

ARES

23

18th International Conference on
Availability, Reliability & Security



PROGRAM GUIDE

29 Aug. – 1 Sep. 2023
Benevento, Italy

Table of Content



© SBA Research

Welcome Messages	4
ARES Program Committee Co-Chairs	4
CD-MAKE Chairpersons	6
ARES Workshop Chairs	10
ARES EU Symposium Workshop Chair	12
Program Overview	14
Tuesday August 29th	15
Wednesday August 30th	16
Thursday August 31st	17
Friday September 1st	18
ARES Women* Session	19
Keynotes	20
ARES Keynotes	20
CD-MAKE Keynotes	22
Workshops Keynotes	24
Social Events	38
Welcome Reception	38
Conference Dinner	39
Conference Venue	40
Venue Details	41
Floor Plan	42
About Benevento	44
Gregorio's Tips for Benevento	47
Useful Information	50
Important Phrases	51
Organizers and Supporters	52

Welcome Messages

Welcome Message from ARES Program Committee Co-Chairs

Dear attendee, a warm welcome to ARES 2023!

The Eighteenth International Conference on Availability, Reliability, and Security (ARES 2023) 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, we are hosted in Benevento, which provides a wonderful and historic setting, as well as a warm atmosphere for all of us who have come to enjoy the great traditions of the Italian South.

This year, the main conference is organized in nine technical sessions, including a session dedicated to the candidates for the Best Paper Award.

We are also honored to host four brilliant keynote speakers:

Elisa Costante, vice president of research at Forescout Technologies, leading a team of cyber security researchers focused on vulnerability research.

Pierangela Samarati, professor at the University of Milan, working on



data and applications security and privacy.

Mireille Hildebrandt, research professor on 'Interfacing Law and Technology' at Vrije Universiteit Brussels and co-Director of the Research Group on Law Science Technology as well as Society studies at the Faculty of Law and Criminology.

Michael Bronstein, DeepMind professor of Artificial Intelligence at the University of Oxford, and head of Graph Learning Research at Twitter.

ARES has received 142 regular papers, 14 SoK papers, and 27 short papers. After desk-rejecting 6 regular papers and 1 short paper, we have accepted 28 regular papers, 3 SoK papers, and 4 short papers. For regular papers, this yields an acceptance rate of 19.7% (considering submitted papers) and 20.6% (considering reviewed papers).

We want to thank all the authors 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 and Daniela Freitag David, from SBA Research, for their relentless support in the organization.

Enjoy ARES 2023!

Maryline Laurent

Télécom SudParis, France

Riccardo Scandariato

*Hamburg University of
Technology, Germany*

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 Benevento, Italy. Thanks to overcoming 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 Ex-traction”, 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, re-tractability, 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 3.500 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.

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

Andreas Holzinger

*Human-Centred AI Lab,
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*



Welcome Message from ARES Workshop Chairs

Welcome to the workshops of the 18th International Conference on Availability, Reliability, and Security (ARES 2023). These workshops play a crucial role in the ARES conference by offering researchers and practitioners from different domains a valuable platform to present and discuss their research findings and work-in-progress.

This year, we are pleased to offer conference attendees a diverse selection of 12 workshops – ranging from emerging “start-ups” to well-established workshops – that all contribute to the success of ARES.

Davy Preuveneers

*imec-DistriNet, KU Leuven,
Belgium*

Andreas Unterweger

*Salzburg University of Applied Sciences,
Austria*



THE WORKSHOPS

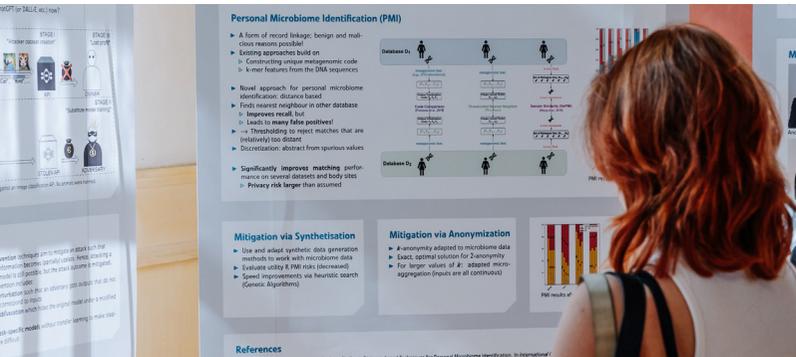
of the 18th International
Conference on Availability,
Reliability and Security

The succeeding listing comprises the workshops of ARES 2022:

CSA	The 4th Workshop on Recent Advances in Cyber Situational Awareness on Military Operations
CUING	The 7th International Workshop on Criminal Use of Information Hiding
EPIC-ARES	Interdisciplinary Workshop on Applied Research in Embedded, Purpose-specific, Integrated Computing and their Availability, Reliability and Security
FARES	The 18th International Workshop on Frontiers in Availability, Reliability and Security
GRASEC	The 4th International Workshop on Graph-based Approaches for Cyber-Security
IoT-SECFOR	The 7th International Workshop on Security and Forensics of IoT
IWAPS	3rd International Workshop on Advances on Privacy Preserving Technologies and Solutions
IWCC	12th International Workshop on Cyber Crime
IWSECC	6th International Workshop on Security Engineering for Cloud Computing
SecIndustry	The 2nd Workshop on Cybersecurity in Industry 4.0
SSE	The 9th International Workshop on Secure Software Engineering
Trustbus	20th International Workshop on Trust, Privacy and Security in the Digital Society
WSDF	The 16th International Workshop on Digital Forensics

Welcome Message from ARES EU Symposium Workshop Chair

The ARES EU Projects Symposium is held for the ninth 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.



© SBA Research

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

CS-EDU	International Workshop on Collaborative Cyber Security Education
DFIR-Train	Workshop Teaching and Training in Digital Forensics and Incident Response
ENS	The 6th International Workshop on Emerging Network Security
EPESec	4th International Workshop on Electrical Power and Energy Systems Safety, Security and Resilience
ETACS	Workshop on Education, Training and Awareness in Cybersecurity
PCSCI	International Workshop on Physical and Cyber Security in Interdependent Critical Infrastructures
SECPID	5th Workshop on Security, Privacy, and Identity Management in the Cloud
SP2I	The 3rd International Workshop on Security and Privacy in Intelligent Infrastructures
STAM	The 3rd International Workshop on Safety and Security Testing and Monitoring

Program Overview



© SBA Research

Tuesday | August 29th

Time (UTC +2)	SA 1	SA 2	SA 3	SA 4	SA 7	SA 9
08:30 18:00	Organizers available 					
09:00 10:30	ETACS I	DFIR-Train I	SP2I I		STAM I	EPESec I
10:30 11:00	Coffee Break 					
11:00 12:30	ETACS II	DFIR-Train II	SP2I II		STAM II	EPESec II
12:30 13:30	Lunch Break 					
13:30 15:00	ETACS III	ENS I	SP2I III	CS-EDU I	CD-MAKE I	PCSCI I
15:00 15:30	Coffee Break 					
15:30 17:00		ENS II	SECPID	CS-EDU II	CD-MAKE II	PCSCI II
17:00 17:15	Coffee Break 					
17:15 18:30	CD-MAKE Keynote Speaker: Michael Bronstein Room: Auditorium					
19:00 22:00	Welcome Reception 					

Time (UTC +2)	SA 1	SA 2	SA 3	SA 4	SA 7	SA 9
08:30 18:00	Organizers available 					
09:00 09:15	ARES Opening Speaker: Maryline Laurent, Riccardo Scandariato Room: Auditorium					
09:15 10:30	ARES Keynote Speaker: Elisa Costante Room: Auditorium					
10:30 11:00	Coffee Break 					
11:00 12:30	SecIndustry I	IWAPS I	Trustbus I	IWCC I	IoT-SECFOR I	CSA
12:30 13:30	Lunch Break 					
13:30 15:00	SecIndustry II	IWAPS II	Trustbus II	IWCC II	IoT-SECFOR II	GRASEC
15:00 15:30	Coffee Break 					
15:30 17:00	SecIndustry III	IWAPS III	Trustbus III	CUING I	WSDF I	FARES I
17:00 17:15	Coffee Break 					
17:15 18:45	SecIndustry IV	IWAPS IV		CUING II	WSDF II	FARES II

Thursday | August 31st

Time (UTC +2)	SA 1	SA 2	SA 3
08:30 18:00	Organizers available 		
09:00 10:30	ARES I	ARES II	ARES III
10:30 11:00	Coffee Break 		
11:00 12:30	ARES IV	ARES V	ARES VI
12:30 13:30	Lunch Break 		
13:30 15:00	ARES VII Best Paper Room: Auditorium		
15:00 15:30	Coffee Break 		
15:30 17:00	ARES VIII	ARES IX	ARES Women* Session
17:00 17:15	Coffee Break 		
17:15 18:30	ARES Keynote Speaker: Pierangela Samarati Room: Auditorium		
19:00 20:30	Conference Dinner 		

Friday | September 1st

Time (UTC +2)	SA 1	SA 2	SA 3
08:30 16:30	Organizers available 		
09:00 10:15	CD-MAKE Keynote Speaker: Mireille Hildebrandt Room: Auditorium		
10:15 10:45	Coffee Break 		
10:45 12:15	CD-MAKE III	EPIC-ARES I (joint session with SSE and IWSECC)	FARES III
12:15 13:15	Lunch Break 		
13:15 14:45	CD-MAKE IV	EPIC-ARES II (joint session with SSE and IWSECC)	
14:45 15:00	Coffee Break 		

SA 3

31st Aug.

15:30–17:00

ARES Women*

Session

We are thrilled to announce that the ARES 2023 Conference will host its first-ever Women* Session!

This new event will bring together women* from the realms of technology, research, and cybersecurity to share their experiences, insights, and visions.

The ARES Women* Session provides a space for exchanging ideas, building connections, and empowering the presence of women* in an industry continuously striving for diversity and inclusivity.

Note: By 'Women*', we refer to all individuals who identify as women or define themselves as female.

The session is open to all who identify and perceive themselves in this way.

SCAN ME

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



Keynotes

ARES Keynotes

Elisa Costante

VP of Research at Forescout Technologies

The Threat Landscape is Constantly Evolving – And So Must Security Solutions. Cyber-criminal organizations, new ransomware tactics, and the proliferation of IoT/OT/loMT devices have rapidly changed the modern threat landscape. To devise effective security solutions, security practitioners and researchers must pay close attention to the continuously evolving cyber threats. In this presentation, I'll explore the last ten years of cyber threats and provide predictions for future trends. I'll also identify opened research questions the industry is looking for that could help further enhance security measures and protect our networks against new and potential threats.

Elisa Costante is the VP of Threat Research at Forescout. In her role, she leads the activities of Vedere Labs, a team of cyber security researchers focused on vulnerability research, threat analysis and threat mitigation. She has 10+ years of experience in the security challenges posed by the IT/OT/IoT convergence. In her prior role she was CTO at SecurityMatters, where she led product innovation activities in the field of network intrusion detection. Elisa holds a PhD in Cyber Security from the Eindhoven University of Technology where she specialized in machine learning techniques for data leakage detection.

Auditorium

30th Aug.

09:15–10:30

Exploring the Cyber Threat Landscape: Analyzing the Past to Uncovering Future Trends

© Elisa Costante



Pierangela Samarati

Università degli Studi di Milano, Italy

Auditorium

31st Aug.

17:15–18:30

Data security and privacy in emerging scenarios

The rapid advancements in Information and Communication Technologies (ICTs) have been greatly changing our society, with clear societal and economic benefits. Mobile technology, Cloud, Big Data, Internet of Things, services and technologies that are becoming more and more pervasive and conveniently accessible, towards to the realization of a 'smart' society. At the heart of this evolution is the ability to collect, analyze, process and share an ever-increasing amount of data, to extract knowledge for offering personalized and advanced services.

A major concern, and potential obstacle, towards the full realization of such evolution is represented by security and privacy issues. As a matter of fact, the (actual or perceived) loss of control over data and potential compromise of their confidentiality can have a strong detrimental impact on the realization of an open framework for enabling collection, processing, and sharing of data, typically stored or processed by external cloud services. In this talk, I will illustrate some security and privacy issues arising in emerging scenarios, focusing in particular on the problem of managing data while guaranteeing confidentiality and integrity of data stored or processed by external providers.

Pierangela Samarati is a Professor at the Department of Computer Science of the Università degli Studi di Milano, Italy. Her main research interests are on data and applications security and privacy, especially in emerging scenarios. She has participated in several EU-funded projects involving different aspects of information protection, also serving as project coordinator. She has published more than 290 peer-reviewed articles in international journals, conference proceedings, and book chapters. She has been Computer Scientist in the Computer Science Laboratory at SRI, CA (USA). She has been a visiting researcher at the Computer Science Department of Stanford University, CA (USA), and at the Center for Secure Information Systems of George Mason University, VA (USA). She is the chair of the IEEE Systems Council Technical Committee on Security and Privacy in Complex Information Systems (TCSPCIS), of the ERCIM Security and Trust Management Working Group (STM), and of the ACM Workshop on Privacy in the Electronic Society (WPES). She is a member of several steering committees. She is IEEE Fellow (2012), ACM Fellow (2021), IFIP Fellow (2021). She has received the IEEE Computer Society Technical Achievement Award (2016) and the ESORICS Outstanding Research Award (2018).

© Pierangela Samarati



Michael Bronstein

University of Oxford, United Kingdom

Auditorium

29th Aug.

17:15–18:30

The message-passing paradigm has been the “battle horse” of deep learning on graphs for several years, making graph neural networks a big success in a wide range of applications, from particle physics to protein design. From a theoretical viewpoint, it established the link to the Weisfeiler-Lehman hierarchy, allowing to analyse the expressive power of GNNs. We argue that the very “node-and-edge”-centric mindset of current graph deep learning schemes may hinder future progress in the field. As an alternative, we propose physics-inspired “continuous” learning models that open up a new trove of tools from the fields of differential geometry, algebraic topology, and differential equations so far largely unexplored in graph ML.

Physics-inspired learning on graphs

Michael Bronstein is the DeepMind Professor of AI at the University of Oxford and Head of Graph Learning Research at Twitter. He was previously a professor at Imperial College London and held visiting appointments at Stanford, MIT, and Harvard, and has also been affiliated with three Institutes for Advanced Study (at TUM as a Rudolf Diesel Fellow [2017-2019], at Harvard as a Radcliffe fellow [2017-2018], and at Princeton as a short-time scholar [2020]). Michael received his PhD from the Technion in 2007. He is the recipient of the Royal Society Wolfson Research Merit Award, Royal Academy of Engineering Silver Medal, five ERC grants, two Google Faculty Research Awards, and two Amazon AWS ML Research Awards. He is a Member of the Academia Europaea, Fellow of IEEE, IAPR, BCS, and ELLIS, ACM Distinguished Speaker, and World Economic Forum Young Scientist. In addition to his academic career, Michael is a serial entrepreneur and founder of multiple startup companies, including Novafora, Invision (acquired by Intel in 2012), Videocites, and Fabula AI (acquired by Twitter in 2019).

© Michael Bronstein



Mireille Hildebrandt

Co-Director LSTS, Vrije Universiteit Brussel (VUB), Belgium

Auditorium

1st Sep.

09:00–10:15

The deployment of AI systems based on machine learning (ML) in real world scenarios faces a number of challenges due to its black box nature. The GDPR right to an explanation has given rise to frantic attempts to develop and design self-explanatory systems, meant to help people understand their decisions and behaviour. In this keynote I will explain (pun intended) why meaningful explanations require keen attention to the proxies used in ML research design. Once those confronted with the decisions or behaviour of ML systems have a better understanding of the pragmatic choices that must be made to allow a machine to learn, it will become easier to foresee what ML systems can and cannot do. Whiteboxing ML should focus on the proxies that stand for real world events, actions and states of affairs, highlighting that a proxy (dataset, variable, model) is not what it stands for.

Whiteboxing machine learning

Mireille Hildebrandt is a Research Professor on 'Interfacing Law and Technology' at Vrije Universiteit Brussels (VUB), appointed by the VUB Research Council. She is co-Director of the Research Group on Law Science Technology and Society studies (LSTS) at the Faculty of Law and Criminology. She also holds the part-time Chair of Smart Environments, Data Protection and the Rule of Law at the Science Faculty, at the Institute for Computing and Information Sciences (iCIS) at Radboud University Nijmegen.

© Mireille Hildebrandt



Her research interests concern the implications of automated decisions, machine learning and mindless artificial agency for law and the rule of law in constitutional democracies. Hildebrandt has published 5 scientific monographs, 23 edited volumes or special issues, and over 100 chapters and articles in scientific journals and volumes. She received an ERC Advanced Grant for her project on 'Counting as a Human Being in the era of Computational Law' (2019-2024), that funds COHUBICOL. In that context she is co-founder of the international peer reviewed Journal of Cross-Disciplinary Research in Computational Law, together with Laurence Diver (co-Editor in Chief is Frank Pasquale). In 2022 she has been elected as a Fellow of the British Academy (FBA).

Martin Steinebach

Fraunhofer Institute, Germany

SA 4

30th Aug.

15:30–17:00

The keynote will address the critical importance of false positive rates in multimedia forensics, a field dedicated to the identification, classification, and authentication of digital content. While the field has historically focused on true positives, this talk aims to highlight the importance of false positives and their impact on forensic investigations and other applications.

The talk will explore the causes of false positives, including limitations of forensic techniques, algorithmic biases, and the inherent complexity of multimedia analysis. It will emphasize the trade-off between false positives and false negatives, and the need for a balanced approach that is appropriate for a given application. The requirements can be very different between monitoring solutions such as upload filters or chat control on the one hand and individual analysis on the other. Steganalysis is another good example: error rates and their consequences depend heavily on the goals of a steganalysis application. While searching for occurrences of the use of simple steganographic tools may allow acceptable error rates, broad monitoring of state-of-the-art embedders with realistic payloads and usage frequencies seems to be at least challenging.

Overall, this talk aims to raise awareness of the importance of false positive rates in multimedia security and to inspire the audience to contribute to the advancement of reliable and fair forensic practices in an increasingly digital world.

Error Rates in Multimedia Forensics

Martin Steinebach heads the Media Security and IT Forensics department at the Fraunhofer Institute for Secure Information Technology SIT. He studied computer science at the TU Darmstadt from 1992 to 1999. In 2003, he received his PhD in Computer Science from the TU Darmstadt with the topic of digital audio watermarking. In March 2002, he became head of the MERIT department at Fraunhofer IPSI, which dealt with media data security, and of the C4M Competence Center for Media Security.

In 2007, following the dissolution of Fraunhofer IPSI, he moved to Fraunhofer SIT, where he first headed a group on media security and then became head of the Media Security and Forensics department in January 2010. Since November 2016, he has been an honorary professor at TU Darmstadt. Since 2019, Martin Steinebach has also been Principal Investigator at the National Research Center for Applied Cyber Security ATHENE, where he leads the research areas “Reliable and Verifiable Information through Secure Media (REVISE)” and “Security and Privacy in Artificial Intelligence (SenPAI)”. With his work on the ForBild project, Martin Steinebach and his colleagues won second place in the 2012 IT Security Award of the Horst Görtz Foundation. He leads numerous projects on IT forensics and media security for industry and the public sector. He is the author of more than 250 technical publications.

© Martin Steinebach



Prof. Michał Choraś

Bydgoszcz University of Science and Technology, Poland

AI solutions are widely used in a plethora of applications, including in the network security domain. However, in order to be fully adopted and accepted by societies, those solutions need to fulfill not only the requirements of effectiveness (e.g., of cyberattacks detection), but also those of trustworthy AI.

In this talk, practical examples of trustworthy AI solutions in network security will be presented and discussed, in particular cybersecurity and fake news detection. The results of selected EU and national projects will be also shown (e.g., AI4Cyber, STARLIGHT, APPRAISE, and SWAROG).

Michał Choraś currently holds a full professorship position with the Bydgoszcz University of Science and Technology, Poland, where he is the Head of the Teleinformatics Systems Division and the PATRAS Research Group. He was granted full professor title in December 2021. He is also affiliated with FernUniversität in Hagen, Germany, where he was a Project Coordinator for successful H2020 SIMARGL project (secure intelligent methods for advanced recognition of malware and stegomaware). He is also project coordinator/manager and security consultant. He is the author of over 300 reviewed scientific publications. In 2021 and 2022, he was included in the Stanford List of Top 2% Scientists. His research interests include AI, machine learning, data science, and pattern recognition in several domains such as cyber security, fake news detection, anomaly detection, data correlation, biometrics, and critical infrastructures protection. He has been involved in more than twenty EU projects (e.g., APPRAISE, AI4CYBER, SPARTA, STARLIGHT, SocialTruth, CIPRNet, Q-Rapids, and InfraStress).

<http://michal-choras.com>.

SA 2

29th Aug.

13:30–15:00

Trustworthy and Explainable AI (xAI) in Emerging Network Security Applications

© Michał Choraś



Fabio Di Franco

ENISA, EU

SA 1

29th Aug.

09:00–10:30

The European Cybersecurity Skills Framework (ECSF) is a tool for a common understanding of the cybersecurity professional role profiles in Europe and common mapping with the appropriate skills and competences required. It is an integral part of the Cybersecurity Skills Academy, which was recently announced by the European Commission, in order to define and assess skills, monitor the evolution of skill gaps and provide indications of emerging needs.

European Cybersecurity Skills Framework

Dr. Fabio Di Franco is leading the activities in ENISA on cyber skills development for highly skilled people. He is the chair of the working group who developed and maintain the European Cybersecurity Skills Framework (ECSF). He is also responsible for developing and delivering trainings to EU member states and EU institutions on information security management and IT security.

© Fabio Di Franco



Kendra Walther

University of Southern California, USA

SA 1

29th Aug.

11:00–12:30

In modern society, surrounded by technology and applications of data analytics, all students need to be digitally fluent. Furthermore, as the pace of technological adoption into foundational aspects of our lives increases, digital fluency and cybersecurity are increasingly co-dependent. Cybersecurity education for all means that learners need to develop cybersecurity awareness to protect themselves, their academic institutions, their employers, and in turn society at large. Additionally, because learners will need to continuously adapt to new threats or risks, both digital fluency and cybersecurity education require developing an attitude and disposition for lifelong learning and problem solving. As educators, we must collaborate to demand and lead the adoption of these initiatives.

Cybersecurity Education for All

Kendra Walther serves as Associate Director for Faculty Affairs and an Associate Professor in the Information Technology Program. Kendra has her bachelor's degree in Computer Science from Harvey Mudd College, and a master's degree in Computer Science from University of Maryland, College Park. She is currently pursuing an EdD in Educational Leadership from Rossier School of Education at USC and creating a curriculum for an undergraduate general education course for digital fluency. Kendra believes in lifelong learning, and really enjoys learning about how people learn best. She loves to bring new ideas and teaching methodologies into her classroom as she inspires her students to understand the principles of programming.

© Kendra Walther



SA 7

30th Aug.

11:00–12:30

Alessandro Brighente

Department of Mathematics, University of Padova, Padua, Italy

Channel hopping denotes the process of adaptively selecting a new communication channel in a given set when the currently used one undergoes significant quality degradation. This strategy might help wireless networks to mitigate both friendly and malicious interference and hence guarantee effective communications. To make the hopping pattern as effective as possible, researchers developed many different strategies including reinforcement learning-based ones. In this talk, we will explore new attacking strategies, their implementation on a real-world testbed, and possible mitigation solutions.

Jumping Jams: Effective Jamming in Channel Hop- ping-Based IoT Networks

Dr. Alessandro Brighente is an Assistant Professor at the University of Padova, Italy. He obtained his Ph.D. in Information Engineering from the University of Padova in 2021. He was visiting researcher at Nokia Bell Labs, Stuttgart, University of Washington, Seattle, and TU Delft, The Netherlands in 2019, 2022, and 2023 respectively. He served as TPC for several international conferences, including ESORICS, and WWW. He is the program chair for DevSecOpsRO, in conjunction with EuroS&P 2023. He has been a guest editor for IEEE Transactions in Industrial Informatics and for Elsevier's Computers and Security. He is part of several industrial and research projects, including EU-funded ones. His current research interests include security and privacy in cyber-physical systems, wireless communications, the Internet of Things, and Blockchain.

© Alessandro Brighente



Dimitris Tsolkas

National and Kapodistrian University of Athens (NKUA), Greece

Fogus Innovations & Services P.C, SME, Greece

During the last decades, the use of Application Programming Interfaces (APIs) has served as a bridge between mobile operators and start-ups in emerging markets. Operators have begun to consider whether to open their APIs, starting from APIs related to mobile messaging, operator billing etc. In addition, the recently witnessed convergence of IT and Telecom worlds has contributed a lot to putting APIs in the epicenter of network programming and service provisioning. A representative example that proves this statement is the 5G Service Based Architecture (SBA), which has been designed based on the flexibility that HTTP/2 Restful APIs to provide interaction among 3GPP network functions. In this context, and in order to avoid duplication and inconsistency among the various API specifications that 3GPP has released, the specification of a common API framework (CAPIF) has been considered.

In the framework of EVOLVED-5G project (<https://evolved-5g.eu/>), Fogus Innovation & Services P.C. and Telefonica Spain have developed and provide as an open-source product the Core Function of the CAPIF (namely the CCF), together with ready to use templates for compliant API service provide/consume entities. In the invited presentation, we will delve into the concept of network core openness through the exposure of CAPIF compliant APIs, and we will discuss the innovation potential that emerges by enabling a secure and interoperable interaction of third-party applications with network functions.

SA 2

30th Aug.

17:15–18:45

The 3GPP Common API framework (CAPIF) – open-source implementation and innovation potential

Dr. Dimitris Tsolkas holds a Ph.D. degree from the Department of Informatics and Telecommunications, National and Kapodistrian University of Athens (NKUA). He is currently a Senior Research Fellow at NKUA and he also leads research and development activities in Fogus Innovations & Services P.C, SME, Greece.

© Dimitris Tsolkas



He has long experience in Research & Development (R&D) as well as in project management, through his participation in a plethora of EC-funded projects. He has made vast contributions to the 5GPPP Technology Board (TB) and the 5GPPP/5GIA Working Groups (WGs) as well.

His research record counts more than 60 articles in high quality journals, books, and conferences; while his current research interests target wireless networks and systems, with emphasis on architectural and resource management aspects in mobile communication networks.

Kacper Gradoń

Warsaw University of Technology, Poland

University College London, United Kingdom

The presentation addresses the potential for the criminal abuse and hybrid-warfare weaponization of Generative Artificial Intelligence technologies. The focus is placed on the opportunities for the possible utilization of such tools by malign actors who engage in the orchestration and running of sophisticated scams (utilizing Open Source Intelligence, social engineering and text/voice/video impersonation), targeted phishing campaigns or who design, produce and propagate disinformation. The (cyber) security implications of technology are presented from the perspective of the Future Crimes and Crime Science disciplines. The presentation raises the questions about the ethical, moral and legal implications of similar technologies and opens the discussion on the responsibility of technology developers for the abuse of their products and on the topic of the IT industry governance.

Dr. hab. Kacper Gradoń, Ph.D., D.Sc. is an Associate Professor in Cybersecurity (Warsaw University of Technology), Honorary Senior Research Fellow and Department of Security and Crime Science (University College London) and Visiting Fulbright Professor at University of Colorado Boulder. He is also the World Health Organization Global Infodemic Manager. He is a double TED Speaker, expert in information warfare and human-centric dimensions of cybersecurity and frequent consultant of law enforcement agencies and intelligence institutions worldwide. He has spoken at over 200 conferences on all continents. Previously he was an Associate Professor and Director of the Centre for Forensic Sciences (University of Warsaw). He was also a civilian expert of the General Headquarters of the Polish National Police (where he was responsible for the creation of the criminal intelligence and analysis framework). He has published extensively on the issues of cyber-crime, future crimes, Artificial Intelligence, hybrid warfare and criminal investigation.

SA 4

30th Aug.

11:00–12:30

What's wrong with Wolfie? Generative Artificial Intelligence and its implications for (Cyber) Security

© Kacper Gradoń



Dr. Sabine Delaitre

The Wick, innovation unit of BOSONIT, Spain

DocExploit team creates innovative and high-quality cybersecurity solutions to give a response to the increasing security needs of the digital transformation process and Industry 4.0. With DocSpot, DocDocker, and SirDocker tools, DocExploit team offers a complete suite that ensure the security of your enterprise applications and container environments. DocSpot detects vulnerabilities in application source code, Docdocker scans for vulnerabilities in containers and SirDocker manages and monitors containers efficiently and securely. Thus, to help to prevent cybersecurity attacks, DocExploit wants to improve the quality and security of software, with high accuracy by drastically reducing false positives, from the very base of its source code by developing a code analyzer based on graph technology, which allows for optimizing the detection of software vulnerabilities in the source code. In this talk, we will describe our technical approach, the different tools of the suite we are developing, and the possible contributions to the industry by fostering security automation and improving security in software and IoT applications.

Dr. Sabine Delaitre is a Computer Scientist with a Doctorate in the areas of Risk Management, Artificial Intelligence and Knowledge Management from the Ecole des Mines de Paris. She has 20+ years expertise on R&D projects. As Senior Innovation Expert, she currently aims at developing R&D projects focusing on Big Data, Advanced Analytics, AI/ML/FL, Semantics, Cybersecurity, lowCode, End-to-end IoT solutions in Industry 4.0, Energy and Smart Cities.

SA 1

30th Aug.

11:00–12:30

DocExploit's Cybersecurity Suite or how to be aware of the security level of your code to build and maintain a more secure one?

© Sabine Delaitre



Aditya Raj

Technology Consultant – Distributed Ledger Technology/Blockchain, Fujitsu, Belgium

In the era of Industry 4.0, where the integration of digital and physical systems is becoming increasingly prevalent, the challenge of establishing trust in decentralized systems is paramount. This keynote will delve into the role of blockchain technology in fostering decentralized trust, thereby enhancing cybersecurity in the context of Industry 4.0. We will explore real-world examples of how blockchain technology, including Hyperledger and Enterprise Ethereum, is being used to secure data, streamline processes, and ensure reliable transactions. The discussion will also look ahead to the future of blockchain and cybersecurity in Industry 4.0, highlighting the potential for further innovation and transformation.

Aditya Raj is a Senior Blockchain Consultant at Fujitsu Track and Trust Solution Center, where he leverages his deep understanding of blockchain and distributed ledger technology to guide customers through their digital transformation journeys. With over 12 years of industry experience, Aditya is a trusted advisor to both customers and colleagues, helping them navigate the complexities of blockchain technology and its potential applications. As a blockchain evangelist, he is passionate about exploring how this revolutionary technology can enhance trust, security, and efficiency in the era of Industry 4.0. Aditya's expertise and forward-thinking approach make him a sought-after speaker and consultant in the field of blockchain technology.

SA 1

30th Aug.

13:30–15:00

Decentralized Trust for Industry 4.0

© Aditya Raj



Jan Willemson

Senior Researcher, Cybernetica, Estonia

The methods of running democratic elections have evolved over the centuries together with the requirements. One of the paradoxes of voting is that these requirements are inherently contradictory. On one hand, we want to have full transparency and verifiability of the whole process by everyone, but on the other hand we want to keep the act of voting private to resist coercion attacks. It turns out that these properties can not be both achieved 100%, so some kind of a trade-off is required. In this talk we take a look at some of the possible equilibrium points and discuss their implications for practical voting systems.

Jan Willemson defended his PhD in computer science at Tartu University, Estonia, in 2002. He has been working at Cybernetica as a researcher since 1998, specializing in information security and cryptography. His areas of interest include risk analysis of heterogeneous systems, secure multi-party computations, e-government solutions and security aspects of Internet voting. He has authored more than 70 research papers published in international journals and conferences.

SA 3
29th Aug.
13:30–15:00

Privacy and verifiability trade-offs in voting systems

© Jan Willemson



Martin Schneider

Head of the Testing in the business unit Quality Engineering (SQC) at the Fraunhofer Institute for Open Communication Systems (Fraunhofer FOKUS), Germany

The Cyber-Resilience Act obliges the manufacturers of software to perform a comprehensive security evaluation. Security testing and monitoring plays a crucial role to meet the requirements arising from the CRA. In the light of these upcoming requirements, also the demands on security testing and monitoring will change, with respect to efficiency, reliability, and independence. In my talk, I will interpret the CRA in the context of security testing and monitoring and will present a solution that partially addresses them.

SA 7

29th Aug.

09:00–10:30

Challenges and Opportunities for Security Testing and Monitoring in the Light of the Cyber-Resilience Act

Martin Schneider is Head of the Testing in the business unit Quality Engineering (SQC) at the Fraunhofer Institute for Open Communication Systems (Fraunhofer FOKUS). His research focuses on security testing of both software systems and machine learning systems. He leads various research projects in these areas at Fraunhofer FOKUS and is active in standardization bodies such as DIN and ETSI. He is author of a primer for the application of fuzzing in the context of common criteria certification published by the German Federal Office for Information Security (BSI), trainer at the Fraunhofer Academy for Security Testing, and co-author of a book in this field.

© Martin Schneider



Ibrahim Baggili

Louisiana State University, Baton Rouge, LA, USA

SA 7

30th Aug.

15:30–17:00

Machine Learning (ML) and Artificial Intelligence (AI) have become inescapable forces, permeating every facet of our society, from business and academia to public and private sectors. However, AI failures are an undeniable reality that demands urgent attention from forensic researchers and practitioners. When AI embarks on mischievous endeavors, an important question arises: Who you gonna call? While AI/ML/<Insert Buzzword> are hailed as powerful tools to enhance digital forensics processing, it is imperative that we redirect our focus towards the forensics of AI. Join me in this keynote as we explore the emerging field of AI forensics, an essential sub-discipline within the realm of digital forensics. Through an overview of this evolving field and a spotlight on intriguing research problems, we will ignite understanding of the pressing need to address AI investigations.

Who You Gonna Call? Unmasking AI Investigations through AI Forensics

Dr. Ibrahim (Abe) Baggili is a first generation Arab American. He is a Professor of Computer Science and Cybersecurity at Louisiana State University and the founder of the BiT Lab (Baggili Truth Lab) where he holds a joint appointment between the Division of Computer Science & Engineering and the Center for Computation and Technology. He has won numerous awards including the CT Civil Medal of Merit, the Medal of Thor from the Military Cyber Professional Association, CT 40 under 40, and is a fellow of the European Alliance for Innovation. Prior to that he was the director of the Connecticut Institute of Technology and Elder Family Endowed Chair of Computer Science & Cybersecurity at the Tagliatela College of Engineering at the University of New Haven. He received his BSc, MSc and PhD all from Purdue University where he worked as a researcher in CERIAS. Work with his students has uncovered vulnerabilities that impact over a billion people worldwide and has been featured in news and TV outlets in over 20 languages and he has published extensively in the domain of digital forensics. To learn more about the BiT Lab, you can visit <https://csc.lsu.edu/~baggili>.

© Ibrahim Baggili



Social Events

Welcome Reception

19:00

29th Aug.

TUE

The official ARES 2023 and CD-MAKE 2023 Welcome Reception takes place at the Palazzo San Domenico. Just a short walk away from the main venue, the Palazzo San Domenico is surrounded by an inviting beautiful garden, filled with Italian Transavantgarde art. The captivating charm of Benevento will welcome you at this first conference evening.

📍 Meeting point:
*in front of Auditorium,
18.45*

SCAN ME

Address: Piazza Guerrazzi, 1, 82100 Benevento

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



© SBA Research

Conference Dinner

19:00

31st Aug.

THU

Exclusive chartered busses will take you for a short ride and right to our Conference Dinner which will take place at **'Masseria Roseto'**.

Meeting point:
*in front of Auditorium,
18.45*

'Masseria Roseto' has been preserving and enhancing the ancient structure of a former monastery. The astonishing surrounding area with a beautiful garden is waiting to be discovered. A traditional Italian dinner party is prepared for the conference attendees.



© Masseria Roseto

SCAN ME

Address: 82100 Contrada Roseto

Scan the QR Code and
find the directions to the bus terminal.



Conference Venue



© Shutterstock

ARES 2023 will be held at the University of Sannio, Benevento, Italy. Lecture halls are located at Complesso Sant'Agostino.

© University of Sannio

Address of ARES 2023 Conference

University of Sannio - Complesso Sant'Agostino
Via Giovanni De Nicastro, 13
82100 Benevento, Italy



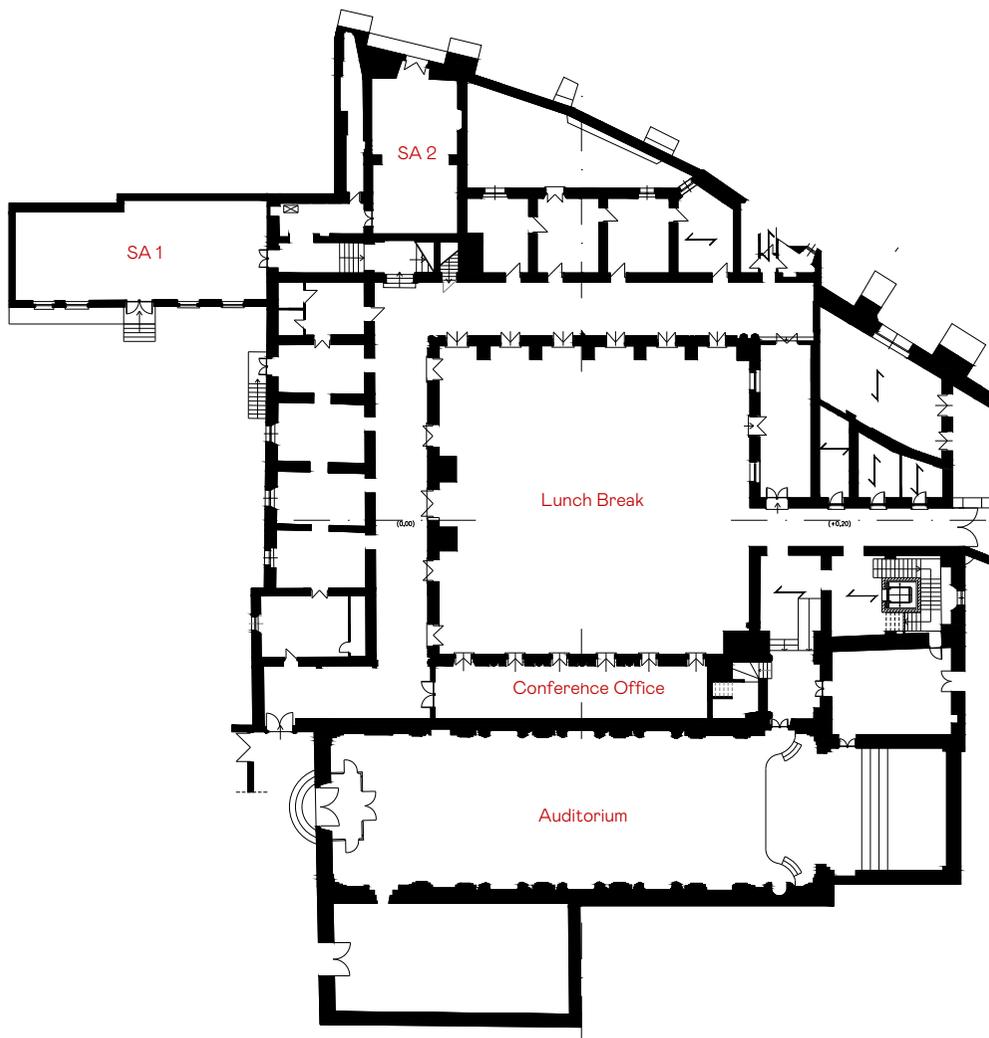
SCAN ME

Your way from the train station to the conference venue.

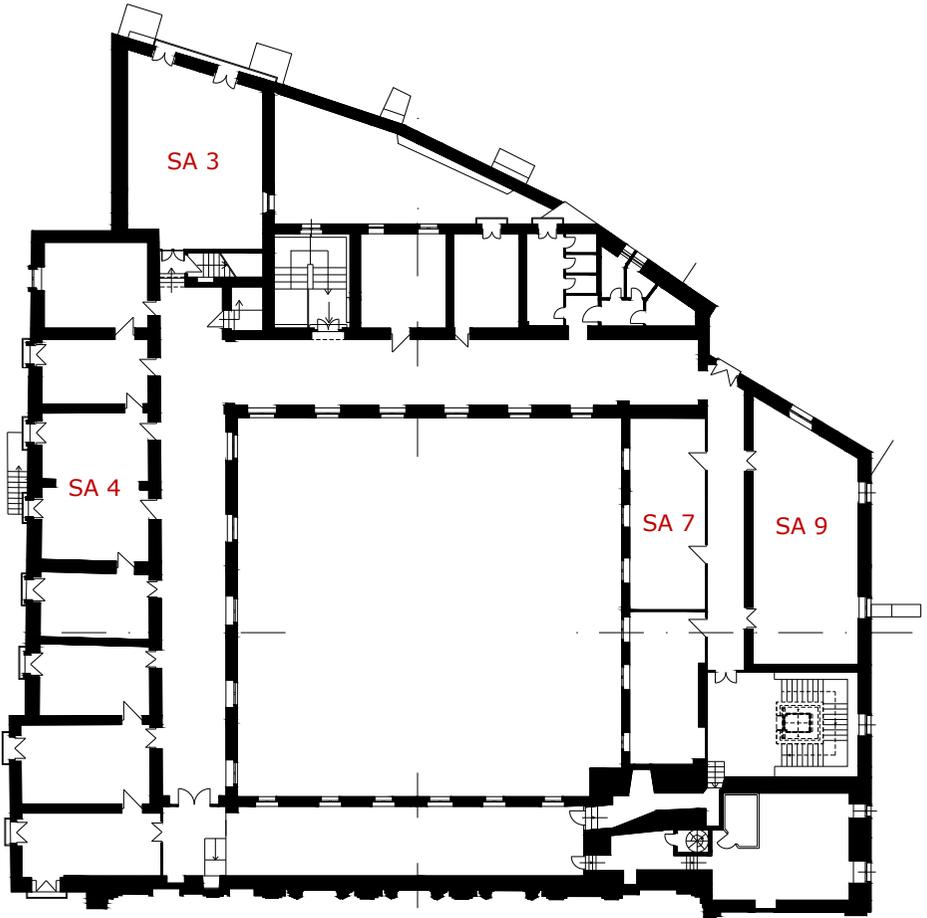


© Shutterstock

Ground Floor



First Floor



About Benevento

Welcome to Benevento, Italy

Welcome to the captivating city of Benevento, nestled in the heart of the sun-kissed Campania region. Prepare to be mesmerized by its timeless charm, rich history, and breathtaking landscapes. Come and immerse yourself in an unforgettable Italian experience like no other!

Uncover Ancient Wonders

Benevento is a city steeped in history, boasting an array of ancient wonders that will transport you back in time. Marvel at the Arch of Trajan, a magnificent Roman triumphal arch standing tall for almost two millennia. Wander through the ancient Roman Theatre, where echoes of long-lost performances still resonate in its awe-inspiring architecture.

Discover Timeless Churches

As you stroll through the picturesque streets, you'll encounter a wealth of stunning churches that showcase Italy's architectural brilliance. Don't miss the Cathedral of Santa Maria Assunta, with its splendid mix of Romanesque, Gothic, and Baroque styles. The Church of Santa Sofia, a UNESCO World Heritage site, will leave you in awe with its delicate beauty and rich history.

© Shutterstock



Explore the Enchanting Beauty of Benevento

Indulge in Gastronomic Delights

Prepare your taste buds for a culinary adventure! Benevento's gastronomy is a delightful fusion of traditional Italian flavors, boasting delectable local dishes and fine wines. Savor the renowned "Tortelli di Zucca," a mouthwatering pumpkin-filled pasta, and delight in the simplicity of "Pagnotta del Dittaino," a rustic bread that pairs perfectly with local cheeses and cured meats.



© Shutterstock



© Shutterstock

Experience the World of Wine

For wine enthusiasts, Benevento is a true paradise. The region is renowned for producing some of Italy's finest wines. Embark on a wine-tasting journey in lush vineyards, savouring the velvety Aglianico reds or the crisp and refreshing Falanghina whites. Let the flavors dance on your palate, and raise a toast to the exquisite Italian craftsmanship.

Nature's Embrace

Surrounded by rolling hills and fertile valleys, Benevento's natural beauty is boundless. Take a scenic drive along the countryside, admiring the vineyards and olive groves that paint the landscape with vivid colors. For the adventurous souls, explore the nearby Taburno Camposauro Regional Park, a haven of lush forests, hidden grottoes, and stunning panoramas.

Festivals and Traditions

The vibrant spirit of Benevento comes alive during its lively festivals and traditions. Experience the annual "Strega Festival," where the city celebrates its legendary witchcraft history with parades, performances, and captivating rituals. Let yourself be enchanted by the local folklore and immerse yourself in the warm embrace of Italian culture.



Gregorio's Tips for Benevento

Restaurants

Roseto All' Arco, Via Traiano, 65, 82100 Benevento BN

Almost adjacent to the conference venue, with outdoor seating overlooking Trajan's arch, offering both a sophisticated menu with top-quality ingredients and an excellent wood-fired pizza.

Ristorante Pizzeria Traiano since 1985, Via Giuseppe Mancioti, 48

Exactly opposite Roseto all'arco, it is the classic southern Italian trattoria; it offers hearty traditional dishes with a view of Arco Traiano.

Teresa Paparella Restaurant, Vico I S. Vittorino, 18

In the heart of the old town, less than 300 metres from the conference venue, is a small restaurant with an intimate atmosphere and freshly prepared dishes.

Gino e Pina, Viale dell'Università, 23

About a 10-minutes walk from the arch is probably the most famous restaurant in the centre of Benevento; it offers traditional Benevento dishes with a very extensive menu with choices of both meat and fish.

Restaurant Osteria Con Gusto, Via Tiengo, 34

Very close to the Trajan Arch, it is a restaurant famous for its wide range of fish dishes.

Pizzerias

Pizzeria 'La Pampanini' di Andrea Lepore, Via S. Pasquale, 8

A few steps from the Trajan Arch, it offers excellent pizza with a very wide choice.

Toledo Pizzeria Napoletana, Via Francesco de Sanctis, 2

About 800 metres from Arco Traiano, this is the only pizzeria in Benevento that offers the classic Neapolitan pizza (very very thin dough, very low crust and very very generous diameter).



© pixabay/jorono

Pubs

Good Fellows, Adjacent Roman Theatre, Via Port'Arsa, 32

In summer you can literally sit a few metres from the arches of the Roman theatre and enjoy one of the best hamburger sandwiches in Benevento.

Sherlock Public House, Viale dei Rettori, 26

Classic English-style pub in the city centre, a few steps from the Trajan Arch.

Beneventum Public House, Viale Dei Rettori 34

In the centre of Benevento is a completely Harry Potter-themed pub; nevertheless it is a great place to have a sandwich even if you are not a fan of the series.

La Ciunnazzeria, Via S. Pasquale, 2

Just a few metres from the Trajan Arch is a more refined pub where you can try not only the classic sandwich, but also a 'tagliere' and a good glass of red wine.



Bar/Bistro/Aperitif/Cocktails

Alimenta Bistrot, Via Traiano, 49/51, 53

With a view of the Trajan Arch also excellent for an aperitif or a bite to eat.

Caffè delle Streghe, aka 'Palazzo Paolo V', Corso Garibaldi, 141

Bar in a historic Benevento building.

Quintessenza Bakery Café, Corso Garibaldi, 5

View of the church of santa sofia, a unesco heritage site.

Café Le Trou, Corso Garibaldi, 30

Famous for its hazelnut coffee.

Caffè del Corso, Corso Garibaldi, 200

With a view of the cathedral.

Dada restaurant & bar, Viale Atlantici, 31

An elegant venue 15 min walk from the Trajan Arch if you want to visit the upper, bourgeois part of town or the nearby villa comunale.

Odeon Mixology & Wine - Cocktail Bar, Via Bartolomeo Camerario, N 52/54

One of the best places to have a good cocktail in the old town.

Al Duca, Via Giuseppe Verdi, 41

This is the area where young people from Benevento usually go to drink after 11pm at the weekend.

SCAN ME

More on Food & Drink Tours in Province of Benevento? Scan this QR code.



Useful Information

WIFI at ARES

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

Emergency Numbers

112	European emergency number
-----	---------------------------

118	Ambulance
-----	-----------

115	Fire Brigade
-----	--------------

113	Police
-----	--------

i Info:

The emergency numbers are free of charge.

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.

Important Phrases

Hello!	Ciao!	Chow !
Goodbye!	Arrivederci!	Ahr-ree-veh-dehr-cheel!
How are you?	Come sta?	Koh-meh stah?
Do you speak English?	Parla Inglese?	Parh-la een-glai-zeh?
You're welcome.	Prego.	Preh-goh.
Please.	Per favore.	Pehr fah-voh-reh.
Yes.	Si.	See.
No.	No.	Noh.
I don't know	Non lo so.	Nonh loh saw.
I (don't) understand.	(Non) capisco.	(Non) kah-pee-skoh.
Okay.	Va bene.	Vah beh-neh.
Help!	Aiuto!	Ay-oo-toh!!
Thank you.	Grazie.	Grah-tsee-eh.
Excuse me. (for attention)	Scusi.	Skooh-zee.
Excuse me. (to pass by)	Permesso.	Pehr-mehs-soh.
Good morning.	Buon giorno.	Bwohn-johr-noh.
Good evening.	Buona sera.	Bwoh-nah-seh-rah.
Good night.	Buona notte.	Bwoh-nah-noh-teh.
Cheers!	Salute!	Sah-loo-tay

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 Sannio of Benevento

The university of Benevento born as a branch of the University of Salerno and acquired full administrative and didactic autonomy starting from 1 January 1998 as the University of Sannio of Benevento. It is made up of three Departments: Department of Law, Economics, Management and Quantitative Methods, Department of Engineering and Department of Sciences and Technologies. Within the framework of national university training, the Sannite University is distinguished by a complex cultural project, characterized, on the one hand, by highly specialized training courses, such as to qualify it as a center of national importance for certain disciplinary fields; on the other hand, from the promotional role that the University proposes in the process of development of the economic and social system of Campania, and in particular of its internal areas.

Sponsors ARES 2023

Thank you to our sponsors Scuola La Tecnica, Tyche Digital Technology and PYNLab for supporting ARES 2023. As sponsors, your contribution is vital to the conferences success and ARES mission of bringing together researchers and practitioners in the field of IT security and privacy from around the globe.

Organizers & Supporters

ARES 2023 is organized by



Supported by



UNIVERSITÀ DEGLI STUDI
DEL SANNIO Benevento

ARES 2023 is sponsored by



ARES 2023

Conference Office Contact

Bettina Jaber

Mobile: +43 664 254 03 14

Daniela Freitag David

Mobile: +43 664 88 00 11 51

E-Mail: ares@sba-research.org

