ARES 24

19th International Conference on Availability, Reliability & Security

PROGRAM GUIDE

July 30 until Aug. 02, 2024

Vienna, Austria

Table of Content

Welcome Messages 4

ARES Program Committee Co-Chairs 4

ARES Workshop Chair 6

ARES EU Symposium Workshop Chair 9

Program Overview 11

Tuesday | 30th July, 2024 12

Wednesday | 31st July, 2024 13

Thursday | 1st August, 2024 14

Friday | 2nd August, 2024 15

Social Events 16

Tuesday | 30th July, 2024 16

Wednesday | 31st July, 2024 17

Thursday | 1st August, 2024 18

Keynotes 19

ARES Keynotes 19

Keynotes 21

Accepted Paper Overview 36

Conference Venue 74

Public Transportation 74

Floor Plan 75

Useful Information 79

Organizers and Supporters 80

Welcome Messages

Welcome Message from ARES Program Committee Co-Chairs

Dear attendee, a warm welcome to ARES 2024!
The Nineteenth International Conference on Availability, Reliability, and Security (ARES 2024) brings together researchers and practitioners in the field of availability, reliability, and computer security. The conference highlights various aspects of these, and we are happy to follow the tradition of previous editions to bring together these crucial areas of research.

This year, the main conference is organized in 11 technical sessions, including a session dedicated to the candidates to the Best Paper Award. We are also honored to host two brilliant keynote speakers: Yuval Shavitt, Professor of Electrical Engineering at Tel Aviv University., renown for his work in the fields of network science, caching, routing, IP hijack attacks, traffic classification and network measurements, and Jan Baumbach, Professor at University of Hamburg, renown for his work in the fields of privacy-preserving algorithms and AI and bioinformatics.
ARES has received 173 full papers, 24 SoK papers, and 30 short papers. After desk-rejecting 3 papers, we have accepted 35 full papers, 5 SoK papers, and 5 short papers. For full & SoK papers, this yields an acceptance rate of 20,5%.

We want to thank all the author that submitted a high volume of quality papers to ARES this year. We are also particularly grateful for the hard work, insights and support displayed by each of the Program Committee Members. Thanks to them, we are confident in offering a technically solid program to you. We further thank all workshop chairs for their efforts in organizing engaging workshop sessions. Last but not least, we would like to deeply thank Bettina Jaber, Daniela Freitag-David, Clara Kubesch and Izem Chaloupka from SBA Research, for their relentless support in the organization.
Enjoy ARES 2024!

Haya Schulman
*Goethe-Universität
Frankfurt and ATHENE
Germany*

Dimitris E. Simos
*SBA Research and
Graz University of Technology,
Austria*

Welcome Message from the ARES Workshop Chair

Welcome to the workshops of the nineteenth International Conference on Availability, Reliability and Security (ARES 2024). The workshops are central events for ARES as they provide an essential platform for researchers and practitioners of various domains to present and discuss their findings and work-in-progress. This year we can offer the conference attendees 19 workshops, which range from "start-ups" to well-established ones supporting ARES

Andreas Unterweger
Salzburg University of
Applied Sciences, Austria

THE WORKSHOPS of the 19th International Conference on Availability, Reliability and Security

The succeeding listing comprises the workshops of ARES 2024

ASOD	Workshop on Advances in Secure Software Deployments
BASS	4th International Workshop on Behavioral Authentication for System Security
COSH	International Workshop on Child Online Safety and Harms
CSA	5th Workshop on Recent Advances in Cyber Situational Awareness and Data-Centric Approaches
CUING	8th International Workshop on Criminal Use of Information Hiding
EDId	International Workshop on Emerging Digital Identities
EPIC-ARES	2nd Interdisciplinary Workshop on Applied Research in Embedded, Purpose-specific, Integrated Computing and their Availability, Reliability and Security
FARES	19th International Workshop on Frontiers in Availability, Reliability and Security
GRASEC	5th International Workshop on Graph-based Approaches for CyberSecurity
IMTrustSec	International Workshop on Incident Management, Trusted Computing, Open Hardware and Advanced Security Attacks
IWAPS	4th International Workshop on Advances on Privacy Preserving Technologies and Solutions

Further workshops → **next page**

THE WORKSHOPS

IWCC	International Workshop on Cyber Crime
IWSECC	13th International Workshop on Security Engineering for Cloud Computing
OHC	International Workshop on Open Hardware and Cybersecurity
SecHealth	4th Workshop on Cybersecurity in Healthcare 4.0
SecIndustry	3rd Workshop on Cybersecurity in Industry 4.0
SPETViD	International Workshop on Security and Privacy Enhancing Technologies for Visual Data
Trustbus	21st International Workshop on Trust, Privacy and Security in the Digital Society
WSDF	17th International Workshop on Digital Forensics

Welcome Message from ARES EU Symposium Workshop Chair

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

We would like to thank the workshop organizers for their great efforts and hard work in proposing the workshops, 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!

Florian Skopik
AIT Austrian Institute of Technology, Austria

THE WORKSHOPS

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

CyberHunt	Hands-On Workshop CyberHunt
ENS	7th International Workshop on Emerging Network Security
EPESec	5th International Workshop on Electrical Power and Energy Systems Safety, Security and Resilience
ETACS	3rd Workshop on Education, Training and Awareness in Cybersecurity
PCSCI	3rd International Workshop on Physical and Cyber Security in Interdependent Critical Infrastructures
SP2I	4th International Workshop on Security and Privacy in Intelligent Infrastructures
STAM	4th International Workshop on Safety and Security Testing and Monitoring

Program Overview

Tuesday | 30th July

Time (UTC +2)	SR 03	SR 04	SR 05	SR 07	SR 08	SR 06	HS 02
09:30 18:30	Organizers available						
09:30 10:30	Coffee available						
10:30 12:00	EPESec I		PCSCI			Sec-Industry I	
12:00 13:00	Lunch Beak						
13:00 14:30	EPESec II	STAM I		ENS I	SP2I I	Sec-Industry II	
14:30 15:00	Coffee Break						
15:00 16:30	ETACS I	STAM II	Cyber-hunt I	ENS II	SP2I II	Sec-Industry III	DOD I
16:30 17:00	Coffee Break						
17:00 18:30	ETACS II	STAM III	Cyber-hunt II	ENS III	SP2I III		DOD II
18:30 19:00	Opening - HS 01						
19:00 21:30	Welcome Reception						

Wednesday | 31st July

Time (UTC +2)	HS 01	SR 03	SR 04	SR 05	SR 07	SR08	HS 02
08:30 17:30	Organizers available						
08:45 10:15	ARES I	TRUST-BUS I	IWAPS I	COSH & WSDF I	EDId I	CUING I	
10:15 10:45	Coffee Break						
10:45 12:15	ARES II	TRUST-BUS II	IWAPS II	COSH & WSDF II	EDId II	CUING II	DOD III
12:15 13:15	Lunch Break						
13:15 14:45	ARES III	TRUST-BUS III	IWAPS III	COSH & WSDF III	FARES I	CUING III	DOD IV
14:45 15:15	Coffee Break						
15:15 16:45	ARES IV	TRUST-BUS IV	IWAPS IV	COSH & WSDF IV	FARES II	IMTrust-Sec	DOD V
16:45 17:00	Short Coffee Break						
17:00 18:15	ARES Keynote - HS 01						
18:15 22:00	Suprise Evening Prater Vienna						

Thursday | 1st August

Time (UTC +2)	**HS 01**	**SR 03**	**SR 04**	**SR 05**	**HS 02**	**SR 07**
08:15 17:30	Organizers available					
08:45 10:15	ARES V	ARES SoK	CSA I	GRASEC I		ICS-CSR I
10:15 10:45	Coffee Break					
10:45 12:15	ARES VI	ARES Short	CSA II	GRASEC II	DOD VI	ICS-CSR II
12:15 13:15	Lunch Break					
13:15 14:15	ARES - Best Paper Session - HS 01				DOD VII	ICS-CSR III
14:15 14:45	Coffee Break					
14:45 16:15	ARES VII	ARES VIII	CSA III	IWSECC & SecHealth	DOD VIII	ICS-CSR IV
16:15 16:30	Short Coffee Break					
16:30 18:00	ARES Keynote & Best Paper Award - HS 01					
18:00 22:00	Traditional Viennese Dinner					

Friday | 2nd August

Time (UTC +2)	SR 03	SR 04	SR 05
08:45 14:45	Organizers available		
09:00- 10:30	BASS I		
10:30 11:00	Coffee Break		
11:00 12:30	BASS II	ASOD	IWCC I
12:30 13:30	Lunch Break		
13:30 15:00	BASS III	SPETViD	IWCC & EPIC-ARES II

Social Events

Welcome Reception

18:30

TUE

30th July.

Join us for an evening of networking at the ARES Conference Welcome Reception! Kick off the conference with great conversations, delicious refreshments, and a vibrant atmosphere. Connect with attendees, speakers, and industry professionals in a relaxed setting, fostering collaborations. Don't miss this opportunity to unwind, make connections, and set the tone for a memorable ARES experience

Meeting point:
Währinger Straße 29,
1090 Vienna

SCAN ME

Address: Währinger Straße 29, 1090 Vienna

Scan the QR Code and
find the directions to the location.

© SBA Research

Surprising Evening

19:00

WED

31st July.

Join us for a magical night at the Prater, the world's oldest amusement park, where surprises await! Your ticket includes a voucher for a delightful drink and transportation. Embrace the mystery, enjoy the enchantment, and let the adventure unfold. See you there!

Meeting point:

Faculty Entrance – 18:15

Start: 19:00

© *Shutterstock*

SCAN ME

Address: Riesenradplatz, 1020 Vienna

Scan the QR Code and
find the directions to the location.

Conference Dinner

19:00
THUR
1st Aug.

Join us for an unforgettable experience at our Conference Dinner, where we'll embark on a journey to the historic "10er Marie". This renowned wine tavern, dating back to 1740, is nestled in Vienna's 16th district of Ottakring, boasting the title of the oldest documented "Heuriger" in the city.
Prepare to be enchanted by the rustic charm and rich history of "10er Marie" as we gather to savor traditional Viennese cuisine and indulge in exquisite local wines. This iconic establishment holds a special place in Vienna's culinary landscape.

Meeting point:
Faculty Entrance – 18:00

SCAN ME

Address: Ottakringer Straße 222-224, 1160 Vienna

Scan the QR Code and
find the directions to the location.

© Fuhrgassl Huber

HS 01

31st July

17:00

Yuval Shavitt

Tel Aviv University, Israel

Machine Learning Solutions for detection of attacks on Internet Routing

Attacks on Internet routing have a long history. Early on, attacks used simple IP hijacking, but now they also include routing deflection using manipulations at the BGP level or even at the data plane.

However, defenses against such attacks are falling behind. RPKI is a standard that is (too) slowly deployed in order to protect against IP hijack attacks, when reaching a critical point, it will make such attacks almost impossible. However, RPKI only protects against falsified first hop in the BGP path attribute, while manipulation of other hops has no solution with RPKI. Even the detection of route manipulations is not trivial.

In this talk I will present a Machine Learning approach, BGP2Vec, to detect such attacks with high accuracy and low false alarm rate. BGP2Vec is based on embedding of the ASNs in a latent space in a way that captures the role of an ASN in the routing. This allows us to cluster ASNs and identify a manipulation of a route if an ASN is replaced with one from a different cluster. I will also discuss embedding of Address Prefixes (AP) in the same space and its advantages for deflection attacks. Finally, I will show how to combine the route geography with ML to detect deflection attacks.

© Yuval Shavitt /

HS 01

1st Aug.

16:30

Jan Baumbach

University of Hamburg, Germany

To share or not to share? Privacy-preserving AI in medicine

European Health Data Spaces, national digital health records archives and similar initiatives aim to provide a mixture of legal and technical frameworks to make privacy-sensitive medical data available for data mining. The goal is to access the yet behind legal barriers hidden healthcare data treasure in order to train prognostic models for personalized medicine – from disease management to individualized drug repurposing prediction. The biggest roadblocks are the GDPR and cyber security.

In the talk, we will discuss federated learning technology that – coupled to other privacy-enhancing technologies – allows for a secure multi-center data mining collaboration. Specifically, we will demonstrate that it does provide as accurate results as centralized solutions. We will discuss concrete applications for multi-centric genome-wide association studies, for meta-genomics, transcriptomics and proteomics analysis including batch effect correction, and for survival time analysis. One application involved >1,000 hospitals in North America, another one involves >100,000 European screening participants. Finally, we discuss remaining cyber security aspects, limitations and prospects of federated learning in healthcare data mining.

© *Jan Baumbach*

SR 03

2nd Aug.

9:00

Luca Ardito

Politecnico di Torino, Italy

Behavioural Modelling for Sustainability in Smart Homes

The keynote delves into the transformative potential of smart home technologies in driving sustainability. This session will explore the integration of behavioral modelling, predictive analytics, and gamification to enhance user engagement and promote sustainable practices in smart homes. By examining comprehensive sustainability metrics – environmental, economic, and social – the talk will uncover how these technologies optimize energy efficiency, reduce carbon footprints, and improve overall quality of life.

The critical role of behavioral interventions, such as real-time feedback, automation, incentives, and nudges, will be discussed in fostering eco-friendly behaviors among residents. Highlighting real case studies on devices, the session will demonstrate practical benefits, including significant energy savings, enhanced comfort, and reduced greenhouse gas emissions.

Addressing privacy concerns is important in the adoption of these technologies. Strategies for robust data protection, transparency, and user education will be outlined to build trust and ensure ethical data use. Furthermore, the session will cover the importance of regulatory frameworks like GDPR and CCPA in safeguarding user privacy and promoting secure smart home ecosystems.

The future of smart homes lies in the intersection of technological advancements, policy development, market growth, and environmental impact. The session will explore how advancements in artificial intelligence, machine learning, and data analytics enhance smart home capabilities and how strategic partnerships and continuous innovation drive market growth. Emphasizing the critical contribution of smart homes to global sustainability efforts, the talk will showcase how these technologies mitigate climate change and conserve natural resources.

A key highlight of this session will be the integration of gamification to increase user engagement and motivation. By applying game-design elements like points, leaderboards, and challenges, sustainable practices can become more engaging and enjoyable, leading to greater user involvement and long-term behavior change.

This speech will provide a comprehensive overview of the current and future directions in smart home sustainability, highlighting the interplay between technology, policy, and user engagement to shape research directions and foster a sustainable and efficient future.

© *Luca Ardito*

SR 04

1st Aug.

8:45

Joachim Klerx

Austrian Institute of Technology (AIT), Austria

The Future of Strategic Military Cyber Situational Awareness (CSA)

In this keynote, the transformative future of military Cyber Situational Awareness (CSA) embedded in multi domain activities will be explored, focusing on the integration of cutting-edge technologies like e.g. offensive Large Language Models (LLMs) and AI supported game theoretic planning. These innovations are poised to revolutionize cyber defense and offense, providing military organizations with unprecedented capabilities to predict, analyze, and respond to large scale military cyber threats. Offensive LLMs did enable real-time reasoning on threat analysis, sophisticated automated responses, and effective cyber deception tactics. Concurrently, Game Theoretic Planning Machines will enhance strategic decision-making by modeling adversary behavior, dynamically adapting tactics, and simulating potential scenarios, including exploit markets, CVE message systems and effective monitoring with sensors. This comprehensive and adaptive overview will pay attention to continuous operational effectiveness, proactive defense, and strategic offensive operations, maintaining a critical edge in the ever-evolving landscape of cyber warfare. The future of military CSA is not just about defense but also about leveraging advanced technology for strategic interests in cyberspace, paying attention to cognitive attacks.

© *Joachim Klerx*

SR 05

31st July

8:45

Caroline Roth-Ebner

University of Klagenfurt, Austria

Mediatized Childhood: Navigating the Opportunities and Risks in an Ever-Connected World

Today, children are immersed in and exposed to media from the moment of their birth or even before (e.g., through ultrasound pictures shared on social media). Childhood under these circumstances can be termed a mediatized childhood, with media such as tablet computers, smartphones, and their applications being ubiquitous. Throughout childhood, media function not only as tools for communication and networking but also as status symbols, sources of orientation and means of self-representation. Consequently, they exert a significant influence on children's identity formation. The effects of a mediatized childhood on the young are complex and contingent upon various contextual factors, with education being particularly noteworthy. Numerous studies have shown that the extent to which children benefit from media in their development often relies on their parents' level of education. Depending on such circumstances, as well as situational factors, one and the same phenomenon can manifest both as an opportunity and a risk. For instance, while social media can foster social inclusivity by connecting people, it can also facilitate destructive communication, such as hate speech or cyberbullying. Media literacy, defined as the ability to use media in a responsible, safe, and self-determined way, is regarded as pivotal for maximizing benefits and mitigating harm. However, such competencies do not naturally develop through media usage alone. Children require active support and guidance in their media practices. This responsibility cannot be solely delegated to parents, who are indeed crucial role models and co-educators, but also demands heightened attention and prioritization on the political agenda.

© Caroline Roth-Ebner

SR 08

31st July

8:45

Rémi Cogranne

University of Technology of Troyes (UTT), France

Statistical Models of digital images for Adversarial Methods in steganography and AI-based generation

While a vast majority of digital image forensics approaches are based on machine learning and, recently, exploits the extremely high accuracy of deep learning, these approaches generally provide a low-level of understanding and interpretability.

In the speech, we will present statistical models that allow assessing detectability of information hidden in digital images. We will review how such models can be used to design original adversarial methods that minimizes the statistical detectability.

Last, but not least, we will study the possible application of a similar adversarial method for AI-based generation of digital images.

© *Remi Cogranne*

SR 07

31st July

8:45

Torsten Lodderstedt

SPRIND, Germany

Vision and Challenges of the EUDI Wallet

The new eIDAS regulation will introduce the EUDI Wallet as a digital companion for users across the EU to access services in digital as well as physical space in a privacy preserving, secure, interoperable, and user-friendly manner. This vision is ambitious and requires functions way beyond what typical wallets do today. It also requires an infrastructure for trust management to protect users from malicious issuers, wallet providers or relying parties. Also, the security and privacy requirements are much higher than what has been implemented in the past, resistance against high attack potential in conjunction with unlinkability and unobservability of transactions, just to name a few. This keynote will describe the vision of the EUDI Wallet and highlight some of the challenges, with a focus on those challenges requiring scientific research.

© *Torsten Lodderstedt*

SR 07

30th July

13:00

Marek Pawlicki

Bydgoszcz University of Science and Technology, Poland

Enhancing Network Cybersecurity with Novel Trustworthy AI Solutions

This presentation will focus on novel trustworthy AI solutions in the field of network intrusion detection (NIDS), The research and development work, particularly in the context of EU-funded projects like H2020 STARLIGHT, HE AI4Cyber, H2020 SPARTA, H2020 APPRAISE, H2020 ELEGANT, H2020 SIMARGL and others has led to significant advancements in NIDS and the security of AI systems.

The core of this presentation details the development of AI-based intrusion detection technologies that leverage flow-based data for real-time threat analysis. These systems are designed with modularity and scalability in mind, utilizing tools like Apache Spark and Kafka for efficient data handling and processing.

Another major focus is on explainability in AI, crucial for gaining user trust and enhancing system transparency. Methodologies for integrating explainable AI (xAI) techniques with existing AI models will be presented, which are critical for sectors requiring an understanding of AI decision-making processes. The practical implementation of these technologies in various industrial and academic projects will be discussed, showcasing their effectiveness in live environments and their adaptability to different types of cyberthreats. The presentation concludes with insights into future research directions and opportunities for further innovation in AI-driven cybersecurity solutions, aiming to improve their reliability, security, and user trust.

© *Marek Pawlicki*

SR 03

30th July

15:00

Joseph Squillace

Penn State Schuylkill, USA

The State of Cybersecurity Today – Exploring the Effectiveness of Cybersecurity Defenses through a Pedagogical Lenses

In today's interconnected digital world, effective cybersecurity defense is paramount to safeguarding information privacy against evolving threats while preserving the data integrity of critical infrastructure, national security, and academic institutions. Ensuring information security concerns are addressed is vital to maintaining a strategic position of cybersecurity readiness today, however, there is a fundamental challenge in how the education is being presented and received. With the pervasive use of technology and the increasing threats in cyberspace, there is a pressing need to reimagine the requisite cybersecurity skills and robust knowledge needed by users, beginning with challenging the traditional pedagogical model used when implementing (cyber) Security Education Training and Awareness (SETA).

Focusing on the pedagogy, the theory and practice of learning, and how this process influences, and is influenced by, the social, political, and psychological development of learners, we begin to better understand why the current cyber education model is ineffective, and what can be done as educators to improve the failed system. Supportive research data highlighting more effective ways to teach cyber education will help identify strategies for enhancing cyber defenses. In addition, collaborative discussions revolving around how academic research can improve our defensive security posture across industries and domains will help facilitate the defensive changes needed.

© Joseph Squillace

SR 05

1st Aug.

8:45

Martin Husák

Masaryk University, Czech Republic

Theory and Practice of Cybersecurity Knowledge Graphs and Further Steps

The keynote surveys the growing adoption of knowledge graphs in cybersecurity and explores their potential in cybersecurity research and practice. By structuring and interlinking vast amounts of cybersecurity data, knowledge graphs offer increasing capabilities for incident response and cyber situational awareness. They enable a holistic view of the protected cyber infrastructures and threat landscapes, facilitating advanced analytics, automated reasoning, vulnerability management, and attack mitigation. We expect the cybersecurity knowledge graphs to assist incident handlers in day-to-day cybersecurity operations as well as strategic network security management. We may see emerging tools for decision support based on knowledge graphs that will leverage continuous data collection. A knowledge graph filled with the right data at the right time can significantly reduce the workload of incident handlers. We may even see rapid changes in incident handling tools and workflows leveraging the knowledge graphs, especially when combined with emerging technologies of generative AI and large language models that will facilitate interactions with the knowledge bases or generate reports of security situations. However, the implementation of cybersecurity knowledge graphs is challenging. Ensuring the quality of the underlying data is a serious concern for researchers and practitioners. Only accurate, complete, and updated data can ensure the reliability of the knowledge graph, leading to good insights and decisions. Additionally, the dynamic nature of cyber threats necessitate continuous data updates and rigorous validation processes.

© *Martin Husak*

SRS 05

1st Aug.

14:45

Svetlana Boudko

Norwegian Computing Center, Oslo, Norway

Where federated learning meets homomorphic encryption: challenges and potential pathways for secure data sharing in AI applications

To ensure data consistency and control, data centralization is a preferred solution for training machine learning models. However, data protection regulations, e.g. GDPR, as well as industrial competition, impose restrictions on information sharing among different organizations and individuals. Furthermore, this approach is technically challenging since the cost of collecting, storing, and processing all data in one centralized location is often prohibitively high. Google proposed federated learning for the collaborative training of machine learning models, aiming to handle the exchange of privacy-sensitive information in distributed environments and to reduce data transmission costs. In contrast to traditional machine learning, federated learning does not require local data to be collected, stored, and processed on a central server. Instead, this method enables on-device model training using client-specific data, with the obtained local model updates further aggregated on a central server. However, federated learning is not without its own privacy concerns, including risks of data leakage and inference attacks. To address these challenges, research is being conducted into various strategies, such as homomorphic encryption. By combining federated learning and homomorphic encryption, we can train machine learning models on encrypted data from different sources, thereby ensuring better data protection. The model never sees the raw data, only the encrypted version, and yet it can still learn from it. However, homomorphic encryption is computationally intensive and can significantly slow down the training process. In this talk, I look at the issues and prospects arising from the intersection of federated learning and multi-key homomorphic encryption, two advanced techniques in the field of secure and collaborative machine learning.

© Svetlana Boudko

SR 06

30th July

13:00

Sabarathinam Chockalingam

Institute for Energy Technology (IFE), Norway

Dynamic Risk Assessment for Industry 4.0

In the age of Industry 4.0, the integration of cyber-physical systems within industrial control environments presents significant opportunities alongside critical challenges, particularly in ensuring resilience. This talk, “Dynamic Risk Assessment for Industry 4.0,” explores advanced methodologies for dynamic and adaptive risk assessment to address risks arising from both intentional and accidental root causes. By providing an overview of dynamic and adaptive risk assessment methods, we delve into the synergy of probabilistic techniques and expert insights to construct comprehensive risk models. These models are illustrated through realistic examples, demonstrating their suitability in various scenarios. Drawing on comprehensive research and advanced frameworks, this talk highlights the importance of adaptive, integrated approaches to risk assessment, ensuring the resilience of critical industrial systems in an increasingly interconnected world.

© Sabarathinam Chockalingam

SR 06

30th July

10:30

Emma Østerbø

NCE Manufacturing (Norwegian Centre of Expertise), Norway

Engaging SMEs in the twin transition

Most manufacturing SMEs do not have the time and/or resources to do the research, translate the results to "better business" and at the same time avoid risk connected to implementation of new technology. The times we live in is just overwhelming in so many ways, that some stick their head in the sand, hope for the best and go on with their traditional business. In Norway, as in other places in Europe, many of these companies are corner stones of their local village. If they do not make it through the current industrial revolution, the crisis is much bigger for Norway than for the company itself. Norwegian Catapult is designed to provide competence and test infrastructure so SMEs can evolve, continue their business, or start new ones, and continue to contribute to a more resilient and sustainable society. In this keynote the CEO of Manufacturing Technology Norwegian Catapult will talk about the experience of finding the key to how to help SMEs finding ways to start or improve manufacturing business in one of the most expensive countries in the world.

© *Emma Østerbø*

SR 08

30th July

15:00

Heribert Vallant

JOANNEUM RESEARCH, Graz, Austria

IoT Discovery as the fundamental basis for AI guided penetration testing

Industrial IoT (IIoT) is an essential element in the context of Industry 4.0, with the aim of making the best possible use of machine operating times for a wide range of production batch sizes along the entire product engineering process. The cyber threat landscape associated with IoT is diverse, rapidly evolving, and has an enormous impact on the security of production facilities and the protection of corporate know-how. A major challenge for the definition of effective security measures in the IoT environment are the high level of complexity, which results from the variety of application areas for IoT. Identifying the assets to be secured in a complex system can be performed manually, using e.g. threat modeling, which aims to identify potential threats and vulnerabilities based on the architecture of the IT/OT system in question. Nevertheless, the dynamic and agile development in the manufacturing domain makes it challenging to secure industrial automation and control systems throughout their lifecycle. Penetration testing, a key mechanism for improving resilience preparedness usually involves manual procedures in the process. To answer to new challenges, automated testing using machine learning methods have become a rapidly emerging field, which puts this kind of testing to the next level.

This talk focuses on the challenges related to complex and dynamic IIoT environments and automated solutions for new devices discovery and AI guided pen testing in such an environment, based on the status of system at a given time - just a snapshot - not all (IoT) components of the CPS may be up and running.

SR 08

30th July

13:00

Petr Svenda

Masaryk University, Czech Republic

On value of large-scale blackbox analysis of software and hardware cryptographic implementations

The security analysis of cryptographic implementations is vital for building secure systems atop core hardware components. Yet, it is also frequently more challenging to assess due to the general closeness of the hardware industry. The resulting black box analysis is typically more complicated to set up, execute, and interpret the observed results. If analyzing only a single device, the likelihood of ending empty-handed is high – the situation not favorable for academic researchers, further decreasing the pool of people motivated to perform independent security analysis. The talk will present lessons learned from large-scale analysis of cryptographic smartcards, Trusted Platform Modules, cryptographic libraries, and cryptocurrency hardware wallets performed over the past decade, which resulted in several high-profile, responsibly disclosed vulnerabilities against RSA and ECC implementations. Such an analysis approach increases the likelihood of a successful attack being found and provides realistic inputs for designing new attack methods. Additionally, the results obtained from all devices can be used to reason about the situation and weaknesses of the whole ecosystem instead of just reporting a single vulnerable device.

© *Petr Svenda*

SR 05

31st July

10:45

Dr Virginia Franqueira

University of Kent, UK

Fighting sexual abuse and exploitation of children

The number of reported victims of Child Sexual Abuse and Exploitation (CSA/CSE) continues to grow worldwide. For example, the WeProtect Global Alliance's Global Threat Assessment 2023 indicates a growth of 87% on the number of CSA/CSE reports since 2019 and the likelihood of a much larger number, since a lot of child exploitation and online abuse remains undetected. The HEROES project (Novel Strategies to Fight Child Sexual Exploitation and Human Trafficking Crimes and Protect Their Victims)[1] and the ALUNA project (Child Protection Centred Strategies to Fight against Sexual Abuse and Exploitation)[2] , both funded by the European Commission, address this growing problem from a prevention, investigation and victims assistance perspectives. Taking a multidisciplinary approach, HEROES and ALUNA develop technical tools, best practices and strategies to equip law enforcement agencies (LEAs), legal stakeholders, non-government organisations (NGOs) and the public with better capabilities for CSA/CSE reporting, prosecution and detection – within and beyond Europe. This talk will provide an overview of some of the tools being developed, and will also lay the foundation for discussion about the emerging challenge of AI-generated CSA/CSE.

[1] https://heroes-fct.eu/

[2] https://www.aluna-isf.eu/

© *Dr Virginia Franqueira*

Accepted Paper Overview

ARES Best Paper Session:

1.8.24 13:15 – 14:15, Room HS01

Provably Secure Communication Protocols for Remote Attestation
Johannes Wilson (Sectra Communications; Linköping University, Sweden), Mikael Asplund (Linköping University, Sweden), Niklas Johansson (Sectra Communications; Linköping University, Sweden), Felipe Boeira (Linköping University, Sweden)

Let the Users Choose: Low Latency or Strong Anonymity? Investigating Mix Nodes with Paired Mixing Techniques
Sarah Abdelwahab Gaballah (Ruhr University Bochum, Germany), Lamya Abdullah (Technical University of Darmstadt, Germany), Max Mühlhäuser (Technical University of Darmstadt, Germany), Karola Marky (Ruhr University Bochum, Germany)

BenchIMP: A Benchmark for Quantitative Evaluation of the Incident Management Process Assessment
Alessandro Palma (Sapienza University of Rome, Italy), Nicola Bartoloni (Sapienza University of Rome, Italy), Marco Angelini (Link Campus University of Rome, Italy)

ARES I:

31.7.24 8:45 – 10:15, Room HS01

A Privacy Measure Turned Upside Down?
Investigating the Use of HTTP Client Hints on the Web
Stephan Wiefling (swiefling.de, Germany), Marian Hönscheid (H-BRS University of Applied Sciences, Germany), Luigi Lo Iacono (H-BRS University of Applied Sciences, Germany)

Privacy Preserving Release of Mobile Sensor Data
Rahat Masood (UNSW Sydney, Australia), Wing Yan Cheng (UNSW Sydney, Australia), Dinusha Vatsalan (Macquarie University, Australia), Deepak Mishra (UNSW Sydney, Australia), Hassan Jameel Asghar (Macquarie University, Australia), Dali Kaafar (Macquarie University, Australia)

Compromising anonymity in identity-reserved k-anonymous datasets through aggregate knowledge
Kevin De Boeck (KU Leuven - DistriNet, Belgium), Jenno Verdonck (KU Leuven - DistriNet, Belgium), Michiel Willocx (KU Leuven - DistriNet, Belgium), Jorn Lapon (KU Leuven - DistriNet, Belgium), Vincent Naessens (KU Leuven - DistriNet, Belgium)

Continuous Authentication Leveraging Matrix Profile
Luis Ibanez-Lissen (Universidad Carlos III de Madrid, Spain), Jose Maria de Fuentes (Universidad Carlos III de Madrid, Spain), Lorena González Manzano (Universidad Carlos III de Madrid, Spain), Nicolas Anciaux (Inria, France)

ARES II:

31.7.24 10:45 – 12:15, Room HS01

Hardware Trust Anchor Authentication for Updatable IoT Devices
Dominik Lorych (Fraunhofer SIT | ATHENE, Germany), Christian Plappert (Fraunhofer SIT | ATHENE, Germany)

SECURA: Unified Reference Architecture for Advanced Security and Trust in Safety Critical Infrastructures
Michael Eckel (Fraunhofer SIT | ATHENE, Germany), Sigrid Gürgens (Fraunhofer SIT | ATHENE, Germany)

Dealing with Bad Apples: Organizational Awareness and Protection for Bit-flip and Typo-Squatting Attacks
Huancheng Hu (Hasso Plattner Institute & University of Potsdam, Germany), Afshin Zivi (Hasso Plattner Institute & University of Potsdam, Germany), Christian Doerr (Hasso Plattner Institute & University of Potsdam, Germany)

Attack Analysis and Detection for the Combined Electric Vehicle Charging and Power Grid Domains
Dustin Kern (Darmstadt University of Applied Sciences, Germany), Christoph Krauß (Darmstadt University of Applied Sciences, Germany), Matthias Hollick (TU Darmstadt, Germany)

ARES III:

31.7.24 13:15 – 14:45, Room HS01

Subjective Logic-based Decentralized Federated Learning for Non-IID Data
Agnideven Palanisamy Sundar (Indiana University - Purdue University - Indianapolis, United States), Feng Li (IUPUI, United States), Xukai Zou (Indiana University Purdue University Indianapolis, United States), Tianchong Gao (Southeast University, China)

Let Them Drop: Scalable and Efficient Federated Learning Solutions Agnostic to Stragglers
Riccardo Taiello (Inria Sophia Antipolis - EURECOM - University Cote d'Azur, France), Melek Önen (EURECOM, France), Clémentine Gritti (EURECOM, France), Marco Lorenzi (Inria Sophia Antipolis - University Cote d'Azur, France)

GNN-IDS: Graph Neural Network based Intrusion Detection System
Zhenlu Sun (Department of Information Technology, Uppsala University, Sweden), André Teixeira (Department of Information Technology, Uppsala University, Sweden), Salman Toor (Department of Information Technology, Uppsala University, Sweden)

Prov2vec: Learning Provenance Graph Representation for Anomaly Detection in Computer Systems
Bibek Bhattarai (Intel, United States), H. Howie Huang (George Washington University, Washington DC, United States)

ARES IV:

31.7.24 15:15 – 16:45, Room HS01

Mealy Verifier: An Automated, Exhaustive, and Explainable Methodology for Analyzing State Machines in Protocol Implementations
Arthur Tran Van (Télécom SudParis, France), Olivier Levillain (Télécom SudParis, France), Herve Debar (Télécom SudParis, France)

Monitor-based Testing of Network Protocol Implementations Using Symbolic Execution
Hooman Asadian (Uppsala University, Sweden), Paul Fiterau-Brostean (Uppsala University, Sweden), Bengt Jonsson (Uppsala University, Sweden), Konstantinos Sagonas (Uppsala University & NTUA, Sweden)

Towards Secure Virtual Elections: Multiparty Computation of Order Based Voting Rules
Tamir Tassa (The Open University of Israel, Israel), Lihi Dery (Ariel University, Israel)

Investigating HTTP Covert Channels Through Fuzz Testing
Kai Hölk (FernUniversität in Hagen, Germany), Wojciech Mazurczyk (Warsaw University of Technology, Poland), Marco Zuppelli (Institute for Applied Mathematics and Information Technologies, Italy), Luca Caviglione (CNR - IMATI, Italy)

ARES V:

1.8.25 08:45 – 10:15, Room HS01

From Code to EM Signals:
A Generative Approach to Side Channel Analysis-based Anomaly Detection
Kurt A. Vedros (University of Idaho, United States), Constantinos Kolias (University of Idaho, United States), Daniel Barbara (George Mason University, United States), Robert Ivans (Idaho National Laboratory, United States)

Towards Reducing Business-Risk of Data Theft Implementing Automated Simulation Procedures of Evil Data Exfiltration
Michael Mundt (Esri Deutschland GmbH, Germany), Harald Baier (Universität der Bundeswehr München, Research Instiute CODE, Germany), Antje Raab-Düsterhöft (Hochschule Wismar, Germany)

SECL: A Zero-Day Attack Detector and Classifier based on Contrastive Learning and Strong Regularization
Robin Duraz (Chaire of Naval Cyberdefense, Lab-STICC, France), David Espes (University of Brest, Lab-STICC, France), Julien Francq (Naval Group (Naval Cyber Laboratory, NCL), France), Sandrine Vaton (IMT Atlantique, Lab-STICC, France)

Graph-Based Spectral Analysis for Detecting Cyber Attacks
Majed Jaber (Laboratory of research of EPITA (LRE), France), Nicolas Boutry (EPITA Research Laboratory (LRE), Le Kremlin-Bicêtre, France., France), Pierre Parrend (EPITA Strasbourg, France)

ARES VI:

1.8.25 10:45 – 12:15, Room HS01

Security Analysis of a Decentralized, Revocable and Verifiable Attribute Based Encryption Scheme
Thomas Prantl (Julius-Maximilians-Universität Würzburg, Germany), Marco Lauer (Julius-Maximilians-Universität Würzburg, Germany), Lukas Horn (Julius-Maximilians-Universität Würzburg, Germany), Simon Engel (Julius-Maximilians-Universität Würzburg, Germany), David Dingel (Julius-Maximilians-Universität Würzburg, Germany), André Bauer (University Chicago, United States), Christian Krupitzer (University of Hohenheim, Germany), Samuel Kounev (Julius-Maximilians-Universität Würzburg, Germany)

Secure Noise Sampling for DP in MPC with Finite Precision
Hannah Keller (Aarhus University, Denmark), Helen Möllering (McKinsey & Company, Germany), Thomas Schneider (Technical University of Darmstadt, Germany), Oleksandr Tkachenko (DFINITY Foundation, Germany), Liang Zhao (Technical University of Darmstadt, Germany)

Comparative Analysis and Implementation of Jump Address Masking for Preventing TEE Bypassing Fault Attacks
Shoei Nashimoto (Mitsubishi Electric Corporation, Japan), Rei Ueno (Tohoku University, Japan), Naofumi Homma (Tohoku University, Japan)

Extracting Randomness from Nucleotide Sequencers for use in a Decentralised Randomness Beacon
Darren Hurley-Smith (Royal Holloway University of London, United Kingdom), Alastair Droop (University of York, United Kingdom), Remy Lyon (Veiovia Ltd., United Kingdom), Roxana Teodor (Veiovia Ltd., United Kingdom)

ARES VII:

1.8.25 14:45 – 16:15, Room HS01

Unveiling Vulnerabilities in Bitcoin's Misbehavior-Score Mechanism: Attack and Defense
Yuwen Zou (Xi'an Jiaotong-Liverpool University, China), Wenjun Fan (Xi'an Jiaotong-Liverpool University, China), Zhen Ma (Xi'an Jiaotong-Liverpool University, China)

A Large-Scale Study on the Prevalence and Usage of TEE-based Features on Android
Davide Bove (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany)

HeMate: Enhancing Heap Security through Isolating Primitive Types with Arm Memory Tagging Extension
Yu-Chang Chen (National Taiwan University, Taiwan), Shih-Wei Li (National Taiwan University, Taiwan)

A Metalanguage for Dynamic Attack Graphs and Lazy Generation
Viktor Engström (KTH Royal Institute of Technology, Sweden), Giuseppe Nebbione (KTH Royal Institute of Technology, Sweden), Mathias Ekstedt (KTH Royal Institute of Technology, Sweden)

ARES VIII:

1.8.25 14:45 – 16:15, Room SR03

On the effectiveness of Large Language Models for GitHub Workflows
Xinyu Zhang (Purdue University, United States), Siddharth Muralee (Purdue University, United States), Sourag Cherupattamoolayil (Purdue University, United States), Aravind Machiry (Purdue University, United States)

Adversary Tactic Driven Scenario and Terrain Generation with Partial Infrastructure Specification
Ádám Ruman (Masaryk University, Czechia), Martin Drašar (Masaryk University, Czechia), Lukáš Sadlek (Masaryk University, Czechia), Shanchieh Jay Yang (Rochester Institute of Technology, United States), Pavel Čeleda (Masaryk University, Czechia)

Digital Forensic Artifacts of FIDO2 Passkeys in Windows 11
Patricio Domingues (Polytechnic Institute of Leiria, Portugal), Miguel Frade (Polytechnic Institute of Leiria, Portugal), Miguel Negrao (Polytechnic Institute of Leiria, Portugal)

Increasing the Confidence in Security Assurance Cases using Game Theory
Antonia Welzel (Chalmers | University of Gothenburg, Sweden), Rebekka Wohlrab (Chalmers | University of Gothenburg, Sweden), Mazen Mohamad (Chalmers | University of Gothenburg, Sweden)

ARES SoK:

1.8.24 08:45 – 10:15, Room SR03

SoK: A Comparison of Autonomous Penetration Testing Agents
Raphael Simon (Royal Military Academy, Belgium), Wim Mees (Royal Military Academy, Belgium)

SoK: Federated Learning based Network Intrusion Detection in 5G: Context, state of the art and challenges
Sara Chennoufi (SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, Palaiseau, France), Gregory Blanc (SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, Palaiseau, France), Houda Jmila (Institute LIST, CEA, Paris-Saclay University, Palaiseau, France), Christophe Kiennert (SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, Palaiseau, France)

SoK: A Unified Data Model for Smart Contract Vulnerability Taxonomies
Claudia Ruggiero (Sapienza Università di Roma, Italy), Pietro Mazzini (Sapienza Università di Roma, Italy), Emilio Coppa (LUISS University, Italy), Simone Lenti (Sapienza Università di Roma, Italy), Silvia Bonomi (Sapienza Università di Roma, Italy)

SoK: How Artificial-Intelligence Incidents Can Jeopardize Safety and Security
Richard May (Harz University of Applied Sciences, Germany), Jacob Krüger (Eindhoven University of Technology, Netherlands), Thomas Leich (Harz University of Applied Sciences, Germany)

SoK: Visualization-based Malware Detection Techniques
Matteo Brosolo (University of Padua, Italy), Vinod Puthuvath (University of Padua, Italy), Asmitha Ka (Cochin University of Science and Technology, Kochi, Kerala, India), Rafidha Rehiman (Cochin University of Science and Technology, Kochi, Kerala, India), Mauro Conti (University of Padua, Italy)

ARES Short:

1.8.24 10:45 – 12:15, Room SR03

Sybil Attack Strikes Again: Denying Content Access in IPFS with a Single Computer
Thibault Cholez (University of Lorraine, CNRS, Inria, LORIA, France), Claudia Ignat (University of Lorraine, CNRS, Inria, LORIA, France)

Combinatorial Testing Methods for Reverse Engineering Undocumented CAN Bus Functionality
Christoph Wech (SBA Research, Austria), Reinhard Kugler (SBA Research, Austria), Manuel Leithner (SBA Research, Austria), Dimitris E. Simos (SBA Research, Austria)

Is Personalization Worth It? Notifying Blogs about a Privacy Issue Resulting from Poorly Implemented Consent Banners

Theresa Kriecherbauer (Ludwig Maximilian University, Germany), Richard Schwank (Technical University of Munich, Germany), Adrian Krauss (Technical University of Munich, Germany), Konstantin Neureither (Technical University of Munich, Germany), Lian Remme (Heinrich Heine University, Germany), Melanie Volkamer (Karlsruhe Institute of Technology, Germany), Dominik Herrmann (University of Bamberg, Germany)

Confidence-Aware Fault Trees

Alexander Günther (Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau, Germany), Peter Liggesmeyer (Technical University of Kaiserslautern, Germany), Sebastian Vollmer (Technical University of Kaiserslautern, Germany)

Reverse Engineered MiniFS File System

Dmitrii Belimov (Technology Innovation Institute, United Arab Emirates), Evgenii Vinogradov (Technology Innovation Institute, United Arab Emirates)

ASOD:

2.8.24 11:00 – 12:30, Room SR04

SoK: Automated Software Testing for TLS Libraries

Ben Swierzy (University of Bonn, Germany), Felix Boes (University of Bonn, Germany), Timo Pohl (University of Bonn, Germany), Christian Bungartz (University of Bonn, Germany), Michael Meier (University of Bonn, Fraunhofer FKIE, Germany)

Accuracy Evaluation of SBOM Tools for Web Applications and System-Level Software

Andreas Halbritter (Augsburg Technical University of Applied Sciences Institute for Innovative Safety and Security, Germany), Dominik Merli (Augsburg Technical University of Applied Sciences Institute for Innovative Safety and Security, Germany)

Enhancing Secure Deployment with Ansible: A Focus on Least Privilege and Automation for Linux

Eddie Billoir (IRIT, Université de Toulouse, CNRS, Toulouse INP, UT3, AIRBUS Protect, France), Romain Laborde (IRIT, Université de Toulouse, CNRS, Toulouse INP, UT3, France), Ahmad Samer Wazan (Zayed University, France), Yves Rutschle (AIRBUS Protect, France), Abdelmalek Benzekri (IRIT, Université de Toulouse, CNRS, Toulouse INP, UT3, France)

BASS I:

2.8.24 09:00 – 10:30, Room SR03

Behavioural Modelling for Sustainability in Smart Homes
Luca Ardito (Politecnico di Torino, Italy)

BASS II:

2.8.24 11:00 – 12:30, Room SR03

A Web Browser Plugin for Users' Security Awareness
Thomas Hoad (University of Southampton, United Kingdom), Erisa Karafili (University of Southampton, United Kingdom)

A tool for IoT Firmware Certification
Giuseppe Marco Bianco (Politecnico di Torino, Italy), Luca Ardito (Politecnico di Torino, Italy), Michele Valsesia (Politecnico di Torino, Italy)

Analysis of the Windows Control Flow Guard
Niels Pfau (Institute of IT Security Research, St. Pölten University of Applied Sciences, Austria), Patrick Kochberger (Institute of IT Security Research, St. Pölten University of Applied Sciences, Austria)

BASS III:

2.8.24 13:30 – 15:00, Room SR03

Image-based detection and classification of Android malware through CNN models
Alessandro Aldini (University of Urbino Carlo Bo, Italy), Tommaso Petrelli (University of Urbino Carlo Bo, Italy)

If It Looks Like a Rootkit and Deceives Like a Rootkit: A Critical Examination of Kernel-Level Anti-Cheat Systems
Christoph Dorner (St. Pölten University of Applied Sciences, Austria), Lukas Daniel Klausner (St. Pölten University of Applied Sciences, Austria)

Systematic Analysis of Label-flipping Attacks against Federated Learning in Collaborative Intrusion Detection Systems
Léo Lavaur (IMT Atlantique / IRISA-SOTERN / Cyber CNI, France), Yann Busnel (IMT Nord Europe / IRISA-SOTERN, France), Fabien Autrel (IMT Atlantique / IRISA-SOTERN, France)

CSA I:

1.8.24 08:45 – 10:15, Room SR04

Operation Assessment in cyberspace: Understanding the effects of Cyber Deception
Salvador Llopis Sanchez (Universitat Politecnica de Valencia, Spain), David Lopes Antunes (Universitat Politecnica de Valencia, Spain)

PQ-REACT: Post Quantum Cryptography Framework for Energy Aware Contexts
Marta Irene Garcia Cid (Indra, Spain), Kourtis Michail-Alexandros (National Centre for Scientific Research "DEMOKRITOS", Greece), David Domingo (Indra Sistemas de Comunicaciones Seguras, Spain), Nikolay Tcholtchev (Fraunhofer Institute for Open Communication Systems, Germany), Vangelos K. Markakis (Hellenic Mediterranean University, Greece), Marcin Niemiec (AGH University, Poland), Juan Pedro Brito Mendez (Universidad Politécnica de Madrid, Spain), Laura Ortiz (Universidad Politécnica de Madrid, Spain), Vicente Martin (Universidad Politécnica de Madrid, Spain), Diego Lopez (Telefonica Investicacion y Desarrollo, Spain), George Xilouris (National Centre for Scientific Research "DEMOKRITOS", Greece), Maria Gagliardi (Scuola Superiore Sant'Anna, Italy), Jose Gonzalez (MTU Autralo Alplha Lab, Estonia), Miguel Garcia (Splorotech S.L., Spain), Giovanni Comande (SMARTEX SRL, Italy), Nikolai Stoianov (Bulgarian Defence Institute, Bulgaria)

RMF: A Risk Measurement Framework for Machine Learning Models
Jan Schröder (Fraunhofer FOKUS and HTW Berlin, Germany), Jakub Breier (TTControl GmbH, Austria)

CSA II:

1.8.24 10:45 – 12:15, Room SR04

NEWSROOM: Towards Automating Cyber Situational Awareness Processes and Tools for Cyber Defence

Markus Wurzenberger (AIT Austrian Institute of Technology GmbH, Austria), Stephan Krenn (AIT Austrian Institute of Technology GmbH, Austria), Max Landauer (AIT Austrian Institute of Technology, Austria), Florian Skopik (AIT Austrian Institute of Technology, Austria), Cora Perner (Airbus, Germany), Jarno Lötjönen (Jamk University of Applied Sciences, Finland), Jani Päijänen (Jamk University of Applied Sciences, Finland), Georgios Gardikis (Space Hellas S.A., Greece), Nikos Alabasis (Space Hellas S.A., Greece), Liisa Sakerman (Sihtasutus CR14, Estonia), Fredi Arro (Sihtasutus CR14, Estonia), Kristiina Omri (CybExer Technologies OÜ, Estonia), Aare Reintam (CybExer Technologies OÜ, Estonia), Juha Röning (University of Oulu, Finland), Kimmo Halunen (University of Oulu, Finland), Romain Ferrari (ThereSIS, Thales SIX GTS, France), Vincent Thouvenot (ThereSIS, Thales SIX GTS, France), Martin Weise (TU Wien, Austria), Andreas Rauber (TU Wien, Austria), Vasileios Gkioulos (Norwegian University of Science and Technology, Norway), Sokratis Katsikas (Norwegian University of Science and Technology, Norway), Luigi Sabetta (LeonardoLabs (Leonardo spa), Italy), Jacopo Bonato (LeonardoLabs (Leonardo spa), Italy), Rocío Ortíz (INDRA, Spain), Daniel Navarro (INDRA, Spain), Nikolaos Stamatelatos (Logstail, Greece), Ioannis Avdoulas (Logstail, Greece), Rudolf Mayer (University of Vienna, Austria), Andreas Ekelhart (University of Vienna, Austria), Ioannis Giannoulakis (Eight Bells Ltd, Cyprus), Emmanouil Kafetzakis (Eight Bells Ltd, Cyprus), Antonello Corsi (CY4GATE SpA, Italy), Ulrike Lechner (Universität der Bundeswehr München, Germany), Corinna Schmitt (Universität der Bundeswehr München, FI CODE, Germany)

Evaluation of Cyber Situation Awareness – Theory, Techniques and Applications

Georgi Nikolov (Royal Military School Brussels, Belgium), Axelle Perez (Université libre de Bruxelles, Belgium), Wim Mees (Royal Military Academy Brussels, Belgium)

Exploring the influence of the choice of prior of the Variational Auto-Encoder on cybersecurity anomaly detection

Tengfei Yang (Software Research Institute, Technological University of the Shannon: Midlands Midwest, Ireland), Yuansong Qiao (Software Research Institute, Technological University of the Shannon: Midlands Midwest, Ireland), Brian Lee (Software Research Institute, Technological University of the Shannon: Midlands Midwest, Ireland)

Analyzing Air-traffic Security using GIS-``blur" with Information Flow Control in the IIIf
Florian Kammueller (Middlesex University London and TU Berlin, United Kingdom)

CSA III:

1.8.24 14:45 – 16:15, Room SR04

On the Application of Natural Language Processing for Advanced OSINT Analysis in Cyber Defence
Florian Skopik (AIT Austrian Institute of Technology, Austria), Benjamin Akhras (AIT Austrian Institute of Technology, Austria), Elisabeth Woisetschlaeger (AIT Austrian Institute of Technology, Austria), Medina Andresel (AIT Austrian Institute of Technology, Austria), Markus Wurzenberger (AIT Austrian Institute of Technology, Austria), Max Landauer (AIT Austrian Institute of Technology, Austria)

Evaluating the impact of contextual information on the performance of intelligent continuous authentication systems
Pedro Miguel Sánchez Sánchez (Department of Information and Communications Engineering, University of Murcia, Spain), Adrián Abenza Cano (Department of Information and Communications Engineering, University of Murcia, Spain), Alberto Huertas Celdrán (Communication Systems Group CSG, Department of Informatics, University of Zurich, Switzerland), Gregorio Martínez Pérez (Department of Information and Communications Engineering, University of Murcia, Spain)

Unlocking the Potential of Knowledge Graphs: A Cyber Defense Ontology for a Knowledge Representation and Reasoning System
José María Jorquera Valero (University of Murcia, Spain), Antonio López Martínez (University of Murcia, Spain), Pedro Miguel Sánchez Sánchez (University of Murcia, Spain), Daniel Navarro Martínez (Indra Digital Labs, Spain), Rodrigo Varas López (Indra Digital Labs, Spain), Javier Ignacio Rojo Lacal (Indra Digital Labs, Spain), Antonio López Vivar (Indra Digital Labs, Spain), Marco Antonio Sotelo Monge (Indra Digital Labs, Spain), Manuel Gil Pérez (University of Murcia, Spain), Gregorio Martínez Pérez (University of Murcia, Spain)

A Technical Exploration of Strategies for Augmented Monitoring and Decision Support in Information Warfare
Frida Muñoz Plaza (Indra, Spain), Inés Hernández San Román (Indra, Spain), Marco Antonio Sotelo Monge (Indra, Spain)

CUING I:

31.7.24 8:45 – 10:15, Room SR08

Are Deepfakes a Game-changer in Digital Images Steganography Leveraging the Cover-Source-Mismatch?

Arthur Méreur (Troyes University of Technology, France), Antoine Mallet (Troyes University of Technology, France), Rémi Cogranne (Troyes University of Technology, France)

Trustworthiness and explainability of a watermarking and machine learning-based system for image modification detection to combat disinformation

Andrea Rosales (Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya, Spain), Agnieszka Malanowska (Warsaw University of Technology, Poland), Tanya Koohpayeh Araghi (Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya, Barcelona, Spain, Spain), Minoru Kuribayashi (Center for Data-driven Science and Artificial Intelligence at Tohoku University Japan, Japan), Marcin Kowalczyk (Warsaw University of Technology, Poland), Daniel Blanche-Tarragó (Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya, Center, Spain), Wojciech Mazurczyk (Warsaw University of Technology, Poland), David Megías (Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya, Barcelona, Spain, Spain)

CUING II:

31.7.24 10:45 – 12:15, Room SR08

A Comprehensive Pattern-based Overview of Stegomalware

Fabian Strachanski (University of Duisburg-Essen, Germany), Denis Petrov (Worms University of Applied Sciences, Germany), Tobias Schmidbauer (Nuremberg Institute of Technology, Germany), Steffen Wendzel (Worms University of Applied Sciences, Germany)

No Country for Leaking Containers:
Detecting Exfiltration of Secrets Through AI and Syscalls

Marco Zuppelli (Institute for Applied Mathematics and Information Technologies, Italy), Massimo Guarascio (ICAR-CNR, Italy), Luca Caviglione (CNR - IMATI, Italy), Angelica Liguori (ICAR-CNR, Italy)

Robust and Homomorphic Covert Channels in Streams of Numeric Data
Jörg Keller (FernUniversität in Hagen, Germany), Carina Heßeling (FernUniversitaet Hagen, Germany), Steffen Wendzel (Worms University of Applied Sciences, Germany)

A Case Study on the Detection of Hash-Chain-based Covert Channels Using Heuristics and Machine Learning
Jeff Schymiczek (University of Helsinki, Finland), Tobias Schmidbauer (Nuremberg Institute of Technology, Germany), Steffen Wendzel (Worms University of Applied Sciences, Germany)

CUING III:

31.7.24 13:15 – 14:45, Room SR08

Natural Language Steganography by ChatGPT
Martin Steinebach (Fraunhofer, Germany)

Single-image steganalysis in real-world scenarios based on classifier inconsistency detection
Daniel Lerch-Hostalot (Universitat Oberta de Catalunya, Spain), David Megías Jimenez (Universitat Oberta de Catalunya, Spain)

How to evade modern web cryptojacking detection tools? A review of practical findings
Pawel Rajba (University of Wroclaw, Poland), Krzysztof Chmiel (University of Wroclaw, Poland)

ZW-IDS: Zero-Watermarking-based network Intrusion Detection System using data provenance
Omair Faraj (Telecom SudParis, Institut Polytechnique de Paris, France), David Megias (Internet Interdisciplinary Institute, Universitat Oberta de Catalunya, Spain), Joaquin Garcia-Alfaro (Telecom SudParis, Institut Polytechnique de Paris, France)

EDiD I:

31.7.24 8:45 – 10:15, Room SR07

An Identity Key Management System with Deterministic Key Hierarchy for SSI-native Internet of Things
Alice Colombatto (LINKS Foundation, Italy), Luca Giorgino (LINKS Foundation, Italy), Andrea Vesco (LINKS Foundation, Italy)

Service Provider Accreditation: Enabling and Enforcing Privacy-by-Design in Credential-based Authentication Systems
Stefan More (Graz University of Technology and Secure Information Technology Center Austria (A-SIT), Austria), Jakob Heher (Graz University of Technology and Secure Information Technology Center Austria (A-SIT), Austria), Edona Fasllija (Graz University of Technology and Secure Information Technology Center Austria (A-SIT), Austria), Maximilian Mathie (Graz University of Technology, Austria)

EDiD II:

31.7.24 10:45 – 12:15, Room SR07

Long-Lived Verifiable Credentials: Ensuring Durability Beyond the Issuer's Lifetime
Ricardo Bochnia (HTW Dresden, Germany), Jürgen Anke (HTW Dresden, Germany)

Towards Post-Quantum Verifiable Credentials
Tim Wood (Digital Catapult, United Kingdom), Keerthi Thomas (Digital Catapult, United Kingdom), Matthew Dean (Digital Catapult, United Kingdom), Swaminathan Kannan (Digital Catapult, United Kingdom), Robert Learney (Digital Catapult, United Kingdom)

Towards Functions for Verifiable Credentials in a 2-Holder Model
Markus Batz (Stadt Köln, Germany), Sebastian Zickau (Stadt Köln, Germany)

DistIN: Analysis and Validation of a Concept and Protocol for Distributed Identity Information Networks
Michael Hofmeier (University of the Bundeswehr Munich, Germany), Daniela Pöhn (University of the Bundeswehr Munich, Germany), Wolfgang Hommel (University of the Bundeswehr Munich, Germany)

ENS II:

30.7.24 15:00 – 16:30, Room SR07

Leveraging Overshadowing for Time-Delay Attacks in 4G/5G Cellular Networks: An Empirical Assessment

Virgil Hamici-Aubert (IMT Atlantique, IRISA, UMR CNRS 6074, France), Julien Saint-Martin (IMT Atlantique, IRISA, UMR CNRS 6074, France), Renzo E. Navas (IMT Atlantique, IRISA, UMR CNRS 6074, France), Georgios Z. Papadopoulos (IMT Atlantique, IRISA, UMR CNRS 6074, France), Guillaume Doyen (IMT Atlantique, IRISA, UMR CNRS 6074, France), Xavier Lagrange (IMT Atlantique, IRISA, UMR CNRS 6074, France)

Identity and Access Management Architecture in the SILVANUS Project

Pawel Rajba (Warsaw University of Technology, Poland), Natan Orzechowski (Warsaw University of Technology, Poland), Karol Rzepka (Warsaw University of Technology, Poland), Przemysław Szary (Warsaw University of Technology, Poland), Dawid Nastaj (Warsaw University of Technology, Poland), Krzysztof Cabaj (Warsaw University of Technology, Poland)

Enhancing Network Security Through Granular Computing: A Clustering-by-Time Approach to NetFlow Traffic Analysis

Mikołaj Komisarek (ITTI Sp. z o.o., Poland), Marek Pawlicki (Bydgoszcz University of Science and Technology, Poland), Salvatore D'Antonio (Naples University Parthenope, Italy), Rafał Kozik (Bydgoszcz University of Science and Technology, Poland), Aleksandra Pawlicka (Warsaw University, POLAND, Poland), Michał Choraś (Bydgoszcz University of Science and Technology, Poland)

Future-proofing Secure V2V Communication against Clogging DoS Attacks

Hongyu Jin (KTH Royal Institute of Technology, Sweden), Zhichao Zhou (KTH Royal Institute of Technology, Sweden), Panos Papadimitratos (KTH Royal Institute of Technology, Sweden)

ENS III:

30.7.24 17:00 – 18:30, Room SR07

Introducing a Multi-Perspective xAI Tool for Better Model Explainability

Marek Pawlicki (Bydgoszcz University of Science and Technology, Poland), Damian Puchalski (ITTI Sp. z o.o., Poland), Sebastian Szelest (ITTI Sp. z o.o., Poland), Aleksandra Pawlicka (ITTI Sp. z o.o., Poland), Rafal Kozik (Bydgoszcz University of Science and Technology, Poland), Michał Choraś (Bydgoszcz University of Science and Technology, Poland)

SoK: A Taxonomy for Hardware-Based Fingerprinting in the Internet of Things
Christian Spinnler (Siemens AG, FAU Erlangen-Nürnberg, Germany), Torsten Labs (Siemens AG, Germany), Norman Franchi (FAU Erlangen-Nürnberg, Chair of Electrical Smart City Systems, AIN, Germany)

Trustworthy AI-based Cyber-Attack Detector for Network Cyber Crime Forensics
Damian Puchalski (ITTI Sp. z o.o., Poland), Marek Pawlicki (Bydgoszcz University of Science and Technology, Poland), Rafał Kozik (Bydgoszcz University of Science and Technology, Poland), Rafał Renk (ITTI Sp. z o.o., Poland), Michał Choraś (Bydgoszcz University of Science and Technology, Poland)

Forensic Investigation of An Android Jellybean-based Car Audio Video Navigation System
Yejin Yoon (Dankook University, South Korea), Jeehun Jung (Dankook University, South Korea), Seong-Je Cho (Dankook University, South Korea), Jongmoo Choi (Dankok University, South Korea), Minkyu Park (Konkuk University, South Korea), Sangchul Han (Konkuk University, South Korea)

EPESec I:

30.7.24 10:30 – 12:00, Room SR03

The Cyber Safe Position:
An STPA for Safety, Security, and Resilience Co-Engineering Approach
Georgios Gkoktsis (Fraunhofer SIT | ATHENE, Germany), Ludger Peters (Fraunhofer SIT | ATHENE, Germany)

Anomaly detection mechanisms for in-vehicle and V2X systems
Alexios Lekidis (University of Thessaly, Greece)

An Analysis of Security Concerns in Transitioning Battery Management Systems from First to Second Life
Julian Blümke (CARISSMA Institute of Electric, Connected and Secure Mobility, Technische Hochschule Ingolstadt, Germany), Kevin Gomez Buquerin (CARISSMA Institute of Electric, Connected and Secure Mobility, Technische Hochschule Ingolstadt, Germany), Hans-Joachim Hof (CARISSMA Institute of Electric, Connected and Secure Mobility, Technische Hochschule Ingolstadt, Germany)

Vulnerability management digital twin for energy systems
Jessica B. Heluany (Norwegian University of Science and Technology, Norway), Johannes Goetzfried (Siemens Energy AG - Industrial Cybersecurity, Germany), Bernhard Mehlig (Siemens Energy AG - Industrial Cybersecurity, Germany), Vasileios Gkioulos (Norwegian University of Science and Technology, Norway)

ETACS I:

30.7.24 15:00 – 16:30, Room SR03

Assessing the Impact of Large Language Models on Cybersecurity Education: A Study of ChatGPT's Influence on Student Performance
Marc Ohm (University of Bonn & Fraunhofer FKIE, Germany), Christian Bungartz (University of Bonn, Germany), Felix Boes (University of Bonn, Germany), Michael Meier (University of Bonn & Fraunhofer FKIE, Germany)

ETACS II:

30.7.24 17:00 – 18:30, Room SR03

Event-based Data Collection and Analysis in the Cyber Range Environment
Willi Lazarov (Brno University of Technology, Czechia), Samuel Janek (Brno University of Technology, Czechia), Zdenek Martinasek (Brno University of Technology, Czechia), Radek Fujdiak (Brno University of Technology, Czechia)

Beyond the Bugs: Enhancing Bug Bounty Programs through Academic Partnerships
Andrej Krištofík (CERIT, Faculty of Informatics, and Institute of Law and Technology, Faculty of Law, Masaryk University, Slovakia), Jakub Vostoupal (CERIT, Faculty of Informatics, and Institute of Law and Technology, Faculty of Law, Masaryk University, Czechia), Kamil Malinka (Institute of Computer Science and Faculty of Informatics, Masaryk University, Czechia), František Kasl (CERIT, Faculty of Informatics, and Institute of Law and Technology, Faculty of Law, Masaryk University, Czechia), Pavel Loutocký (CERIT, Faculty of Informatics, and Institute of Law and Technology, Faculty of Law, Masaryk University, Czechia)

Enhancing Cybersecurity Curriculum Development: AI-Driven Mapping and Optimization Techniques
Petr Dzurenda (Brno University of Technology, Czechia), Sara Ricci (Brno University of Technology, Czechia), Marek Sikora (Brno University of Technology, Czechia), Michal Stejskal (Brno University of Technology, Czechia), Imre Lendák (Faculty of technical sciences, Serbia), Pedro Adao (Instituto Superior Tecnico, Portugal)

Tackling the cybersecurity workforce gap with tailored cybersecurity study programs in Central and Eastern Europe
Marko Zivanovic (PhD Student, Faculty of Technical Science, Novi Sad, Serbia, Serbia), Imre Lendák (Professor, Faculty of Technical Science, Novi Sad, Serbia, Serbia), Ranko Popovic (Retired professor, Faculty of Technical Science, Novi Sad, Serbia, Serbia)

FARES I:

31.7.24 13:15 – 14:45, Room SR07

Modelling the privacy landscape of the Internet of Vehicles
Ruben Cacciato (University of Catania, Italy), Mario Raciti (IMT School for Advanced Studies Lucca, Italy), Sergio Esposito (University of Catania, Italy), Giampaolo Bella (University of Catania, Italy)

A Systematic Review of Contemporary Applications of Privacy-Aware Graph Neural Networks in Smart Cities
Jingyan Zhang (Dublin City University, Ireland), Irina Tal (Dublin City University, Ireland)

The Right to Be Zero-Knowledge Forgotten
Ivan Visconti (DIEM, University of Salerno, Italy)

On Implementing Linear Regression on Homomorphically Encrypted Data: A Case-Study
Gianluca Dini (University of Pisa, Italy)

Navigating the landscape of IoT security and associated risks in critical infrastructures
Andrej Pastorek (Prague Advanced Technology and Research Innovation Center, Czechia), Andrea Tundis (German Aerospace Center (DLR), Germany)

FARES II:

31.7.24 15:15 – 16:45, Room SR07

Towards realistic problem-space adversarial attacks against machine learning in network intrusion detection
Marta Catillo (Università degli Studi del Sannio, Italy), Antonio Pecchia (Università degli Studi del Sannio, Italy), Antonio Repola (Università degli Studi del Sannio, Italy), Umberto Villano (Università degli Studi del Sannio, Italy)

Enhancing Algorithmic Fairness: Integrative Approaches and Multi-Objective Optimization Application in Recidivism Models
Michael Farayola (Lero Research Centre, School of Computing, Dublin City University, Ireland), Malika Bendechache (Lero & ADAPT Research Centres, School of Computer Science, University of Galway, Ireland), Takfarinas Saber (Lero Reseach Centre, School of Computer Science, University of Galway, Ireland), Regina Connolly (Lero Research Centre, School of Business, Dublin City University, Ireland), Irina Tal (Lero Research Centre, School of Computing, Dublin City University, Ireland)

Toward a Log-based Anomaly Detection System for Cyber Range Platforms
Francesco Blefari (University of Calabria, Italy), Francesco Aurelio Pironti (University of Calabria, Italy), Angelo Furfaro (University of Calabria, Italy)

SBOM Ouverture: What We Need and What We Have
Gregorio Dalia (University of Sannio, Italy), Corrado Aaron Visaggio (University of Sannio, Italy), Andrea Di Sorbo (University of Sannio, Italy), Gerardo Canfora (University of Sannio, Italy)

GRASEC I:

1.8.24 08:45 – 10:15, Room SR05

NORIA UI: Efficient Incident Management on Large-Scale ICT Systems Represented as Knowledge Graphs
Lionel Tailhardat (Orange, France), Yoan Chabot (Orange, France), Antoine Py (Orange, France), Perrine Guillemette (Orange, France)

GRASEC II:

1.8.24 10:45 – 12:15, Room SR05

Comparing Hyperbolic Graph Embedding models on Anomaly Detection for Cybersecurity
Mohamed Yacine Touahria Miliani (École Nationale Supérieure d'Informatique, Algeria), Souhail Abdelmouaiz Sadat (École Nationale Supérieure d'Informatique, Algeria), Hamida Seba (University Lyon1, France), Mohammed Haddad (Université Claude Bernard Lyon-1, France)

FedHE-Graph: Federated Learning with Hybrid Encryption on Graph Neural Networks for Advanced Persistent Threat Detection
Atmane Ayoub Mansour Bahar (École Nationale Supérieure d'Informatique, Alger, Algérie, Algeria), Kamel Soaïd Ferrahi (École Nationale Supérieure d'Informatique, Alger, Algérie, Algeria), Mohamed-Lamine Messai (Université Lumière Lyon 2, France), Hamida Seba (University Lyon 1, France), Karima Amrouche (École Nationale Supérieure d'Informatique, Alger, Algérie, Algeria)

Advancing ESSecA: a step forward in Automated Penetration Testing
Massimiliano Rak (University of Campania, Luigi Vanvitelli, Italy), Felice Moretta (University of Campania "Luigi Vanvitelli", Italy), Daniele Granata (Università della Campania "Luigi Vanvitelli", Italy)

A Model-based Approach for Assessing the Security of Cyber-Physical Systems
Hugo Teixeira De Castro (Télécom Sud Paris, France), Ahmed Hussain (KTH Royal Institute of Technology, Sweden), Gregory Blanc (Institut Mines-Télécom, Télécom SudParis, Institut Polytechnique de Paris, France), Jamal El Hachem (Institut de Recherche en Informatique et Systèmes Aléatoires (IRISA), Université de Bretagne Sud (UBS), France), Dominique Blouin (Telecom Paris, France), Jean Leneutre (Telecom Paris, France), Panos Papadimitratos (KTH Royal Institute of Technology, Sweden)

IMTrustSec:

31.7.24 15:15 – 16:45, Room SR08

Acceleration of DICE Key Generation using Key Caching
Dominik Lorych (Fraunhofer SIT | ATHENE, Germany), Lukas Jäger (Fraunhofer SIT | ATHENE, Germany), Andreas Fuchs (Fraunhofer SIT | ATHENE, Germany)

Analysis of the Capability and Training of Chat Bots in the Generation of Rules for Firewall or Intrusion Detection Systems
Bernardo Louro (Universidade da Beira Interior, Portugal), Raquel Abreu (Universidade da Beira Interior, Portugal), Joana Cabral Costa (Universidade da Beira Interior and Instituto de Telecomunicações, Portugal), João B. F. Sequeiros (Universidade da Beira Interior and Instituto de Telecomunicações, Portugal), Pedro R. M. Inácio (Universidade da Beira Interior and Instituto de Telecomunicações, Portugal)

Anomaly-Based Intrusion Detection for Blackhole Attack Mitigation
Ashraf Abdelhamid (Nile University, Egypt), Mahmoud Said Elsayed (University College Dublin, Ireland), Heba K. Aslan (Nile University, Egypt), Marianne A. Azer (National Telecommunication Institute, Egypt)

Threat-TLS: A Tool for Threat Identification in Weak, Malicious, or Suspicious TLS Connections
Diana Gratiela Berbecaru (Politecnico di Torino, Italy), Antonio Lioy (Politecnico di Torino, Italy)

IWAPS I:

31.7.24 08:45 – 10:15, Room SR04

AIAS: AI-ASsisted cybersecurity platform to defend against adversarial AI attacks
Georgios Petihakis (University of Piraeus, Greece), Aristeidis Farao (University of Piraeus, Greece), Panagiotis Bountakas (University of Piraeus, Greece), Athanasia Sabazioti (Department of Tourism Studies, University of Piraeus, Greece), John Polley (School of Communication, University of Southern California, Greece), Christos Xenakis (University of Piraeus, Greece)

ARGAN-IDS: Adversarial Resistant Intrusion Detection Systems using Generative Adversarial Networks
João Costa (INOV INESC Inovação, Portugal), Filipe Apolinário (INOV INESC Inovação, Portugal), Carlos Ribeiro (Universidade de Lisboa, Portugal)

SYNAPSE – An Integrated Cyber Security Risk & Resilience Management Platform, With Holistic Situational Awareness, Incident Response & Preparedness Capabilities
Panagiotis Bountakas (Sphynx Technology Solutions, Switzerland), Konstantinos Fysarakis (Sphynx Technology Solutions, Switzerland), Thomas Kyriakakis (Dienekes SI IKE, Greece), Panagiotis Karafotis (Dienekes SI IKE, Greece), Sotiropoulos Aristeidis (AEGIS IT RESEARCH GmbH, Germany), Maria Tasouli (Insuretics Limited, Cyprus), Cristina Alcaraz (University of Malaga, Spain), George Alexandris (Nodalpoint Systems, Greece), Vassiliki Andronikou (Nodalpoint Systems, Greece), Tzortzia Koutsouri (Cyberalytics Limited, Cyprus), Romarick Yatagha (Framatome, Germany), George Spanoudakis (Sphynx Technology Solutions, Switzerland), Sotiris Ioannidis (Dienekes SI IKE, Greece), Fabio Martinelli (Consiglio Nazionale delle Ricerche, Italy), Oleg Illiashenko (Consiglio Nazionale delle Ricerche, Italy)

NITRO: an Interconnected 5G-IoT Cyber Range
Aristeidis Farao (University of Piraeus, Greece), Christoforos Ntantogian (Ionian University - Department of Informatics, Greece), Stylianos Karagiannis (Ionian University - Department of Informatics, Greece), Emmanouil Magkos (Ionian University - Department of Informatics, Greece), Alexandra Dritsa (University of Piraeus, Greece), Christos Xenakis (University of Piraeus, Greece)

IWAPS II:

31.7.24 10:45 – 12:15, Room SR04

PAKA: Pseudonymous Authenticated Key Agreement without bilinear cryptography
Raphael Schermann (Institute of Technical Informatics, Graz University of Technology, Austria), Simone Bussa (Department of Control and Computer Engineering, Politecnico di Torino, Italy), Rainer Urian (Infineon Technologies AG, Augsburg, Germany), Roland Toegl (Infineon Technologies Austria AG, Austria), Christian Steger (Institute of Technical Informatics, Graz University of Technology, Austria)

Advanced methods for generalizing time and duration during dataset anonymization
Jenno Verdonck (DistriNet, KU Leuven, Belgium), Kevin De Boeck (DistriNet, KU Leuven, Belgium), Michiel Willocx (DistriNet, KU Leuven, Belgium), Vincent Naessens (DistriNet, KU Leuven, Belgium)

Immutability and non-repudiation in the exchange of key messages within the EU IoT-Edge-Cloud Continuum
Salvador Cuñat (Universitat Politècnica de València, Spain), Raúl Reinosa (Universitat Politècnica de València, Spain), Ignacio Lacalle (Universitat Politècnica de València, Spain), Carlos E. Palau (Universitat Politècnica de València, Spain)

Just Rewrite It Again: A Post-Processing Method for Enhanced Semantic Similarity and Privacy Preservation of Differentially Private Rewritten Text
Stephen Meisenbacher (Technical University of Munich, Germany), Florian Matthes (Technical University of Munich, Germany)

IWAPS III:

31.7.24 13:15 – 14:45, Room SR04

Integrating Hyperledger Fabric with Satellite Communications: A Revolutionary Approach for Enhanced Security and Decentralization in Space Networks
Anastassios Voudouris (University of Piraeus, Greece), Aristeidis Farao (University of Piraeus, Greece), Aggeliki Panou (University of Piraeus, Greece), John Polley (School of Communication, University of Southern California, United States), Christos Xenakis (University of Piraeus, Greece)

Entity Recognition on Border Security
George Suciu (Beia Consult Int, Romania), Mari-Anais Sachian (Beia Consult Int, Romania), Razvan Bratulescu (Beia Consult Int, Romania), Kejsi Koci (Beia Consult Int, Romania), Grigor Parangoni (Beia Consult Int, Romania)

Towards 5G Advanced network slice assurance through isolation mechanisms
Alexios Lekidis (University of Thessaly, Greece)

Multimodal Security Mechanisms for Critical Time Systems using blockchain in Chriss project
Mari-Anais Sachian (BEIA CONSULT INTERNATIONAL, Romania), George Suciu (BEIA CONSULT INTERNATIONAL, Romania), Maria Niculae (BEIA CONSULT INTERNATIONAL, Romania), Adrian Paun (BEIA CONSULT INTERNATIONAL, Romania), Petrica Ciotirnae (BEIA CONSULT INTERNATIONAL, Romania), Ivan Horatiu (BEIA CONSULT INTERNATIONAL, Romania), Cristina Tudor (BEIA CONSULT INTERNATIONAL, Romania), Robert Florescu (BEIA CONSULT INTERNATIONAL, Romania)

IWAPS IV:

31.7.24 15:15 – 16:45, Room SR04

Developing a Call Detail Record Generator for Cultural Heritage Preservation and Theft Mitigation: Applications and Implications
Robert Vatasoiu (Beia Consult International, Romania), Alexandru Vulpe (Beia Consult International, Romania), Robert Florescu (Beia Consult International, Romania), Mari-Anais Sachian (Beia Consult International, Romania)

Open V2X Management Platform Cyber-Resilience and Data Privacy Mechanisms
Alexios Lekidis (University of Thessaly, Greece), Hugo Morais (Universidade de Lisboa, Portugal)

PCSCI:

30.7.24 10:30 – 12:00, Room SR05

SOVEREIGN – Towards a Holistic Approach to Critical Infrastructure Protection
Georg Becker (DCSO GmbH, Germany), Thomas Eisenbarth (Universität zu Lübeck, Germany), Hannes Federrath (Universität Hamburg, Germany), Mathias Fischer (Universität Hamburg, Germany), Nils Loose (Universität zu Lübeck, Germany), Simon Ott (Fraunhofer AISEC, Germany), Joana Pecholt (Fraunhofer AISEC, Germany), Stephan Marwedel (Airbus Commercial Aircraft, Germany), Dominik Meyer (Helmut Schmidt Universität, Germany), Jan Stijohann (Langlauf Security Automation, Germany), Anum Talpur (Universität Hamburg, Germany), Matthias Vallentin (Tenzir GmbH, Germany)

Towards Availability of Strong Authentication in Remote and Disruption-Prone Operational Technology Environments
Mohammad Nosouhi (Deakin Cyber Research and Innovation Centre, Deakin University, Geelong, Australia, Australia), Divyans Mahansaria (Tata Consultancy Services (TCS) Ltd., Kolkata, India, India), Zubair Baig (Deakin Cyber Research and Innovation Centre, Deakin University, Geelong, Australia, Australia), Lei Pan (Deakin Cyber Research and Innovation Centre, Deakin University, Geelong, Australia, Australia), Robin Doss (Deakin Cyber Research and Innovation Centre, Deakin University, Geelong, Australia, Australia), Keshav Sood (Deakin Cyber Research and Innovation Centre, Deakin University, Geelong, Australia, Australia), Debi Prasad Pati (Tata Consultancy Services (TCS) Ltd., Kolkata, India, India), Praveen Gauravaram (Tata Consultancy Services (TCS) Ltd., Brisbane, Australia, Australia)

SecIndustry I:

30.7.24 10:30 – 12:00, Room SR06

EmuFlex: A Flexible OT Testbed for Security Experiments with OPC UA
Alexander Giehl (Fraunhofer, Germany), Michael P. Heinl (Fraunhofer AISEC, Germany), Victor Embacher (Fraunhofer AISEC, Germany)

Gateway to the Danger Zone: Secure and Authentic Remote Reset in Machine Safety
Sebastian N. Peters (Technical University of Munich & Fraunhofer AISEC, Germany), Nikolai Puch (Technical University of Munich & Fraunhofer AISEC, Germany), Michael P. Heinl (Technical University of Munich & Fraunhofer AISEC, Germany), Philipp Zieris (Technical University of Munich & Fraunhofer AISEC, Germany), Mykolai Protsenko (Fraunhofer AISEC, Germany), Thorsten Larsen-Vefring (TRUMPF Werkzeugmaschinen SE + Co. KG, Germany), Marcel Ely Gomes (TRUMPF Werkzeugmaschinen SE + Co. KG, Germany), Aliza Maftun (Siemens AG, Germany), Thomas Zeschg (Siemens AG, Germany)

An IEC 62443-security oriented domain specific modelling language
Jolahn Vaudey (Inria, France), Stéphane Mocanu (Grenoble INP, France), Gwenaël Delaval (Université Grenoble alpes, France), Eric Rutten (Inria, France)

SecIndustry II:

30.7.24 13:00 – 14:30, Room SR06

Using Artificial Intelligence in Cyber Security Risk Management for Telecom Industry 4.0
Ijeoma Ebere-Uneze (Royal Holloway, University of London, United Kingdom), Syed Naqvi (Liverpool John Moores University, United Kingdom)

Vulnerability detection tool in source code by building and leveraging semantic code graph
Sabine Delaitre (Bosonit group, Spain), José Maria Pulgar Gutiérrez (DocExploit, Spain)

A SOAR platform for standardizing, automating operational processes and a monitoring service facilitating auditing procedures among IoT trustworthy environments
Vasiliki Georgia Bilali (Institute of Communication & Computer Systems (ICCS), Greece), Eustratios Magklaris (Institute of Communication & Computer Systems (ICCS), Greece), Dimitrios Kosyvas (Institute of Communication & Computer Systems (ICCS), Greece), Lazaros Karagiannidis (Institute of Communication & Computer Systems (ICCS), Greece), Eleftherios Ouzounoglou (Institute of Communication & Computer Systems (ICCS), Greece), Angelos Amditis (Institute of Communication & Computer Systems (ICCS), Greece)

SP2I I:

30.7.24 13:00 – 14:30, Room SR08

Lattice-based Multisignature Optimization for RAM Constrained Devices
Sara Ricci (Brno University of Technology, Czechia), Vladyslav Shapoval (Brno University of Technology, Czechia), Petr Dzurenda (Brno University of Technology, Czechia), Peter Roenne (University of Luxembourg, Luxembourg), Jan Oupicky (University of Luxembourg, Luxembourg), Lukas Malina (Brno University of Technology, Czechia)

Quantum-Resistant and Secure MQTT Communication
Lukas Malina (Brno University of Technology, Czechia), Patrik Dobias (Brno University of Technology, Czechia), Petr Dzurenda (Brno University of Technology, Czechia), Gautam Srivastava (Brandon University, Canada)

SP2I II:

30.7.24 15:00 – 16:30, Room SR08

Comparison of Multiple Feature Selection techniques for Machine Learning-Based Detection of IoT Attacks
Viet Anh Phan (Brno University of Technology, Czechia), Jan Jerabek (Brno University of Technology, Czechia), Lukas Malina (Brno University of Technology, Czechia)

Identification of industrial devices based on payload
Ondrej Pospisil (Brno University of Technology, Faculty of Electrical Engineering and Communication, Department of Telecommunication, Czechia), Radek Fujdiak (Brno University of Technology, Faculty of Electrical Engineering and Communication, Department of Telecommunication, Czechia)

SP2I III:

30.7.24 17:00 – 18:30, Room SR08

DDS Security+: Enhancing the Data Distribution Service With TPM-based Remote Attestation
Paul Georg Wagner (Fraunhofer IOSB, Germany), Pascal Birnstill (Fraunhofer IOSB, Germany), Tim Samorei (Karlsruhe Institute of Technology, Germany), Jürgen Beyerer (Karlsruhe Institute of Technology, Germany)

Secure and Privacy-Preserving Car-Sharing Systems

Lukas Malina (Brno University of Technology, Czechia), Petr Dzurenda (Brno University of Technology, Czechia), Norbert Lövinger (Brno University of Technology, Czechia), Ijeoma Faustina Ekeh (University of Tartu, Estonia), Raimundas Matulevicius (University of Tartu, Estonia)

DECEPTWIN: Proactive Security Approach for IoV by Leveraging Deception-based Digital Twins and Blockchain

Mubashar Iqbal (University of Tartu, Institute of Computer Science, Estonia), Sabah Suhail (Queen's University Belfast, United Kingdom), Raimundas Matulevičius (University of Tartu, Institute of Computer Science, Estonia)

SPETVID:

2.8.24 13:30 – 15:00, Room SR08

Chain Links on Wheels: A Security Scheme for IoV Connectivity through Blockchain Integration

Ibtisam Ehsan (University of Chinese Academy of Sciences, Beijing, China, China), Muhammad Irfan Khalid (University of Sialkot, Pakistan), Mansoor Ahmed (ADAPT Centre, Innovation Value Institute, Maynooth University Maynooth, Ireland, Ireland), Markus Helfert (ADAPT Centre, Innovation Value Institute, Maynooth University Maynooth, Ireland, Ireland)

GDPR-compliant Video Search and Retrieval System for Surveillance Data

Amna Shifa (University of Galway School of Computer Science , Ireland), Rónán Kennedy (University of Galway School of Law, Ireland), Mamoona Naveed Asghar (University of Galway School of Computer Science, Ireland)

STAM I:

30.7.24 13:00 – 14:30, Room SR04

A Multi-layer Approach through Threat Modelling and Attack Simulation for Enhanced Cyber Security Assessment

Eider Iturbe (TECNALIA Research Innovation, Basque Research and Technology Alliance (BRTA), Spain), Javier Arcas (TECNALIA Research Innovation, Basque Research and Technology Alliance (BRTA), Spain), Erkuden Rios (TECNALIA Research Innovation, Basque Research and Technology Alliance (BRTA), Spain)

A Framework Towards Assessing the Resilience of Urban Transport Systems
Gérald Rocher (Université Côte d'Azur (UniCA), Centre National de la Recherche Scientifique (CNRS, I3S), France), Jean-Yves Tigli (Université Côte d'Azur (UniCA), Centre National de la Recherche Scientifique (CNRS, I3S), France), Stéphane Lavirotte (Université Côte d'Azur (UniCA), Centre National de la Recherche Scientifique (CNRS, I3S), France), Nicolas Ferry (Université Côte d'Azur (UCA), Institut national de recherche en sciences et technologies du numérique (INRIA, Kairos), France)

Towards the adoption of automated cyber threat intelligence information sharing with integrated risk assessment
Valeria Valdés Ríos (Université Paris-Saclay - Montimage, France), Fatiha Zaidi (Université Paris-Saclay, CNRS, ENS Paris-Saclay, Laboratoire Méthodes Formelles, France), Ana Rosa Cavalli (Institut Polytechnique, Telecom SudParis - Montimage, France), Angel Rego (Tecnalia, Basque Research and Technology Alliance (BRTA), Spain)

The PRECINCT Ecosystem Platform for Critical Infrastructure Protection: Architecture, Deployment and Transferability
Djibrilla Amadou Kountche (AKKODIS Reaserach, France), Jocelyn Aubert (Luxembourg Institute of Science and Technology, Luxembourg), Manh Dung Nguyen (Montimage, France), Natalia Kalfa (ATTD, Greece), Nicola Durante (ENGINEERING, Italy), Cristiano Passerini (LEPIDA, Italy), Stephane Kuding (KONNECTA, Greece)

STAM II:

30.7.24 15:00 – 16:30, Room SR04

Transfer Adversarial Attacks through Approximate Computing
Valentina Casola (University of Naples Federico II, Italy), Salvatore Della Torca (Università degli Studi di Napoli Federico II, Italy)

AI-Powered Penetration Testing using Shennina: From Simulation to Validation
Stylianos Karagiannis (Ionian University - Department of Informatics, PDM, Greece), Camilla Fusco (University of Naples Federico II, Italy), Leonidas Agathos (PDM, Portugal), Wissam Mallouli (Montimage, France), Valentina Casola (University of Naples Federico II, Italy), Christoforos Ntantogian (Ionian University - Department of Informatics, Greece), Emmanouil Magkos (Department of Informatics, Ionian University, Corfu, Greece, Greece)

AI4SOAR: A Security Intelligence Tool for Automated Incident Response
Manh-Dung Nguyen (Montimage EURL, France), Wissam Mallouli (Montimage EURL, France), Ana Rosa Cavalli (Montimage EURL, France), Edgardo Montes de Oca (Montimage EURL, France)

Automated Passport Control: Mining and Checking Models of Machine Readable Travel Documents
Stefan Marksteiner (AVL List Gmbh, Austria / Mälardalen University, Sweden), Marjan Sirjani (Mälardalen University, Sweden), Mikael Sjödin (Mälardalen University, Sweden)

STAM III:

30.7.24 17:00 – 18:30, Room SR04

A comprehensive evaluation of interrupt measurement techniques for predictability in safety-critical systems
Daniele Lombardi (University of Naples Federico II Department of Electrical Engineering and Information Technologies, Italy), Mario Barbareschi (University of Naples Federico II Department of Electrical Engineering and Information Technologies, Italy), Salvatore Barone (Università degli Studi di Napoli - Federico II Department of Electrical Engineering and Information Technologies, Italy), Valentina Casola (University of Naples Federico II Department of Electrical Engineering and Information Technologies, Italy)

Automating Side-Channel Testing for Embedded Systems: A Continuous Integration Approach
Philipp Schloyer (Technical University of Applied Sciences Augsburg, Germany), Peter Knauer (Technical University of Applied Sciences Augsburg, Germany), Bernhard Bauer (Uni Augsburg, Germany), Dominik Merli (Technical University of Applied Sciences Augsburg, Germany)

NERO: Advanced Cybersecurity Awareness Ecosystem for SMEs
Charalambos Klitis (eBOS Technologies Ltd, Cyprus), Ioannis Makris (METAMIND INNOVATIONS IKE, Greece), Pavlos Bouzinis (METAMIND INNOVATIONS IKE, Greece), Dimitrios Christos Asimopoulos (METAMIND INNOVATIONS IKE, Greece), Wissam Mallouli (MONTIMAGE EURL, France), Kitty Kioskli (TRUSTILIO BV, Netherlands), Eleni Seralidou (TRUSTILIO BV, Netherlands), Christos Douligeris (UNIVERSITY OF PIRAEUS RESEARCH CENTER, Greece), Loizos Christofi (eBOS Technologies Ltd, Cyprus)

A Framework for In-network Inference using P4
Huu Nghia Nguyen (Montimage, France), Manh-Dung Nguyen (Montimage, France), Edgardo Montes de Oca (Montimage, France)

TRUSTBUS I:

31.7.24 08:45 – 10:15, Room SR03

Further Insights: Balancing Privacy, Explainability, and Utility in Machine Learning-based Tabular Data Analysis
Wisam Abbasi (Informatics and Telematics Institute (IIT) of National Research Council, Italy), Paolo Mori (IIT-CNR, Italy), Andrea Saracino (Consiglio Nazionale delle Ricerche, Italy)

A Unified Framework for GDPR Compliance in Cloud Computing
Argyri Pattakou (Dept. of Cultural Technology and Communication, University of the Aegean Lesvos, Greece, Greece), Vasiliki Diamantopoulou (Dept. of Information and Communication Systems Engineering, University of the Aegean Samos, Greece, Greece), Christos Kalloniatis (Dept. of Cultural Technology and Communication, University of the Aegean Lesvos, Greece, Greece), Stefanos Gritzalis (Department of Digital Systems University of Piraeus, Greece, Piraeus, Greece, Greece)

Create, Read, Update, Delete: Implications on Security and Privacy Principles regarding GDPR
Michail Pantelelis (University of the Aegean, Greece), Christos Kalloniatis (Department of Cultural Technology and Communication-University of the Aegean, Greece)

The Trade-off Between Privacy & Quality for Counterfactual Explanations
Vincent Dunning (Netherlands Organisation for Applied Scientific Research (TNO), Netherlands), Dayana Spagnuelo (Netherlands Organisation for Applied Scientific Research (TNO), Netherlands), Thijs Veugen (Netherlands Organisation for Applied Scientific Research (TNO), University of Twente, Netherlands), Sjoerd Berning (Netherlands Organisation for Applied Scientific Research (TNO), Netherlands), Jasper van der Waa (Netherlands Organisation for Applied Scientific Research (TNO), Netherlands)

TRUSTBUS II:

31.7.24 10:45 – 12:15, Room SR03

A Framework for Managing Separation of Duty Policies

Sebastian Groll (University of Regensburg, Germany), Sascha Kern (Nexis GmbH, Germany), Ludwig Fuchs (Nexis GmbH, Germany), Günther Pernul (Universität Regensburg, Germany)

A Trust and Reputation System for Examining Compliance with Access Control

Thomas Baumer (Nexis GmbH, Germany), Johannes Grill (Universität Regensburg, Germany), Jacob Adan (Universität Regensburg, Germany), Günther Pernul (Universität Regensburg, Germany)

Individual privacy levels in query-based anonymization

Sascha Schiegg (University of Passau, Germany), Florian Strohmeier (University of Passau, Germany), Armin Gerl (HM University of Applied Sciences Munich, Germany), Harald Kosch (University of Passau, Germany)

DealSecAgg: Efficient Dealer-Assisted Secure Aggregation for Federated Learning

Daniel Demmler (ZAMA, Germany), Joshua Stock (Universität Hamburg, Germany), Henry Heitmann (Universität Hamburg, Germany), Janik Noel Schug (Universität Hamburg, Germany), Daniel Demmler (ZAMA, Germany)

TRUSTBUS III:

31.7.24 13:15 – 14:45, Room SR03

A Risk Assessment and Legal Compliance Framework for Supporting Personal Data Sharing with Privacy Preservation for Scientific Research

Christos Baloukas (National Technical University of Athens, Greece), Lazaros Papadopoulos (National Technical University of Athens, Greece), Kostas Demestichas (National Technical University of Athens, Greece), Axel Weissenfeld (AIT Austrian Institute of Technology, Austria), Sven Schlarb (AIT Austrian Institute of Technology, Austria), Mikel Aramburu (Fundación Vicomtech, Basque Research and Technology Alliance (BRTA), Spain), David Redó (Fundación Vicomtech, Basque Research and Technology Alliance (BRTA), Spain), Jorge García (Fundación Vicomtech, Basque Research and Technology Alliance (BRTA), Spain), Seán Gaines (Fundación Vicomtech, Basque Research and Technology Alliance (BRTA), Spain), Thomas Marquenie (KU Leuven, Belgium), Ezgi Eren (KU Leuven, Belgium), Irmak Erdogan Peter (KU Leuven, Belgium)

What Johnny thinks about using two-factor authentication on GitHub: A survey among open-source developers
Agata Kruzikova (Masaryk University, Czechia), Jakub Suchanek (Masaryk University, Czechia), Milan Broz (Masaryk Universtiy, Czechia), Martin Ukrop (Red Hat, Czechia), Vashek Matyas (Masaryk Universtiy, Czechia)

Aligning eIDAS and Trust Over IP: A Mapping Approach
Cristian Lepore (IRIT, France), Romain Laborde (IRIT, France), Jessica Eynard (Uniersity Toulouse Capitole, France)

Article 45 of the eIDAS Directive Unveils the need to implement the X.509 4-cornered trust model for the WebPKI
Ahmad Samer Wazan (Zayed University, United Arab Emirates), Romain Laborde (Université Toulouse 3 Paul Sabatier, France), Abdelmalek Benzekri (Université Toulouse 3 Paul Sabatier, France), Imran Taj (Zayed University, United Arab Emirates)

TRUSTBUS IV:

31.7.24 15:15 – 16:45, Room SR03

Deployment of Cybersecurity Controls in the Norwegian Industry 4.0
Kristian Kannelønning (NTNU, Norway), Sokratis Katsikas (Norwegian University of Science and Technology, Norway)

Elevating TARA: A Maturity Model for Automotive Threat Analysis and Risk Assessment
Manfred Vielberth (Continental Engineering Services GmbH, Germany), Kristina Raab (University of Regensburg, Germany), Magdalena Glas (University of Regensburg, Germany), Patrick Grümer (Continental Engineering Services GmbH, Portugal), Günther Pernul (University of Regensburg, Germany)

Trust-minimizing BDHKE-based e-cash mint using secure hardware and distributed computation
Antonín Dufka (Masaryk University, Czechia), Jakub Janků (Masaryk University, Czechia), Petr Švenda (Masaryk University, Czechia)

OOBKey: Key Exchange with Implantable Medical Devices Using Out-Of-Band Channels
Mo Zhang (University of Birmingham, UK; University of Melbourne, Australia, United Kingdom), Eduard Marin (Telefonica Research, Spain), Mark Ryan (University of Birmingham, UK, United Kingdom), Vassilis Kostakos (The University of Melbourne, Australia), Toby Murray (University of Melbourne and Data61, Australia), Benjamin Tag (Monash University, Australia), David Oswald (The University of Birmingham, School of Computer Science, United Kingdom),

COSH & WSDF I:

31.7.24 08:45 – 10:15, Room SR05

A Quantitative Analysis of Inappropriate Content, Age Rating Compliance, and Risks to Youth on the Whisper Platform
Jeng-Yu Chou (University of Massachusetts Amherst, United States), Brian Levine (University of Massachusetts Amherst, United States)

COSH & WSDF II:

31.7.24 10:45 – 12:15, Room SR05

Give Me Steam: A Systematic Approach for Handling Stripped Symbols in Memory Forensics of the Steam Deck
Ruba Alsmadi (Louisiana State University, United States), Taha Gharaibeh (Louisiana State University, United States), Andrew Webb (Louisiana State University, United States), Ibrahim Baggili (Louisiana State University, United States)

Forensic Investigation of Humanoid Social Robot: A Case Study on Zenbo Robot
Joseph Brown (Louisiana State University, United States), Abdur Rahman Onik (Louisiana State University, United States), Ibrahim Baggili (Louisiana State University, United States)

ScaNeF-IoT: Scalable Network Fingerprinting for IoT Device
Tadani Nasser Alyahya (University of Southampton School of Electronics and Computer Science , United Kingdom), Leonardo Aniello (University of Southampton School of Electronics and Computer Science , United Kingdom), Vladimiro Sassone (University of Southampton School of Electronics and Computer Science , United Kingdom)

COSH & WSDF III:

31.7.24 13:15 – 14:45, Room SR05

Using DNS Patterns for Automated Cyber Threat Attribution
Cristoffer Leite (Eindhoven University of Technology, Netherlands), Jerry Den Hartog (Eindhoven University of Technology, Netherlands), Daniel Ricardo dos Santos (Forescout Technologies, Netherlands)

Timestamp-based Application Fingerprinting in NTFS
Michael Galhuber (Wittur Group, Austria), Robert Luh (St. Pölten University of Applied Sciences, Austria)

Forensic Analysis of Artifacts from Microsoft's Multi-Agent LLM Platform AutoGen
Clinton Walker (Louisiana State University, United States), Taha Gharaibeh (Louisiana State University, United States), Ruba Alsmadi (Louisiana State University, United States), Cory Hall (MITRE, United States), Ibrahim Baggili (Louisiana State University, United States)

Manipulating the Swap Memory for Forensic Investigation
Maximilian Olbort (FernUniversität in Hagen, Germany), Daniel Spiekermann (FH Dortmund, Germany), Jörg Keller (FernUniversität in Hagen, Germany)

COSH & WSDF IV:

31.7.24 15:15 – 16:45, Room SR05

Don't, Stop, Drop, Pause: Forensics of CONtainer CheckPOINTs (ConPoint)
Taha Gharaibeh (Louisiana State University, United States), Steven Seiden (Louisiana State University, United States), Mohamed Abouelsaoud (Louisiana State University, United States), Elias Bou-Harb (Louisiana State University, United States), Ibrahim Baggili (Louisiana State University, United States)

Blue Skies from (X's) Pain: A Digital Forensic Analysis of Threads and Bluesky
Joseph Brown (Louisiana State University, United States), Abdur Rahman Onik (Louisiana State University, United States), Ibrahim Baggili (Louisiana State University, United States)

Sustainability in Digital Forensics
Sabrina Friedl (University of Regensburg, Germany), Charlotte Zajewski (Universität Regensburg, Germany), Günther Pernul (Universität Regensburg, Germany)

IWCC I:

2.8.24 11:00 – 12:30, Room SR05

An Exploratory Case Study on Data Breach Journalism
Jukka Ruohonen (University of Southern Denmark, Denmark), Kalle Hjerppe (University of Turku, Finland), Maximilian von Zastrow (University of Southern Denmark, Denmark)

IWCC & EPIC-ARES II:

2.8.24 13:30 – 15:00, Room SR05

Detection of AI-Generated Emails – A Case Study
Paweł Gryka (Warsaw University of Technology, Poland), Kacper Gradoń (Warsaw University of Technology, Poland), Marek Kozłowski (Warsaw University of Technology, Poland), Miłosz Kutyła (Warsaw University of Technology, Poland), Artur Janicki (Warsaw University of Technology, Poland)

Unveiling the Darkness: Analysing Organised Crime on the Wall Street Market Darknet Marketplace using PGP Public Keys
Shiying Fan (Fraunhofer SIT, Germany), Paul Moritz Ranly (Fraunhofer SIT, Germany), Lukas Graner (Fraunhofer SIT, Germany), Inna Vogel (Fraunhofer SIT, Germany), Martin Steinebach (Fraunhofer SIT, Germany)

ParsEval: Evaluation of Parsing Behavior using Real-world Out-in-the-wild X.509 Certificates
Stefan Tatschner (Fraunhofer AISEC; University of Limerick, Germany), Sebastian N. Peters (Fraunhofer AISEC; Technical University of Munich, Germany), Michael P. Heinl (Fraunhofer AISEC; Technical University of Munich, Germany), Tobias Specht (Fraunhofer AISEC, Germany), Thomas Newe (University of Limerick, Ireland)

IWSECC & SecHealth:

1.8.24 14:45 – 16:15, Room SR05

Proxy Re-Encryption for Enhanced Data Security in Healthcare: A Practical Implementation
Pablo Cosio (i2CAT Foundation, Spain)

Telemetry data sharing based on Attribute-Based Encryption schemes for cloud-based Drone Management system
Alexandr Silonosov (Blekinge Institute of Technology, Sweden), Lawrence Henesey (Blekinge Institute of Technology, Sweden)

The State of Boot Integrity on Linux – a Brief Review
Robert Haas (Institute of IT Security Research, St.Pölten University of Applied Sciences, Austria), Martin Pirker (Institute of IT Security Research, St.Pölten University of Applied Sciences, Austria)

ICS – CSR II:

01.8.24 10:45 – 12:15

How to Find out What's Going on in Encrypted Smart Meter Networks – without Decrypting Anything
Oliver Eigner (St. Pölten University of Applied Sciences, Austria), Hubert Schölnast (St. Pölten University of Applied Sciences, Austria), Paul Tavolato (University of Vienna, Austria)

Assessing the Performance of Ethereum and Hyperledger Fabric Under DDoS Attacks for Cyber-Physical Systems
Vijay Jayadev (University of Greenwich, United Kingdom), Naghmeh Moradpoor (Edinburgh Napier University, United Kingdom), Andrei Petrovski (Robert Gordon University, United Kingdom)

A Blockchain-based Multi-Factor Honeytoken Dynamic Authentication Mechanism
Vassilis Papaspirou (University of West Attica, Greece), Ioanna Kantzavelou (University of West Attica, Greece), Yagmur Yigit (Edinburgh Napier University, United Kingdom), Leandros Maglaras (Edinburgh Napier University, United Kingdom), Sokratis Katsikas (NORCICS, Norway)

ICS – CSR III:

01.8.24 13:15 – 14: 15

Modeling Human Error Factors with Security Incidents in Industrial Control Systems: A Bayesian Belief Network Approach
Pushparaj Bhosale (TU Wien, Austria), Wolfgang Kastner (TU Wien, Austria), Thilo Sauter (TU Wien, Austria)

Evaluating Cyber Security Dashboards for Smart Cities and Buildings: Enhancing User Modeling with LLMs
Hanning Zhao (Tampere University, Finland), Bilhanan Silverajan (Tampere University, Finland)

ICS – CSR IV:

01.8.24 14:45 – 16:15

Evaluating Cybersecurity Risk: A Comprehensive Comparison of Vulnerability Scoring Methodologies
Konstantina Milousi (CERTH-ITI, Greece), Prodromos Kiriakidis (CERTH-ITI, Greece), Notis Mengidis (CERTH-ITI, Greece), Georgios Rizos (CERTH-ITI, Greece), Mariana S. Mazi (CERTH-ITI, Greece), Antonis Voulgaridis (CERTH-ITI, Greece), Konstantinos Votis (CERTH-ITI, Greece), Dimitrios Tzovaras (CERTH-ITI, Greece)

Network Intrusion Response using Deep Reinforcement Learning in an Aircraft IT-OT Scenario
Matthew Reaney (Queen's University Belfast, United Kingdom), Kieran McLaughlin (Queen's University Belfast, United Kingdom), James Grant (Queen's University Belfast, United Kingdom)

From Seaweed to Security: Harnessing Alginate to Challenge IoT Fingerprint Authentication
Pouria Rad (Ph.D. Student and Research Assistant, School of Computer & Cyber Sciences, Augusta University, GA., United States), Gokila Dorai (Assistant Professor, School of Computer & Cyber Sciences, Augusta University, GA., United States), Mohsen Jozani (Assistant Professor, School of Computer & Cyber Sciences, Augusta University, GA., United States)

Conference Venue

ARES 2024 will be held at the University of Vienna, Austria. Lecture halls are located at the Faculty for Computer Science.

Address of ARES 2024 Conference
Faculty of Computer Science
University of Vienna
Währinger Straße 29, 1090 Vienna, Austria

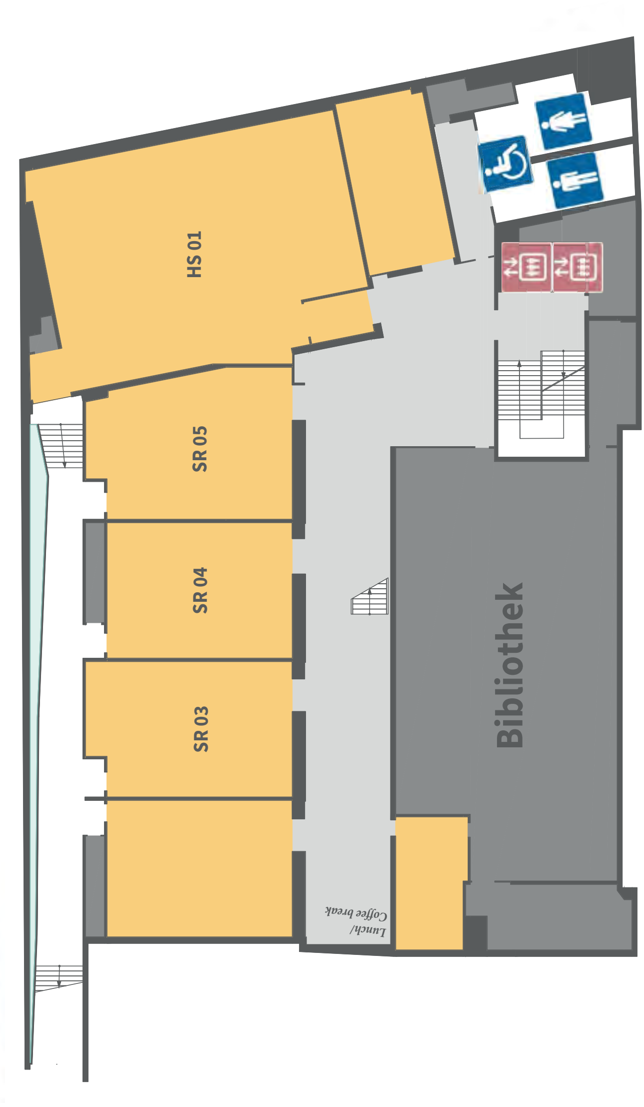
SCAN ME

Public transportation: Tram: 37, 38, 40, 41, 42
Stop: Sensengasse or Spitalgasse

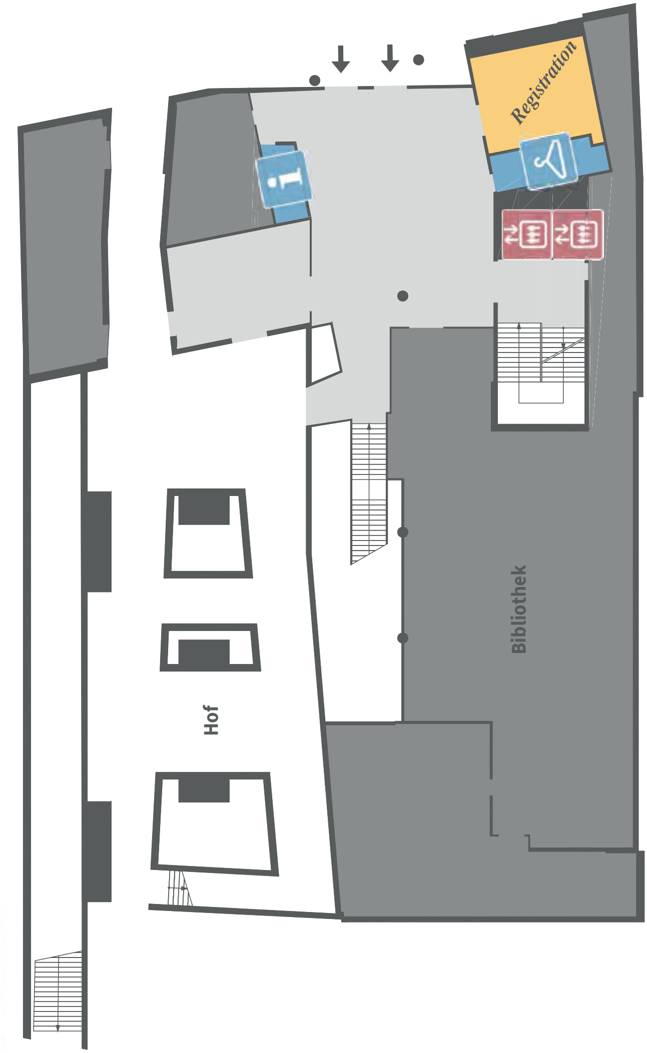
Directions from the tram station to the venue just a quick scan away!

© University of Vienna

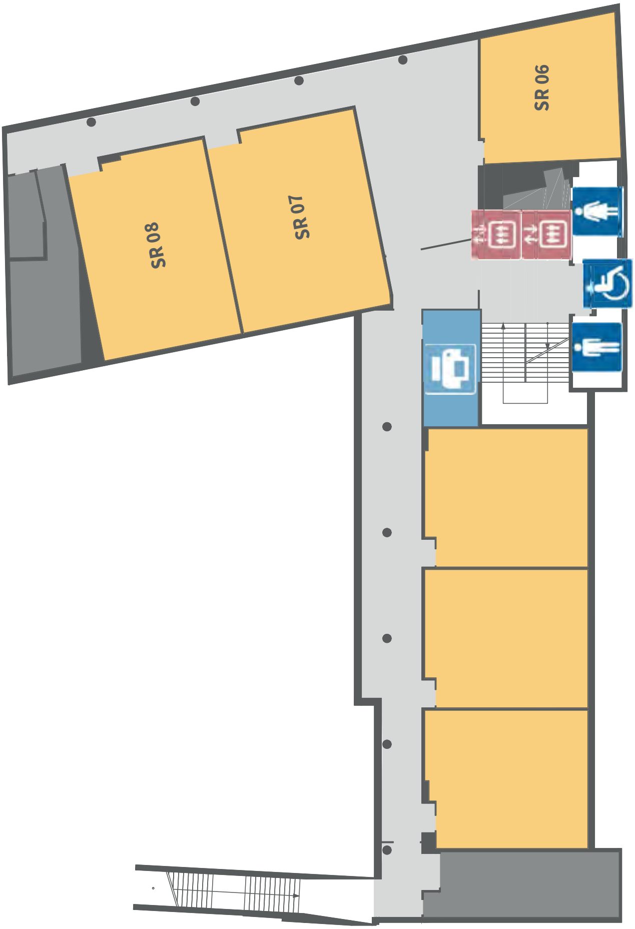
Basement



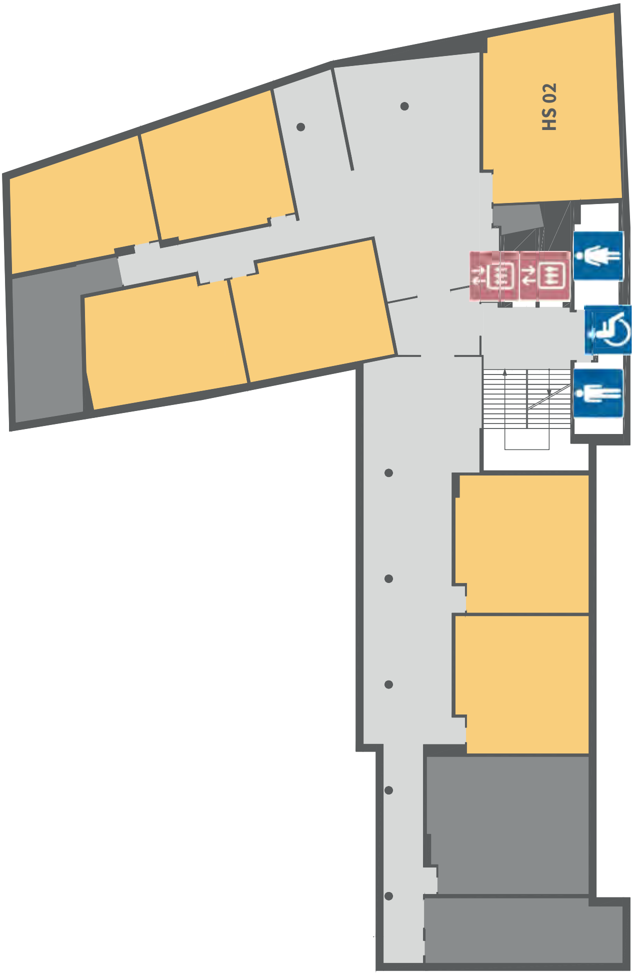
Ground Floor



First Floor



Second Floor



Useful Information

WIFI At ARES

You can access with your Eduroam at the University of Vienna or will be supplied with a unique WIFI login at the Conference Office/Registration.

Emergency Numbers

112	European emergency number
122	Fire Brigarde
133	Poilce
144	Ambulance service

ⓘ **Info:**
The emergency numbers can be called free of charge from any phone in Austria.

Conference Office

Our dedicated team at the Conference Office is here to ensure that your conference experience is nothing short of exceptional.

Registration and Check-In: We'll provide you with your conference materials, name badge, and any necessary information to help you navigate the event effortlessly.

Schedule and Updates: We'll keep you informed and up-to-date with the conference schedule, session changes, and important announcements. Check the bulletin boards or simply ask our staff to stay in the loop.

Lost and Found: Misplaced something? Don't worry! The Conference Office will operate a Lost and Found area to help reunite you with your belongings.

Don't hesitate to approach our knowledgeable team with any questions or concerns

Organizers & Supporters

ARES 2024 is organized by

SBA Research

Supported by

universität wien

MEETING DESTINATION VIENNA
NOW ◆ TOGETHER

Stadt Wien | Kultur

SBA Research

Founded in 2006, SBA Research is a COMET Competence Center for Excellent Technologies located in Vienna, Austria. Our approx. 120 employees – researchers and practitioners – are specialized in Information Security. In cooperation with, among others, the Vienna University of Technology and the University of Vienna as well as other national and international institutions, we follow a dual approach of scientific research and practical implementation. SBA offers a unique portfolio of services, ranging from research cooperation to penetration testing to covering security aspects of future key areas such as Artifical Intelligence, IoT/Industry 4.0, Secure Software Development and security in digitalization. This is complemented by numerous training courses.

University of Vienna / Security & Privacy (SEC) group

Duke Rudolph IV founded the University of Vienna in 1365 as the Alma Mater Rudolphina Vindobonensis, one of the oldest and largest universities in Europe. The Security & Privacy (SEC) group was established in 2020 as part of the Faculty of Computer Science. Information Security and Privacy have always been areas where a multidisciplinary approach is indispensable. With the increased interconnectivity and ubiquitous data access, new services and threats have emerged. Two domains are critical and challenging areas of research that the SEC group currently works in: Distributed Ledger Technology (aka Blockchains) in cooperation with SBA Research; Development Lifecycle of IT in Production Environments with the CD-Lab SQI. In both areas, technical and formal research is best combined with usability research to create solutions incorporating fundamental research results and having a significant and lasting impact.

Notes

Notes

Notes

ARES 2024

Conference Office Contact

Bettina Jaber
Mobile: +43 664 254 03 14
E-Mail: ares@sba-research.org

Clara Kubesch
Mobile: +43 664 88 00 11 61
E-Mail: ares@sba-research.org

ARES
conference
Availability • Reliability • Security