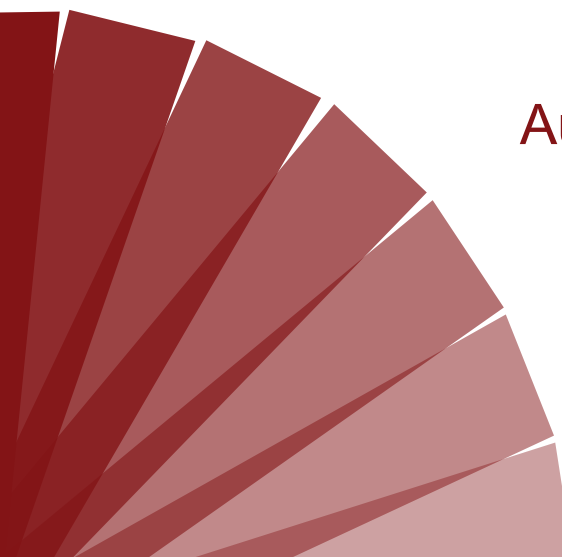


A dark red banner with a slightly irregular, torn-edge effect at the bottom.

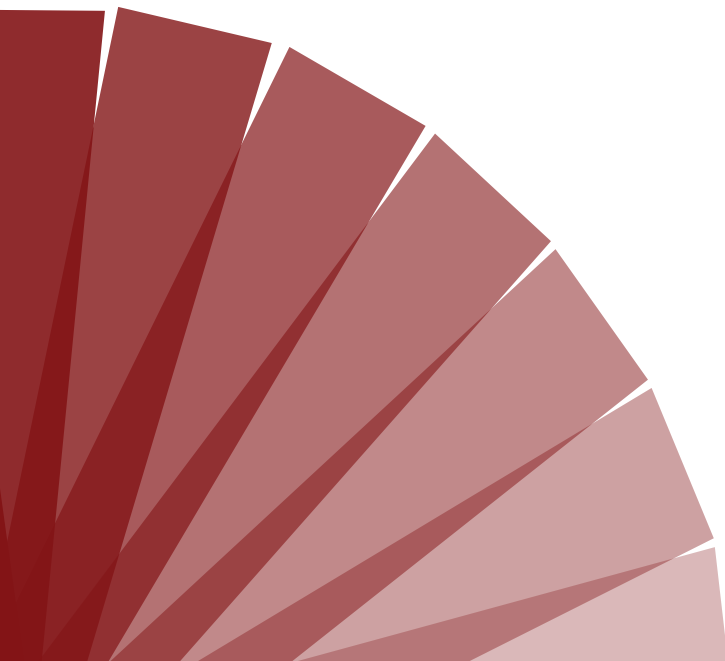
# PROGRAM GUIDE

# ARES 2022

17th International Conference on  
Availability, Reliability and Security

A decorative graphic in the bottom left corner consisting of several overlapping, semi-transparent red fan-like shapes radiating from the corner.

August 23-26, 2022  
Vienna, Austria



# ARES 2022

## Table of Content

<b>Welcome Messages</b>	<b>4</b>
ARES Program Committee Co-Chairs	4
CD-MAKE Chairpersons	5
ARES Workshop Chair	7
ARES EU Symposium Workshop Chair	8
 <b>Program Overview</b>	 <b>9</b>
Tuesday - August 23, 2022	9
Wednesday - August 24, 2022	11
Thursday - August 25, 2022	12
Friday - August 26, 2022	13
 <b>Keynotes</b>	 <b>14</b>
ARES Keynotes	14
CD-MAKE Keynotes	16
Workshops Keynotes	19
 <b>Social Events</b>	 <b>28</b>
Tuesday - August 23, 2022	28
Wednesday - August 24, 2022	28
Thursday - August 25, 2022	30
 <b>Conference Venue</b>	 <b>29</b>
Map - Public Transportation	30
Floor Plan	31
 <b>About Vienna</b>	 <b>34</b>
 <b>Useful Information</b>	 <b>36</b>
 <b>Important Phrases</b>	 <b>37</b>
 <b>Notes</b>	 <b>38</b>
 <b>Organizers and Supporters</b>	 <b>39</b>

# **ARES 2022**

## **The 17th International Conference on Availability, Reliability and Security**

### **Welcome Message from ARES Program Committee Co-Chairs**

It is our great pleasure to welcome you to the Seventeenth International Conference on Availability, Reliability, and Security (ARES 2022).

ARES 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.

Having ARES in real life again with the possibility to interact personally is a great delight for us after two virtual conferences in 2020 and 2021. In 2022, ARES not only returns to real life, but also to its origins in Vienna. The city of Vienna with its great cultural atmosphere will provide a perfect environment for exchange of ideas and the discussion of recent advances and work in the field.

This year we are delighted to welcome two exceptional keynote speakers: Delphine Reinhardt, professor at the Universität Göttingen working on computer security and privacy, and Steven Furnell, professor at the University of Nottingham working on human, technological and organizational aspects of cyber security.

ARES has received 142 full, short, and SoK paper submissions this year and after a thorough review process, in which we requested and obtained 416 reviews, 25 full papers, 7 short papers and 5 SoK papers got accepted. For full papers this yields an acceptance ratio of 21,73%.

The quality of submissions has steadily improved over the last years, such that the program committee had to make a couple of difficult decisions when selecting papers. Moreover, several workshops and short papers are included in the program, presenting intermediate results of ongoing research projects and offer interesting starting points for discussions.

Organizing a conference like ARES 2022 requires an incredible amount of work that has only been possible in a team effort. We want to thank first and foremost the authors for submitting their latest research results. We are grateful to the members of the program committee and the reviewers, who have worked very hard in reviewing papers and giving feedback to the authors. We further thank all workshop chairs for their efforts in organizing engaging workshop sessions. Last but not least, we would like to thank Bettina Jaber and Daniela Freitag David from SBA Research for their support in the organization.

Enjoy ARES 2022, which is finally organized as an in-person event again.

**Dominik Engel**  
*Salzburg University of Applied Sciences,  
Austria*

**Mathias Fischer**  
*Universität Hamburg,  
Germany*

# CD-MAKE 2022

## 6th International Cross Domain Conference for Machine Learning & Knowledge Extraction

### Welcome Message from CD-MAKE Chairpersons

The International Cross Domain Conference for Machine Learning & Knowledge Extraction CD-MAKE is a joint effort of IFIP TC 5, TC 12, IFIP WG 8.4, IFIP WG 8.9 and IFIP WG 12.9 and is held in conjunction with the International Conference on Availability, Reliability and Security (ARES) – this time in beautiful Vienna, Austria. Thanks to the current good situation of the Corona Pandemic which affected us all heavily, we are all happy that we can meet all our international colleagues and friends in-vivo again.

For those who are new to our meanwhile traditional conference: The letters CD in CD-MAKE stand for "Cross-Domain" and describe the integration and appraisal of different fields and application domains to provide an atmosphere to foster different perspectives and opinions. We are strongly convinced that exactly this cross-domain approach is very fruitful for new developments and novel discoveries. The conference fosters an integrative machine learning approach, considering the importance of data science and visualization for the algorithmic pipeline with a strong emphasis on privacy, data protection, safety and security. It is dedicated to offer an international platform for novel ideas and a fresh look on methodologies to put crazy ideas into business for the benefit of humans. Serendipity is a desired effect and shall cross-fertilize methodologies and transfer of algorithmic developments.

The acronym MAKE stands for "MACHINE Learning & Knowledge Extraction", a field of Artificial Intelligence (AI) that, while quite old in its fundamentals, has just recently begun to thrive based on both, novel developments in the algorithmic area, and the availability of vast computing resources at a comparatively low cost. Machine learning (ML) studies algorithms that can learn from data to gain knowledge from experience and to generate decisions and predictions. A grand goal is in understanding intelligence for the design and development of algorithms that work autonomously (ideally without a human-in-the-loop) and can improve their learning behaviour over time. The challenge is to discover relevant structural and/or temporal patterns ("knowledge") in data, which is often hidden in arbitrarily high dimensional spaces, and thus simply not accessible to humans. Knowledge Extraction is one of the oldest fields in AI and sees a renaissance, particularly in the combination of statistical methods with classical ontological approaches.

AI currently undergoes a kind of Cambrian explosion and is the fastest growing field in computer science today thanks to the successes in machine learning to help to solve real-world problems. There are many application domains, e.g., in agriculture, climate research, forestry, etc. with many use cases from our daily lives, which can be useful to help to solve various problems. Examples include recommender systems, speech recognition, autonomous driving, cyber-physical systems, robotics, etc. However, to our opinion the grand challenges are in sensemaking, in context understanding, and in decision making under uncertainty, as well as solving the problem of human interpretability, explainability, and verification.

Our real world is full of uncertainties and probabilistic inference enormously influenced AI generally and ML specifically. The inverse probability allows to infer unknowns, to learn from data and to make predictions to support decision- making. Whether in social networks, recommender systems, health applications or industrial applications, the increasingly complex data sets require a joint interdisciplinary effort bringing the human-in-control and to foster ethical, social issues, accountability, retractability, explainability, causability and privacy, safety and security!

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

IFIP is incorporated in Austria by decree of the Austrian Foreign Ministry (20th September 1996, GZ 1055.170/120-I.2/96) granting IFIP the legal status of a non-governmental international organization under the Austrian Law on the Granting of Privileges to Non-Governmental International Organizations (Federal Law Gazette 1992/174). IFIP brings together more than 3500 scientists without boundaries from both academia and industry, organized in more than 100 Working Groups (WGs) and 13 Technical Committees (TCs).

To acknowledge all those who contributed to the efforts and stimulating discussions would be impossible in a preface like this. Many people contributed to the development of this volume, either directly or indirectly, so it would be sheer impossible to list all of them. We herewith thank all local, national and international colleagues and friends for their positive and supportive encouragement. Finally, yet importantly we thank the Springer management team and the Springer production team for their professional support.

This year CD-MAKE received 45 submissions, which all have been carefully reviewed by our program committee in a double-blind review. Finally 23 papers have been accepted and were presented at the conference in Vienna.

Thank you to all! Let's MAKE it cross-domain!

**Andreas Holzinger**  
*Human-Centred AI Lab,  
University of Natural Resources  
and Life Sciences Vienna,  
Austria*

**Peter Kieseberg**  
*St. Pölten University of Applied  
Sciences, Austria*

**Edgar Weippl**  
*University of Vienna,  
SBA Research, Austria*

**A Min Tjoa**  
*Vienna University Of Technology,  
SBA Research, Austria*

# The Workshops

## of the 17th International Conference on Availability, Reliability and Security

### Welcome Message from ARES Workshop Chair

Welcome to the workshops of the seventeenth International Conference on Availability, Reliability and Security (ARES 2022).

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 14 workshops, which range from “start-ups” to well-established ones supporting ARES.

The succeeding listing comprises the workshops of ARES 2022:

**CSA** - The 3rd Workshop on Recent Advances in Cyber Situational Awareness on Military Operations

**CUING** - The 6th International Workshop on Criminal Use of Information Hiding

**FARES** - The 17th International Workshop on Frontiers in Availability, Reliability and Security

**IOSec** - International Workshop on Information & Operational Technology (IT & OT) Security Systems

**IoT-SECFOR** - The 6th International Workshop on Security and Forensics of IoT

**IWAPS** - 2nd International Workshop on Advances on Privacy Preserving Technologies and Solutions

**IWCC** - 11th International Workshop on Cyber Crime

**IWSECC** - 5th International Workshop on Security Engineering for Cloud Computing

**IWSMA** - 11th International Workshop on Security of Mobile Applications

**IWSMR** - 4th International Workshop on Information Security Methodology and Replication Studies

**IWSRSC** - 1st International Workshop on Secure and Resilient Supply Chains

**SecHealth** - The 2nd Workshop on Cybersecurity in Healthcare 4.0

**SSE** - The 8th International Workshop on Secure Software Engineering

**WSDF** - The 15th International Workshop on Digital Forensics

These workshops are organized each on specific topics and thus offer researchers the opportunity to learn from a rich multi-disciplinary experience. The workshop chair would like to thank the workshop organizers for their great efforts in the workshop proposal, paper selection, program generation and arrangements during the conference. Furthermore, we are also thankful for everyone who further contributes to and supports the workshops. We hope you enjoy the workshop programs and proceedings.

**Maria Leitner**

*University of Vienna,*

*AIT Austrian Institute of Technology, Austria*

# The 8th EU Projects Symposium at ARES 2022

## Welcome Message from ARES EU Symposium Workshop Chair

The ARES EU Projects Symposium is held for the sixth 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.

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

**CS-EDU** - International Workshop on Collaborative Cyber Security Education

**CyberSANE** - International Workshop on Cybersecurity on Critical Infrastructures Management

**ENS** - The 5th International Workshop on Emerging Network Security

**EPESec** - 3rd International Workshop on Electrical Power and Energy Systems Safety, Security and Resilience

**ETACS** - Workshop on Education, Training and Awareness in Cybersecurity

**IWCSEC** - International Workshop on Continuous Software Evaluation and Certification

**IWPSMTS** - International Workshop on Privacy and Security of Multi-Modal Transport Systems

**NG-SOC** - 4th International Workshop on Next Generation Security Operations Centers

**PCSCI** - International Workshop on Physical and Cyber Security in Interdependent Critical Infrastructures

**SECPID** - 4th Workshop on Security, Privacy, and Identity Management in the Cloud

**SP2I** - The 2nd International Workshop on Security and Privacy in Intelligent Infrastructures

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*









Tuesday - August 23, 2022 - morning

Time (UTC +2)	HS 01	SR03	SR 04	SR 05	SR 06	SR 07	SR 08
08:00 19:00	Organizers available						
08:45 09:00	ARES Opening Edgar Weippl, Mathias Fischer 📍 HS 01						
09:00 09:10	EU- Workshop Pitch Session 📍 Florian Skopik 📍 HS 01						
09:10 10:30	ARES Keynote 📍 Steve Fumell 📍 HS 01						
10:30 10:45	Short Coffee Break						
10:45 12:45	HS 01	SR03	SR 04	SR 05	SR 06	SR 07	SR 08
	ARES I Best Paper	EPESec I	IWCSEC I	NG - SOC I	SP2I I	ETACS I	SECPID I
12:45 13:45	Lunch Break						

## Tuesday - August 23, 2022 - afternoon

13:45 15:15	HS 01 IWPSMTS I	SR03 EPESec II	SR 04 IWCSEC II	SR 05 NG - SOC II	SR 06 SP2I II	SR 07 ETACS II	SR 08 SECPID II
15:15 15:45	Coffee Break						
15:45 17:15	HS 01 IWPSMTS II	SR03 EPESec III	SR 04 ENS I	SR 05 PCSCI I	SR 06 SP2I III	SR 07 CyberSane I	SR 08 CS-EDU
17:15 17:30	Short Coffee Break						
17:30 19:00	HS 01 IWPSMTS III		SR 04 ENS II	SR 05 PCSCI II		SR 07 CyberSane II	
19:15 23:30	Evening Reception and "Welcome back to ARES" Party						

Time (UTC +2)	HS 01	SR03	SR 04	SR 05	SR 08
08:30 17:30	Organizers available				
08:45 10:00	<b>ARES Keynote</b>  Delphine Reinhardt  HS 01				
10:00 10:30	Coffee Break				
10:30 12:00	HS 01	SR03	SR 04	SR 05	SR 08
	<b>ARES II</b>	<b>CD-MAKE I</b>	<b>ENS III</b>	<b>CUING I</b>	<b>CSA I</b>
12:00 13:00	Lunch Break				
13:00 14:30	HS 01	SR03	SR 04	SR 05	SR 08
	<b>ARES III</b>	<b>CD-MAKE II</b>	<b>ENS IV</b>	<b>CUING II</b>	<b>CSA II</b>
14:30 15:00	Coffee Break				
15:00 16:30	HS 01	SR03	SR 04	SR 05	SR 08
	<b>ARES IV</b>	<b>CD-MAKE III</b>	<b>WSDF</b>	<b>CUING III</b>	<b>IWSECC</b>
16:30 16:45	Short Coffee Break				
16:45 17:30	<b>CD-MAKE Keynote</b>  R.G. Goebel  HS 01				
19:00 20:30	<b>Sightseeing Tour Schönbrunn Palace</b>				

Time (UTC +2)	HS 01	SR03	SR 04	SR 05	SR 08
08:15 18:00	Organizers available				
08:30 10:00	HS 01	SR03	SR 04	SR 05	SR 08
	<b>ARES V</b>	<b>CD-MAKE IV</b>	<b>IoT-SECFOR I</b>	<b>CUING IV</b>	<b>IWAPS I</b>
10:00 10:15	Short Coffee Break				
10:15 11:45	HS 01	SR03	SR 04	SR 05	SR 08
	<b>ARES VI</b>	<b>CD-MAKE V</b>	<b>IoT-SECFOR II</b>	<b>FARES I</b>	<b>IWAPS II</b>
11:45 12:45	Lunch Break				
12:45 14:00	<b>CD-MAKE Keynote</b>  Matthew E. Taylor  HS 01				
14:00 14:30	Coffee Break				
14:30 16:00	HS 01	SR03	SR 04	SR 05	SR 08
	<b>ARES VII</b>	<b>IWSMR</b>	<b>SecHealth I</b>	<b>FARES II</b>	<b>IWAPS III</b>
16:00 16:30	Coffee Break				
16:30 18:00	HS 01	SR03	SR 04	SR 05	SR 08
	<b>ARES VIII</b>	<b>IWSMA IWSRSC Joint Session</b>	<b>SecHealth II</b>	<b>IWCC</b>	<b>IWAPS IV</b>
19:00 20:30	Traditional Viennese Conference Dinner				

Time (UTC +2)	HS 01	SR03	SR 04	SR 05
08:45 - 14:45	Organizers available			
09:00 - 10:15	ARES Keynote ✍ Alexander Jung 👤 HS 01			
10:15 - 10:45	Coffee Break			
10:45 - 12:15	HS 01	SR03	SR 04	SR 05
	ARES IX	CD-MAKE VI	IOSec I	SSE I
12:15 - 13:15	Lunch Break			
13:15 - 14:45	HS 01		SR 04	SR 05
	ARES X		IOSec II	SSE II

Want to find out more about ARES detailed program?  
Scan this QR code.



# Keynotes

## ARES Keynotes



**Steven Furnell**

*University of Nottingham, United Kingdom*

### **The strange world of the password**

Despite years of evidence of poor practice, people continue to choose weak passwords and continue to be allowed to do so. Normally, if something is broken then the answer is to fix or replace it. However, with passwords the problem seems able to persist unchecked and we continue to use them extensively despite the flaws. Adding further evidence of the issue, this presentation reports on the fifth run of a study into the provision of password guidance and

the enforcement of password rules by a series of leading websites. The investigation has been conducted every 3-4 years since 2007 and the latest findings continue to reveal areas of notable weakness. This includes many sites still offering little or no meaningful guidance, and still permitting users to choose passwords that ought to be blocked at source. It seems that while we remain ready to criticise users for making poor choices, we repeatedly fail to take steps that would help them to do better.

**Steven Furnell** is Professor of Cyber Security at the University of Nottingham in the United Kingdom. He is also an Adjunct Professor with Edith Cowan University in Western Australia and an Honorary Professor with Nelson Mandela University in South Africa. His research interests include usability of security and privacy, security management and culture, and technologies for user authentication and intrusion detection. He has authored over 350 papers in refereed international journals and conference proceedings, as well as various books, book chapters and industry reports. Prof. Furnell is the UK representative to Technical Committee 11 (security and privacy) within the International Federation for Information Processing, as well as the editor-in-chief of Information and Computer Security, and a Fellow and board member of the Chartered Institute of Information Security.



**Delphine Reinhardt**  
University of Göttingen, Germany

### **Usable Privacy: Retrospective and Challenges ahead**

Since the introduction of the GDPR and the resulting cookie banners, providing or not our consent to data collection has become a recurrent activity that requests attention and time for each visited website. While consent is an important instrument to protect our privacy, its implementation is a source of annoyance for most website visitors due to its lack of usability. As a result, they may choose the easiest way and click on the most attractive

button without a second thought, thus voiding the original intention beyond an informed consent. To avoid such effects for which the users are not to blame, different usable privacy solutions have been proposed in the past. In this keynote, we will consider the different steps beyond consent in which the users can be involved and detail selected examples. Based on them, we will identify future research directions and discuss challenges that we will need to solve in the next years as a community.

**Prof. Dr.-Ing. Delphine Reinhardt** is a full Professor and Head of the Computer Security and Privacy group at the University of Göttingen. She is a member of the Institute of Computer Science and the Campus Institute Data Science (CIDAS). In 2019, she was nominated as one of 10 worldwide “Rising Stars in Networking and Communications” by N2Women and was awarded the Johann-Philipp-Reis-Preis for outstanding innovative publications. Before moving to Göttingen in January 2018, she was an Assistant Professor at Rheinische Friedrich-Wilhelms-Universität Bonn in Germany from 2014 to 2017, leading the “Privacy and Security in Ubiquitous Computing” group at the Institute of Computer Science 4. She was also associated to the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE) during that time. She completed her doctoral degree in computer science (with distinction) on privacy in participatory sensing in 2013 at Technische Universität Darmstadt. Her dissertation was awarded by the Communication and Distributed Systems Group (KuVS) supported by the German Informatics Society (GI) and ITG-VDE, the Information Technology Society (ITG) of the German Association for Electrical, Electronic and Information Technologies (VDE), as well as the Association of the Friends of the Technische Universität Darmstadt for outstanding academic achievements. Since 2009, she holds a double-degree in electrical engineering from TU Darmstadt and Ecole Nationale Supérieure de l’Electronique et ses Applications (ENSEA), France.



### Alexander Jung

*Assistant Professor, Aalto University, Finland*

*Associate Editor, IEEE Signal Processing Letters*

### Explainable Empirical Risk Minimization

The successful application of machine learning (ML) methods becomes increasingly dependent on their interpretability or explainability. Designing explainable ML systems is instrumental to ensuring transparency of automated decision-making that targets humans. The explainability of ML methods is also an essential ingredient for trustworthy artificial intelligence. A key challenge in

ensuring explainability is its dependence on the specific human user ("explainee").

The users of machine learning methods might have vastly different background knowledge about machine learning principles. One user might have a university degree in machine learning or related fields, while another user might have never received formal training in high-school mathematics. We measure explainability via the conditional entropy of predictions, given some user signal. This user signal might be obtained from user surveys or biophysical measurements.

We propose explainable empirical risk minimization (EERM) principle of learning a hypothesis that optimally balances between the subjective explainability and risk.

The EERM principle is flexible and can be combined with arbitrary machine learning models. We present several practical implementations of EERM for linear models and decision trees. Numerical experiments demonstrate the application of EERM to detecting the use of inappropriate language on social media.

**Alexander Jung** received the Ph.D. degree (with sub auspiciis) in 2012 from Technical University Vienna (TU Vienna). After Post-Doctoral periods at TU Vienna and ETH Zurich, he joined Aalto University as an Assistant Professor for Machine Learning in 2015. He leads the group "Machine Learning for Big Data" that studies explainable machine learning in network-structured data. Prof. Jung first-authored a paper that won a Best Student Paper Award at IEEE ICASSP 2011. He received an AWS Machine Learning Research Award and was the "Computer Science Teacher of the Year" at Aalto University in 2018. Currently, he serves as an associate editor for the *IEEE Signal Processing Letters* and as the chair of the *IEEE Finland Jt. Chapter on Signal Processing and Circuits and Systems*. He authored the textbook, *Machine Learning: The Basics* (Springer, 2022).





## **R.G. Goebel**

*University of Alberta, Canada*

*XAI-Lab in Edmonton, Alberta, Canada*

### **Explanation as an essential component of machine-mediated acquisition of knowledge for predictive models**

Explanation is not a recent invention precipitated by black-box predictive models, but rather a revival of the role of scientific explanation as a remedy to create trust and transparency for applications of machine learning.

We note two strong trends in the grand challenge of the knowledge acquisition bottleneck, and propose that explanatory knowledge must be acquired concurrently in the process of supervised learning. The resource costs to do so must be balanced in a tradeoff of explainability and knowledge acquisition resources, e.g., as in federated learning systems.

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



## **Matthew E. Taylor**

*Director, Intelligent Robot Learning Lab, Associate Professor & Graduate Admissions Chair, Computing Science, Canada*

*Fellow and Fellow-in-Residence, Alberta Machine Intelligence Institute, Canada  
Canada CIFAR AI Chair, Amii*

### **Reinforcement Learning in the Real World: Challenges and Opportunities for Human-Agent Interaction**

While reinforcement learning (RL) has had many successes in video games and toy domains, recent success in high-impact problems shows that this mature technology can be useful in the real world. This talk will highlight some of these successes, with an emphasis on how RL is making an impact in commercial settings, as well as what problems remain before it can become plug-and-play like many supervised learning technologies. Further, we will argue that RL, like all current AI technology, is fundamentally a human-in-the-loop paradigm. This framing will help motivate why additional fundamental research at the interaction of humans and RL agents is critical to helping RL move out of the lab and into the hands of non-academic practitioners.

**Matt Taylor** is an Associate Professor of Computing Science at the University of Alberta, where he directs the Intelligent Robot Learning Lab. He is also a Fellow and Fellow-in-Residence at Amii (the Alberta Machine Intelligence Institute). His current research interests include fundamental improvements to reinforcement learning, applying reinforcement learning to real-world problems, and human-AI interaction. His book “Reinforcement Learning Applications for Real-World Data” by Osborne, Singh, and Taylor is aimed at practitioners without degrees in machine learning and has an expected release date of Summer 2022.



### Joachim Klerx

*Innovation Systems Center, Austrian Institute of Technology, Austria*

#### **Horizon scanning and strategic knowledge management for future military operations**

Actionable information and strategic knowledge have always created competitive advantages in war situations. However, the digital revolution of the last decades has been proven to be a game changer in the strategic knowledge management for future military operations.

Digital innovations did change processes, technologies and capabilities in conflict scenarios and is continuing to do so. This is obvious for operative intelligence, surveillance and reconnaissance (ISR) but is not so obvious for the strategic knowledge management for future military operations.

In this talk, results from long-term monitoring of military cyber research and AI horizon scanning with intelligent agents are presented. After a short introduction into the methodical approach, this talk will summarize the horizon scanning results for future military AI solutions, including some corresponding future threat scenarios, innovations and trends. Finally, the impacts on cyber situational awareness and future security policy perspectives are discussed.

**Dr. Joachim Klerx** is researcher at AIT Innovation Systems Center and visiting researcher at the National Defence Academy. His main research focus is currently the development of new foresight and horizon scanning methods including developing national horizon scanning centres. Some of his achievements in recent years were the development of ISA (Intelligent screening agent) software agents, who are looking for weak signals of emerging issues on the Internet, financed by SESTI an EU project about identification of weak signals developed for emerging issues. In the EU project ETTIS Joachim Klerx worked on a system for threat-identification and political agenda setting. In EFP, he did the engineering for a global knowledge exchange platform for the world foresight community. As visiting researcher at the National Defence Academy, he developed the concept for CDRC (the national horizon scanning centre for cyber security in Austria), which is working since 2014, and ongoing. More recently, he did coordinate the development dark-net crawling suite to identify hidden networks of organized crime (ANITA) and terrorism (DANTE). In ASGARD, he coordinated the development of next generation foresight and horizon scanning technologies for different European Law Enforcement Agencies. In TRACE, he is coordinating the development of a horizon scanning system, to identify hidden networks of global money laundering and corruption.



© Steffen Wendzel

### **Steffen Wendzel**

*Scientific Director Center of Technology & Transfer and Professor, Hochschule Worms, Germany  
Lecturer, FernUniversität Hagen, Germany*

### **Describing Steganography Hiding Methods with a Unified Taxonomy**

Steganography embraces several hiding techniques which spawn across multiple domains, such as digital media steganography, text steganography, cyber-physical systems steganography, network steganography (network covert channels), and filesystem steganography. However,

the related terminology is not unified among the different domains. To cope with this, an attempt has been made in 2015 with the introduction of the so-called “hiding patterns”. Hiding patterns allow to describe hiding techniques in a more abstract manner. Despite significant enhancements, the main limitation of the original taxonomy is that it only considers the case of network steganography. The 2015-taxonomy was optimized over the years (see <https://ih-patterns.blogspot.com>) but a major revision (presented at ARES' CUING'21) has paved the path towards a taxonomy that covers all steganography domains.

This keynote introduces the concept of hiding patterns and reviews the development of the methodology. It will also present a major revision of the patterns-taxonomy, which was developed by a consortium with members from several countries (HS Worms [Germany], CNR [Italy], WUT [Poland], Univ. Goce Delcev [North Macedonia], University of Magdeburg [Germany], and TH Brandenburg [Germany]). The new version of the taxonomy will be made publicly available in mid-August (<https://patterns.ztt.hs-worms.de>).

**Steffen Wendzel** is a Professor of Information Security and Computer Networks at Hochschule Worms, Germany, where he is also the Scientific Director of the Center for Technology and Transfer (ZTT). In addition, he is a lecturer at the Faculty of Mathematics & Computer Science at the FernUniversität in Hagen, Germany, from which he also received his Ph.D. (2013) and Habilitation (2020). Before joining Hochschule Worms, he led a smart building security research team at Fraunhofer FKIE in Bonn, Germany. Steffen (co-)authored more than 170 publications and (co-)organized several conferences and workshops (incl. ARES IWSMR'19-'22) and special issues for major journals, such as IEEE Security & Privacy (S&P), Elsevier Future Generation Computer Systems (FGCS), and IEEE Transactions Industrial Informatics (TII). He is editorial board member of J.UCS and JCSM. His major research focus is on covert channels, network steganography, scientific taxonomy, and IoT security. Website: <https://www.wendzel.de>.



**Christos Xenakis**  
*University of Piraeus, Greece*

### **Distributed Key Management in Microgrids**

Security for smart industrial systems is prominent due to the proliferation of cyber threats threatening national critical infrastructures. Smart grid comes with intelligent applications that can utilize the bidirectional communication network among its entities. Microgrids are small-scale smart grids that enable Machine-to-Machine (M2M) communications as they can operate with some degree of independence from the main grid. In addition to protecting critical microgrid applications, an underlying key management scheme is needed to enable secure M2M message transmission and authentication. Existing key management schemes are not adequate due to microgrid special features and requirements. We propose the Micro sElf-orgaNiSed mAnagement (MENSA), which is the first hybrid key management and authentication scheme that combines Public Key Infrastructure (PKI) and Web-of-Trust concepts in micro-grids. Our experimental results demonstrate the efficiency of MENSA in terms of scalability and swiftness.

**Prof. Christos Xenakis** received his B.Sc degree in computer science in 1993 and his M.Sc degree in telecommunication and computer networks in 1996, both from the Department of Informatics and Telecommunications, University of Athens, Greece. In 2004 he received his Ph.D. from the University of Athens (Department of Informatics and Telecommunications). From 1998–2001, he was with a Greek telecoms system development firm, where he was involved in the design and development of advanced telecommunications subsystems. From 1996–2007, he was a member of the Communication Networks Laboratory of the University of Athens. Since 2007, he is a faculty member of the Department of Digital Systems of the University of Piraeus, Greece, where he currently is a Professor, a member of the Systems Security Laboratory and the director of the Postgraduate Degree Programme, on “Digital Systems Security”. He has participated in numerous projects realized in the context of EU Programs (ACTS, ESPRIT, IST, AAL, DGHOME, Marie Curie, Horizon2020) as well as National Programs (Greek). He is the project manager the CUREX, SECONDO, INCOGNITO and SealedGRID projects, funded by Horizon2020, while he was the project manager of the ReCRED project funded by Horizon 2020 and the technical manager of the UINFC2 project funded by DGHOME/ISEC. He is also a steering committee member of the European Cyber Security Challenge (ECSC) and the leader of the Hellenic Cyber Security Team. He is a member of the editorial board of four Thomson Reuters indexed journals: a) Computers & Security Journal of the Elsevier publishing, b) Computer Communications Journal of the Elsevier publishing, c) IET Information Security of the Institute of Engineering and Technology and d) The Computer Journal of the Oxford University Press. His research interests are in the field of systems, networks and applications security. He has authored more than 100 papers in peer-reviewed journals and international conferences.



© Fabio Di Franco

**Fabio Di Franco**  
ENISA, Greece

### **Cybersecurity Skills Gap: ENISA Analysis and Actions**

Fabio will provide a holistic view on the nature and characteristics of the skills gap in Europe and the results of the joint effort done with other EU players (eg., the pilots of the EU Competence Network). He will report on the European Cybersecurity Skills Framework (ECSF) which aims to close the cybersecurity skills' gap on the European labour market, building comprehensive bridges between European workplace context and learning environment through an EU skills framework. He will also provide insights on the cybersecurity higher education database (CyberHEAD), an initiative to allow young talents to make informed decisions on the variety of possibilities offered by higher education in cybersecurity through an easy-to-use web portal.

***Fabio Di Franco** is currently leading the activities in ENISA on cyber skills development for highly skilled people. He is also responsible for developing and delivering trainings to EU member states and EU institutions on information security management and IT security. Fabio has a PhD in telecommunication engineering and is a Certified Information Systems Security Professional (CISSP).*



© Yulia Cherdantseva

**Yulia Cherdantseva**

*Senior Lecturer at the School of Computer Science & Informatics at Cardiff University, United Kingdom*

### **CyBOK – The Cyber Security Body Of Knowledge**

Cyber Security Body of Knowledge (CyBOK) is a major project sponsored by the UK National Cyber Security Centre with the aim of developing a substantial resource offering a guide to the Cyber Security as a discipline and as a field of professional practice. CyBOK codifies the foundational knowledge in cyber security for education and professional training. It is an open and freely accessible resource ([www.cybok.org](http://www.cybok.org)) developed by the Community with contributions from over 115 experts across the world since 2017. CyBOK v1.1 is constituted by 21 knowledge areas. There are also free supplementary resources for students, educators and trainers, e.g. podcasts, resources for developing programmes based on CyBOK, lab materials, case studies for use in classroom, etc. This presentation will describe the process of developing CyBOK and maintaining it up to date, discuss the role of the international community in this process, outline the use cases of CyBOK and the future directions of the CyBOK project evolution.

***Dr. Yulia Cherdantseva** is a Senior Lecturer at the School of Computer Science & Informatics at Cardiff University. Yulia worked as a lead researcher on the project "Supervisory Control and Data Acquisition Systems Cyber Security Lifecycle (SCADA-CSL)" funded by the Airbus Group Endeavour Wales and the Welsh Assembly Government, where she developed a novel SCADA Cyber Security, Safety and Risk (SCADA CSSR) graphical extension for BPMN 2.0 and a configurable dependency model of a SCADA*



system. In 2020-2021, she led an NCSC and RISCS funded project about cyber-security decision-making by SMEs which resulted in the development of the Best Practice Guide for SME in Cyber Security Investment Decision-Making. In 2021, she was awarded an EPSRC grant for developing a framework for risk-informed and metrics-enriched cybersecurity playbooks for enhancing CNI resilience. Yulia is a cyber skills lead at the School and is interested in cybersecurity education from the primary school up to professional development level. Since May 2021, Yulia is a member of the CyBOK Executive Board. Yulia is passionate about equality and diversity in cybersecurity – she is a member of the CII Sec's Steering Committee "Women in Cyber" and of the CREST's working group on Inclusion and Diversity.

## IOSec Keynote



### George Spanoudakis

City University London, United Kingdom

#### Security for Healthcare Services: Needs, Solutions and Challenges

This talk reviews the current state of practice and state of the art in the security of healthcare services. More specifically, it reviews the key security challenges faced by healthcare service providers, the types of security assessments needed, the methods for security risk management, and the landscape of the security solutions available. The latter are reviewed in terms of maturity and

the expectations for emerging solutions in the short (1-2 years) and medium-term (3-5 years).

**Prof. George Spanoudakis** (BSc, MSc, and Ph.D. in Computer Science) is the chairman of the management board of SPHYNX TECHNOLOGY SOLUTIONS AG and a Professor of Software Engineering at City University London and Director of the Centre of Adaptive Computing Systems (CeNACS). His research interests are in software systems security, software engineering and biomedical computing. In these areas, he has published extensively (more than 175 peer-reviewed publications with more than 4100 citations, and an H-index of 33).

Professor Spanoudakis has more than 20 years of expertise in managing R&D projects and has received more than €120m of R&D funding from national funding bodies, the EU, and directly from the industry. In total, he has been the principal investigator of more than thirty FP6, FP7, and H2020 projects at Sphynx and prior to it at City, University of London. In several of these projects, he has been the scientific and technical coordinator (e.g., CUMULUS, EVOTION, CYBERSURE, BIO-PHOENIX, SMART BEAR). Professor Spanoudakis has been in the program committees of more than 190 international conferences and has chaired several of them including, for example, ENASE 2019, SCC 2018, ENASE 2018, SEKE 2007, and SEKE 2006. He has also been a member of the editorial boards of several international journals.



### **Sokratis K. Katsikas**

*Director of the Norwegian Centre for Cybersecurity in Critical Sectors*

*Professor with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Norway*

### **Cyber Security when IT meets OT**

The current trend of automation and data exchange in industry, through the development, use and integration of cyber-physical systems, the Internet of things, cloud computing, artificial intelligence and other enabling technologies is expected to bring tremendous benefits in the economy, including improved productivity and efficiency, better flexibility and agility, and increased profitability. However, it also comes with increased cybersecurity risks, primarily deriving from the integration of information technology and operational technology. Thus, as in all cases of a major shift in computing paradigms, a number of cybersecurity challenges arise, that cannot be addressed by simply porting solutions from other domains. In this talk a brief overview of such challenges, and current best practices for addressing them, as well as open issues will be provided.

**Sokratis K. Katsikas** was born in Athens, Greece, in 1960. He is the Director of the Norwegian Centre for Cybersecurity in Critical Sectors and Professor with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Norway. He is also Professor Emeritus of the Department of Digital Systems, University of Piraeus, Greece. In 2019 he was awarded a Doctorate Honoris Causa from the Department of Production and Management Engineering, Democritus University of Thrace, Greece. In 2021, he was ranked 7th in the security professionals category of the IFSEC Global influencers in security and fire list. He has authored or co-authored more than 300 journal papers, book chapters and conference proceedings papers. He is serving on the editorial board of several scientific journals, he has co-authored/edited 46 books and has served on/chaired the technical programme committee of more than 800 international scientific conferences. He chairs the Steering Committee of the ESORICS Conference and he is the Editor-in-Chief of the International Journal of Information Security.





**Reijo M. Savola**  
*University of Jyväskylä, Finland*

### **IoT security for smart health and smart assisted living**

IoT solutions are in the core of effective and efficient smart health and smart assisted living solutions. Considerable increase in well-being and cost savings can be achieved by them. During the last years, IoT cybersecurity threat landscape has become wider, due to the rapidly increasing use of IoT in smart services, and the scarce computational resources available in IoT devices. This increases the risk of compromising reliable and secure use of them.

Systematic proactive assistance of IoT-based smart services with cybersecurity services is essential. Cybersecurity should be designed in the services and the technologies used in a seamless way, and automation is needed. In this talk, a brief overview of challenges in IoT security for smart health and smart assisted living is will be provided, with current practices to overcome them, as well as directions for further research.

**Reijo Savola** is currently working as a Project Manager (cybersecurity and software production) at University of Jyväskylä, Faculty of Information Technology, Finland. He has experience in cyber security systems engineering, risk analysis and risk-driven methods, software engineering, telecommunications, and digital signal processing. Earlier, he has worked as Principal Scientist, cybersecurity at VTT Technical Research Centre of Finland. He received the degree of M.Sc. in Electrical Engineering from the University of Oulu, Finland, 1992, and the degree of Licentiate of Technology in Computer Science from the Tampere University of Technology, Finland, 1995. In addition to research experience, he has seven years of industrial experience in telecommunications sector, having worked as a software engineering and digital signal processing projects for Elektrobit Group Plc. in Oulu, Finland and in Redmond, WA, United States. Mr. Savola acts as the Chairman of the Finnish Mirror Group for ISO/IEC JTC1/SC27 standardization (Information security, cybersecurity and privacy protection) and CEO of the Northern European Cybersecurity Cluster (NECC).



© Gabriele Costa

### Gabriele Costa

*IMT School for Advanced Studies Lucca, Italy*

#### **Security-by-Design in Intelligent Infrastructures: the HALL-T orchestrator**

In the last years, Security-by-Design has emerged as the main methodology for securing the life cycle of software and systems. Its effectiveness is the result of a strong integration with all the development phases, from the earliest conceptualization and design to the final disposal. Large scale, critical infrastructures can benefit the most from this approach. Nevertheless, they also carry

an extreme degree of complexity that must be dealt with. In this talk we will consider the SPARTA perspective on the definition and implementation of a secure orchestrator for making intelligent infrastructures Secure-by-Design.

**Assoc. Prof. Gabriele Costa** is Associate Professor at the SySMA Group of the IMT School for Advanced Studies. He received his M.Sc. in Computer Science in 2007 and his Ph.D. in Computer Science in 2011, both at the University of Pisa. He was a member of the cybersecurity group of the Istituto di Informatica e Telematica (IIT) of the CNR. His appointments include a period as visiting researcher at ETH Zurich in 2016-2017. He was co-founder of the Computer Security Laboratory (CSEC) at DIBRIS (Computer Science and Computer Engineering Department of the University of Genoa). He is co-founder and CRO of Talos, a spin-off of DIBRIS focused on Cybersecurity. His main focus is on studying and applying formal methods for the automatic verification and security testing of mobile and modular systems.



© Xiaolu Hou

### Xiaolu Hou

*Faculty of Informatics and Information Technologies, Slovak University of Technology, Slovakia*

#### **Artificial Intelligence-Assisted Side Channel Attacks**

Deep neural networks (DNN) have gained popularity in the last decade due to advances in available computational resources. In particular, side-channel attacks (SCA) have received the most attention as being a classification problem, DNN comes as a natural candidate. In this talk, we will first provide the basics of SCA and explain how it can recover the secret key of a cryptographic

implementation. Then, we will present the recent literature on applications of DNN to SCA. As a demonstration, we will detail a work that aims to propose a general framework that helps users with the overall trace analysis aided by DNN, minimizing the necessity for architecture adjustments by the user.

**Dr. Xiaolu Hou** is currently an Assistant Professor at Slovak University of Technology. She received her Ph.D. degree in Mathematics from Nanyang Technological University, Singapore, in 2017. Her current research focus is on fault injection and side-channel attacks on both cryptographic implementations and neural networks. She also has research experience in AI-assisted cryptanalysis, location privacy, and multiparty computation.



### Andrew Marrington

*Advisor to the Provost for Programs & Curricula at Zayed University, United Arab Emirates*

#### Coming Back to the Backlog: Can Digital Investigations Catch Up?

Digital evidence is crucial in a wide variety of criminal investigations and prosecutions. The digital footprint of everyday life and the proximity of smartphones and other digital devices to physical crime scenes means that the relevance of digital evidence is by no means confined to cybercrime cases. As a result, law enforcement agencies

around the world have huge backlogs of digital evidence awaiting extraction and examination. In the UK alone, the collective backlog is at least 21,000 digital devices (smartphones, computers, tablets, etc), contributing to significant delays in investigations and prosecutions.

For two decades, digital forensics research has been grappling with this backlog in a variety of ways. Researchers have proposed faster methodologies and tools, more automation of the process of examination and analysis, triage techniques to make better use of examiner time, and more. Nevertheless, the problem of large backlogs persists. This keynote considers the causes of the backlog problem, and discusses how the digital forensics community can try to address it in the years ahead.

**Dr. Andrew Marrington** is the Advisor to the Provost for Programs & Curricula at Zayed University. Dr. Marrington received his PhD in digital forensics from Queensland University of Technology (QUT), where he studied at the Information Security Institute. Dr. Marrington's primary field of research is digital forensics, although he is also interested in other aspects of information security, and in the security and investigative implications of emerging technologies. He serves on the program committees of various conferences and workshops in digital forensics and information security, and on the editorial boards of several journals in the same field. With his colleagues Dr. Don Kerr and Dr. John Gammack, he has co-edited a book of refereed chapters on the security of wearable technologies. In the past, he has served as Associate and Acting Dean of the College of Technological Innovation at Zayed University, and in his current capacity he oversees curriculum development and academic quality assurance across the institution.

# Social Events

**Tuesday, August 23, 2022**

## **Evening Reception and “Welcome back to ARES” Party**

After almost 3 years we will welcome you warmly back at ARES & CD-MAKE in Vienna.

The official ARES & CD-MAKE 2022 reception takes place at the Van-Swieten-Saal. Just a short walk away from the main venue, the Van-Swieten-Saal is located at the Medical University of Vienna. Enjoy delicious finger food and drinks, mingle, dance and network. “Welcome back to ARES!”

**SCAN ME**



**Address: Van Swieten - Gasse 1a, 1090 Vienna**

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

**Meeting point**

**19:00**

*in the foyer  
of the University*

**Wednesday, August 24, 2022**

## **Sightseeing Tour Schönbrunn Palace**

**Meeting point**

**18:30**

*in front of  
Schloss Schönbrunn*

We will visit Schönbrunn Palace, the No. 1 sight in Vienna! Join us on this evening's exclusive ARES tour through Schönbrunn, where our guides will tell us everything there is to know about Vienna's imperial residence.

At the end of the seventeenth century Emperor Leopold I commissioned the Baroque architect Johann Bernhard Fischer von Erlach, who had received his training in Rome, to design an imperial hunting lodge for his son, Crown Prince Joseph, later to become Emperor Joseph I.

Replacing the château de plaisance built on this site for the dowager empress Eleonora of Gonzaga in 1642, it was to grow into a palatial imperial residence over the course of the eighteenth century.

**Address: Schönbrunner Schloßstraße 47, 1130 Wien**

**SCAN ME**



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

**Thursday August 25, 2022**

### **Traditional Viennese Conference Dinner**

We will meet at 18.00 after the last session in front of the University. Please keep in mind that there is no possibility to store your laptop at the University.

We have organized a ride with a vintage tram to the Heurigenrestaurant “10er Marie”, the oldest wine tavern of Vienna (1740) and the location of the Mayor's Reception. During the ride you will be able to see several main attractions such as the Vienna State Opera, the Museum of Fine Arts, the Museum of Natural History, the Heldenplatz and the Austrian Parliament.

**Address: Ottakringer Strasse 222-224, 1160 Vienna**

*Want to find out more about “10er Marie”?  
Scan this QR code.*

**Meeting point**  
**18:00**  
*in the foyer  
of the University*

**Don't be late!**  
*The “Bim”  
won't wait.*

**SCAN ME**



## **Conference Venue**

ARES 2022 will be held at the University of Vienna, Austria.  
Lecture halls are located at the Faculty for Computer Science.

### **Address of ARES 2022 Conference**

University of Vienna  
Faculty of Computer Science  
Währinger Straße 29, 1090 Vienna, Austria

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

**SCAN ME**



### **Public transportation**

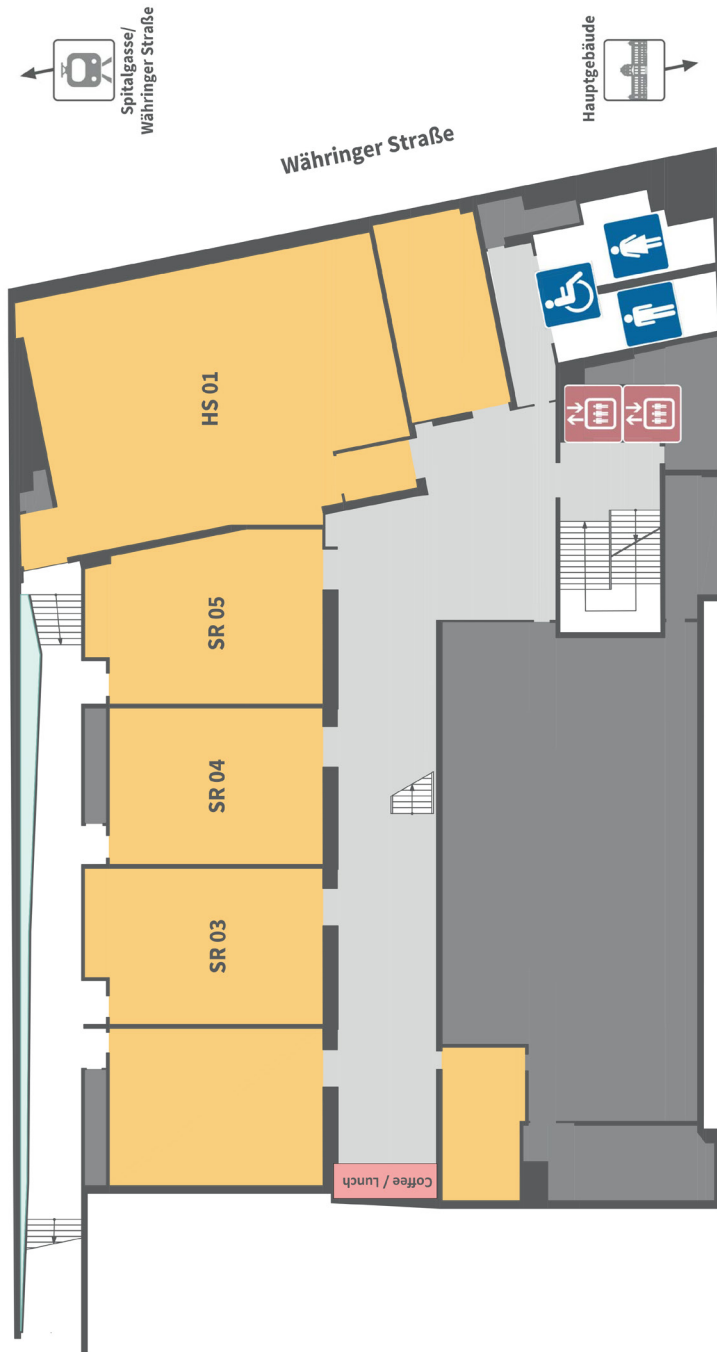
Tram: 37, 38, 40, 41, 42 – stop: Sensengasse or Spitalgasse

## Map - Public Transportation



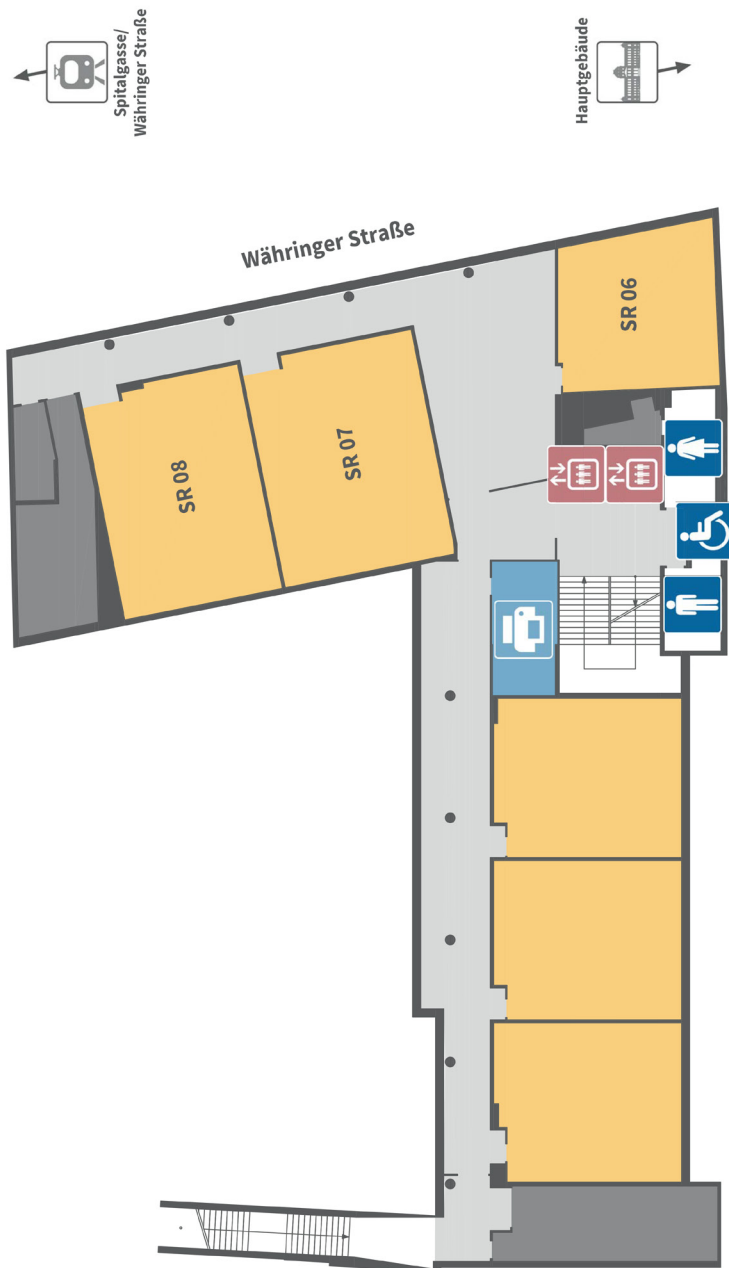
Scan the QR-Code  
and get your tickets  
for Vienna's  
public transportation.

© Wiener Linien, April 2021



## Lecture hall floor plan First Level

## Währinger Straße 29 Übersichtsplan der Veranstaltungsräume 1. Stock







# About Vienna

© SBA Research



Vienna is old, Vienna is new – and so diverse: from the magnificent Baroque buildings to “golden” Art Nouveau or the latest architecture. Vienna is packed with imperial history; at the same time it has exciting contemporary museums, lively eating and a vibrating nightlife, but also many quiet corners to explore.

Few cities can boast the imperial grandeur of Vienna, once the center of the powerful Habsburg monarchy. Lipizzaner stallions performing elegant equine ballet, the angelic tones of the Vienna Boys’ Choir drifting across a courtyard and, outrageously opulent palaces.

The Mercer Study has chosen Vienna as the world’s number one most livable city for the sixth time in a row in 2015. More than half of the metropolitan area is made up of green spaces. 280 imperial parks and gardens enrich the cityscape. It’s hard to imagine a more livable city than Vienna. This is a metropolis where regulars sit in cozy coffee houses and offer credible solutions to the world’s chaos over the noble bean; where “Beisl’n” (bistro pubs) serve delicious brews, wines and traditional food; where talented chefs are taking the capital in new culinary directions; and where an efficient transport system will ferry you across town from a restaurant to a post-dinner drink in no time at all. It’s safe, it has lots of bicycle tracks and it even has its own droll sense of humor.

## Attractions In Vienna

Walk in the footsteps of the Habsburgs, visit the splendid baroque Schönbrunn or Belvedere Palaces, or stroll along the magnificent Ring Boulevard to take a look at the heart of the former vast Habsburg Empire, the Imperial Palace. Get a sense of the luster and glory of the old empire by visiting St. Stephen’s Cathedral, the Spanish Riding School, and the Giant Ferris Wheel at the Prater, as well as the sarcophagi in the Imperial Vault.

## Stephens Cathedral (*Stephansdom*)

St. Stephen's Cathedral is the symbol of Vienna. Construction commenced in the 12th century. Today, it is one of the most important Gothic structures in Austria. Stephen's Cathedral is located directly in the city center, at the religious and geographical heart of Vienna. It's giant Pummerin bell features on television as it rings in the New Year.



© Bild von Gertfried Wagner auf Pixabay



© Bild von andreas N auf Pixabay

## The Ring Boulevard (*Ringstraße*)

Emperor Franz Joseph officially opened Vienna's Ring Boulevard (Ringstrasse) on May 1, 1865. Vienna celebrated its 150th birthday in 2015 with numerous events and exhibitions. The most beautiful boulevard in the world not only rich in sights, it also has large parks, important monuments, and much more. About 800 buildings line the boulevard today. Additional sights on the Ring Boulevard, aside from the many opulent buildings, include the black-gold lattice fence in front of the Hofburg, the world's longest fence from the age of Historicism, the 5.5-meter-tall Pallas Athene statue in front of the Parliament, and the "Rathausmann", a statue of a man on the tower of the City Hall.

## The Culinary Side Of Vienna

Vienna is famous for its cuisine, its coffee house culture and the 'Heurige' wine taverns. Vienna boasts one of the world's most famous culinary traditions. A diverse yet delectably harmonious range of dishes reflects the city's mix of nationalities and food cultures through the centuries, and inspires visitors from all over the globe.

The most famous Viennese dishes are:

Wiener Schnitzel (bread-crumbed and fried veal escalope), Apfelstrudel (an apple-filled pastry), Palatschinken (Viennese crêpes), Sachertorte (a special Viennese chocolate cake) and Kaiserschmarrn (dessert of shredded pancake and stewed fruit).

The Viennese coffee house is known around the globe for its informal pleasantness, as an oasis of "Gemütlichkeit". Traditional cafés entice with a wide variety of coffee drinks, international newspapers and pastry creations. Since 2011, the traditional Viennese coffee house culture has even belonged to the intangible cultural heritage of UNESCO.

*More on eating out and shopping tips in Vienna?  
Scan this QR code.*

SCAN ME



# Useful Information

## WIFI At ARES

There is WIFI available at the venue of ARES 2022: Eduroam  
You will be supplied with a unique Wi-Fi log in order to access University of Vienna's internet during your stay. At the registration desk ARES will provide the participants with WIFI vouchers.

## Emergency Numbers

Fire service	<b>122</b>
Police	<b>133</b>
Emergency doctor	<b>141</b>
Ambulance service	<b>144</b>

The emergency numbers can be called free of charge from any phone in Austria.

## Covid-19 Information

All immigration regulations imposed because of the pandemic have been lifted: 3G proof (tested, vaccinated, recovered) is no longer needed upon arrival. It is therefore possible to enter Austria from all countries of the world again without any restrictions.

**Free Antigen test kits are available at the registration.** We kindly ask you to test at arrival.  
**All participants will be provided with free FFP2 masks.**

If you develop any COVID-19 symptoms during the conference, we ask you not to enter the venue and contact the Conference Office Contact.

## Travel Within Vienna

On all public transportation, such as the Austrian Federal Railways, buses or trams, you must wear an FFP2 mask. Find one for free at the registration desk.

## Conference Office Contact

### Bettina Jaber

Mobile: +43 664 254 03 14

E-Mail: [bjaber@sba-research.org](mailto:bjaber@sba-research.org)

### Daniela Freitag David

Mobile: +43 664 88 00 11 51

E-Mail: [dfreitag-david@sba-research.org](mailto:dfreitag-david@sba-research.org)

# Important Phrases

<b>Hello!</b>	Hallo!	<i>Ha-low!</i>
<b>Hello! (informal)</b>	Servus!	<i>sea-r-wooz!</i>
<b>Goodbye!</b>	Auf Wiedersehen!	<i>Aouf-we-der-zehen!</i>
<b>How are you?</b>	Wie geht's?	<i>Vee gits?</i>
<b>Do you speak English?</b>	Sprechen Sie Englisch?	<i>Shprexh-en zee eng-lish?</i>
<b>Can you help me?</b>	Können Sie mir helfen?	<i>Kuh-nen zee mir hel-fen?</i>
<b>You're welcome.</b>	Bitte gerne.	<i>Bi-te ger-nay.</i>
<b>Please.</b>	Bitte.	<i>Bi-te.</i>
<b>Yes.</b>	Ja.	<i>Ya.</i>
<b>No.</b>	Nein.	<i>Niyn.</i>
<b>I don't know</b>	Ich weiß nicht.	<i>Ikhw wise nikht.</i>
<b>I (don't) understand.</b>	Ich verstehe (nicht).	<i>Ikhw ver-shte-he (nikht).</i>
<b>Okay.</b>	Okay.	<i>Okay.</i>
<b>Help!</b>	Hilfe!	<i>Heel-fe!</i>
<b>Thank you</b>	Danke.	<i>Dan-ker.</i>
<b>Thank you very much</b>	Vielen Dank!	<i>Vee-len dank.</i>
<b>Excuse me. / Sorry.</b>	Entschuldigen Sie.	<i>Ent-schul-dig'n zee.)</i>
<b>I'm sorry.</b>	Es tut mir leid.	<i>Es toot mir lied.</i>
<b>Good morning!</b>	Guten Morgen!	<i>Goot-en mor-gen/targ!</i>
<b>Good evening!</b>	Guten Abend!	<i>Goot-en-ar-bent!</i>
<b>Good night!</b>	Gute Nacht!	<i>Goot-er naxht!</i>
<b>See you later!</b>	Bis später!	<i>Biz spae-ter!</i>

# Notes



# Organizers And Supporters



## ARES Conference

*International Conference on Availability, Reliability and Security*

ARES 2022 is organized by



Supported by



MEETING  
DESTINATION  
VIENNA  
NOW ♦ TOGETHER



### 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 SQL. 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.

