00 Industrial Talk
11:00-11:30	Coffee Break					
11:30-13:00	Rooms					
	LH D (121)	LH H (222)	LH E (122)	LH F (220)	LH C (120)	LH G (221)
	ARES Short III	FARES II	SAW II	iPAT II	MAKE-Explainable AI II	Paper 8, 9 & 10
13:00-14:00	Lunch				Room 221 Ost MAKE Journal Editorial Board Meeting	Lunch
14:00-15:30	Rooms					
	LH D (121)				LH C (120)	LH G (221)
	ARES Short IV				MAKE-Topology	14:00 - 15:45 Paper 11, 12 & 13; Conference Closing
15:45 - 16:00						short Coffee Break
						Rooms
						LH G (221)
						16:00 - 17:30 Limes-Cyber-Game