

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
Conference Venue	36
Public Transportation	36
Floor Plan	37
Useful Information	41
Organizers and Supporters	42

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, renowned 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, renowned 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*

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









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 Break							
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	DOD III
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 IV
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 V
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 VI
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	DOD VII	ICS-CSR I
10:15 10:45	Coffee Break					
10:45 12:15	ARES VI	ARES Short	CSA II	GRASEC II	DOD VIII	ICS-CSR II
12:15 13:15	Lunch Break					
13:15 14:15	ARES - Best Paper Session - HS 01				DOD IX	ICS-CSR III
14:15 14:45	Coffee Break					
14:45 16:15	ARES VII	ARES VIII	CSA III	IWSECC & SecHealth	DOD X	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

Keynotes

ARES Keynotes

Yuval Shavitt

Tel Aviv University, Israel

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.

HS 01

31st July

17:00

Machine Learning Solutions for detection of attacks on Internet Routing

© Yuval Shavitt |



Jan Baumbach

University of Hamburg, Germany

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.

HS 01

1st Aug.

16:30

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

© Jan Baumbach



Luca Ardito

Politecnico di Torino, Italy

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.

SR 03

2nd Aug.

9:00

Behavioural Modelling for Sustainability in Smart Homes

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



Joachim Klerx

Austrian Institute of Technology (AIT), Austria

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.

SR 04

1st Aug.

8:45

The Future of Strategic Military Cyber Situational Awareness (CSA)

© Joachim Klerx



Caroline Roth-Ebner

University of Klagenfurt, Austria

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 mediatised 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 mediatised 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.

SR 05

31st July

8:45

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

© Caroline Roth-Ebner



Rémi Cogranne

University of Technology of Troyes (UTT), France

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.

SR 08

31st July

8:45

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

© Remi Cogranne



Torsten Lodderstedt

SPRIND, Germany

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.

SR 07

31st July

8:45

Vision and Challenges of the EUDI Wallet

© Torsten Lodderstedt



Marek Pawlicki

Bydgoszcz University of Science and Technology, Poland

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.

SR 07

30th July

13:00

Enhancing Network Cybersecurity with Novel Trustworthy AI Solutions

© Marek Pawlicki



Joseph Squillace

Penn State Schuylkill, USA

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.

SR 03
30th July
15:00

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

© Joseph Squillace



Martin Husák

Masaryk University, Czech Republic

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.

SR 05
1st Aug.
8:45

Theory and Practice of Cybersecurity Knowledge Graphs and Further Steps

© Martin Husak



Svetlana Boudko

Norwegian Computing Center, Oslo, Norway

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.

SRS 05

1st Aug.

14:45

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

© Svetlana Boudko



Sabarathinam Chockalingam

Institute for Energy Technology (IFE), Norway

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.

SR 06

30th July

13:00

Dynamic Risk Assessment for Industry 4.0

© Sabarathinam Chockalingam



Emma Østerbø

NCE Manufacturing (Norwegian Centre of Expertise), Norway

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.

SR 06

30th July

10:30

Engaging SMEs in the twin transition

© Emma Østerbø



Heribert Vallant

JOANNEUM RESEARCH, Graz, Austria

SR 08

30th July

15:00

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 IIoT 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 IIoT environment are the high level of complexity, which results from the variety of application areas for IIoT. 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 (IIoT) components of the CPS may be up and running.

IIoT Discovery as the fundamental basis for AI guided penetration testing

Petr Svenda

Masaryk University, Czech Republic

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.

SR 08

30th July

13:00

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

© Petr Svenda



Dr Virginia Franqueira

University of Kent, UK

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/>

SR 05

31st July

10:45

Fighting sexual abuse and exploitation of children

© Dr Virginia Franqueira



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!

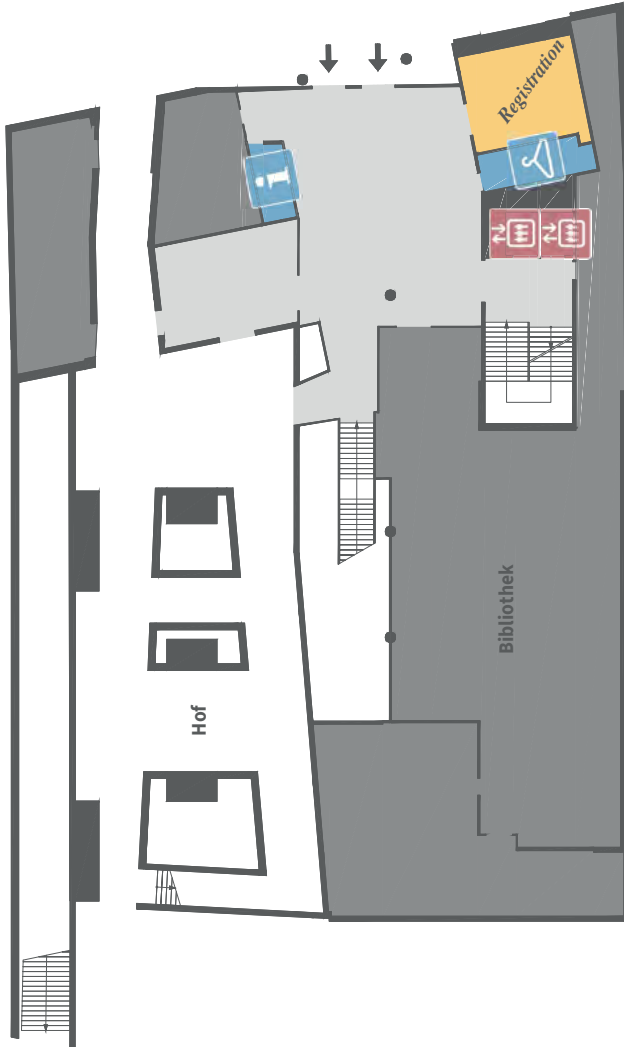


© University of Vienna

Basement

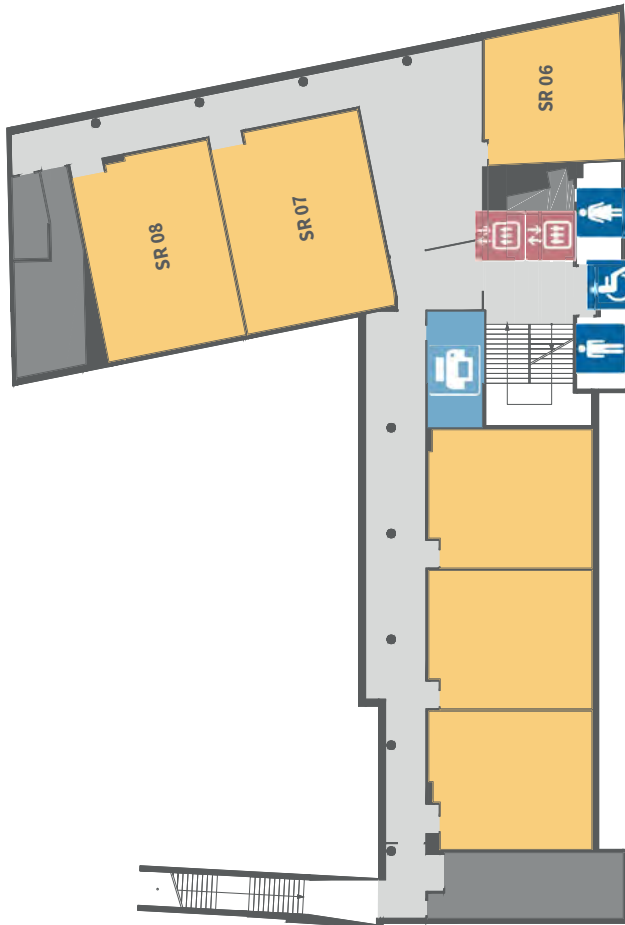


Ground Floor

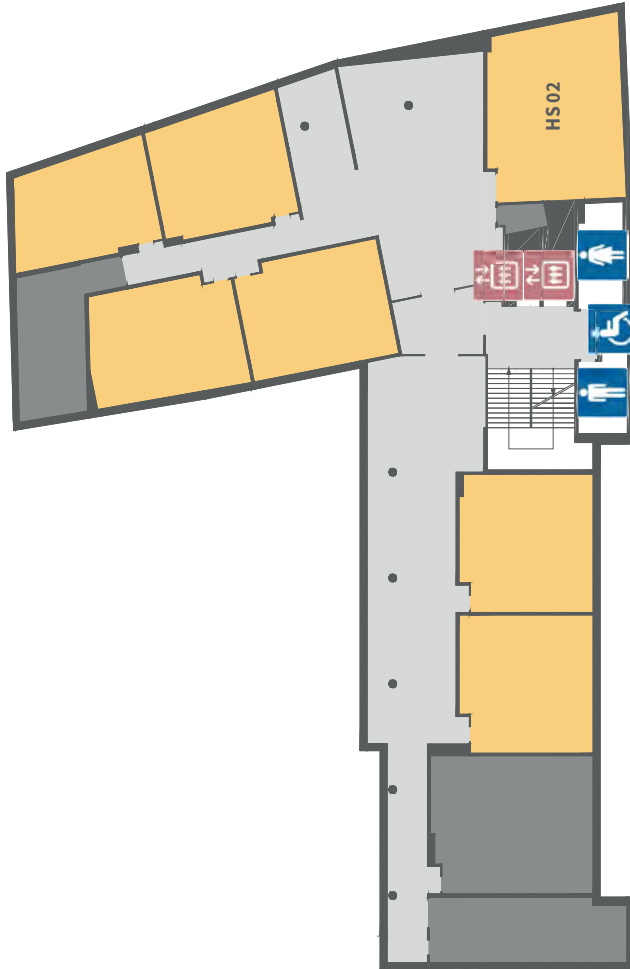


© Universitäts Wien, Veranstaltungsmanagement, Stand Dezember 2017

First Floor



Second Floor



© Universitäts Wien, Veranstaltungsmanagement, Stand Dezember 2017

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 Brigade

133 Police

144 Ambulance service

i 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



Supported by



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 Artificial 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 S&P. 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.

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