



NetsLab 

CONNECT
Centre for Future Networks

1ST SECURENET 2023 WORKSHOP

11 September 2023

08:30 AM - 05:00 PM CEST

UCD University Club

UNIVERSITY COLLEGE DUBLIN
DUBLIN, IRELAND



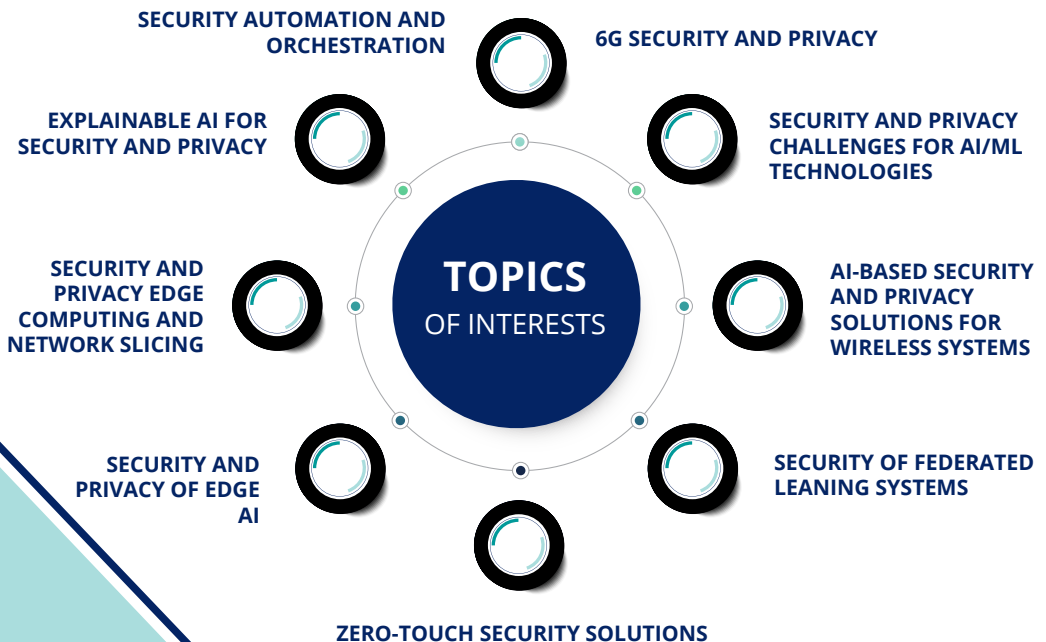
Funded by
the European Union

WHAT IS IT ABOUT?

The SECURENET 2023 workshop is an academic event jointly organized by Network Softwarization and Security Labs (NETSLAB) research group at the UCD School of Computer Science and SFI CONNECT Centre.

FOCUS ON

- The security and privacy of future mobile networks, including 5G and 6G.
- It discusses these concerns and highlights cutting-edge solutions to ensure that the networks are secure and resilient against potential security threats.



ORGANISERS



MORE INFORMATION
WWW.netslab.ucd.ie



MORE INFORMATION
WWW.ucd.ie

Network Softwarization and Security Labs (NETSLAB) is a research group at the UCD School of Computer Science that mainly focuses on the security and privacy of future mobile networks, including 5G and 6G. Dr. Madhusanka Llyanage leads the lab. With the increasing reliance on mobile networks in various sectors, the security and privacy of these networks has become a significant concern. NETSLAB aims to address these concerns and provide cutting-edge solutions to ensure the networks are secure and resilient against potential security threats.

NETSLAB researches various aspects of network softwarization and security, such as network slicing, software-defined networking and edge computing. The team is particularly interested in using blockchain and artificial intelligence (AI) to enhance the security of future mobile networks. By exploring and developing these technologies, NETSIAB is positioning itself as a leading research group in network security.

NETSLAB actively participates in national, EU, and international research projects and has established collaborative partnerships with industry leaders. This collaboration allows the team to stay up-to-date on the latest trends and innovations in the industry and translate their research into practical applications. Through these partnerships, NETSLAB has successfully delivered research outcomes adopted by industry leaders, ensuring the security and stability of future mobile networks.



MORE INFORMATION
WWW.connectcentre.ie

Its mission is to research and develop innovative solutions for the communications challenges facing society today. The Internet of Things, 5G/6G networks and future communications services are the Centre's main areas of focus. Over 300 CONNECT researchers across 10 Higher Education Institutes are supported by €90 million of funding from the Science Foundation Ireland Research Centres Programme, the European Regional Development Fund and industry partners. CONNECT focuses on six research themes looking to the next generation of networks: Dependable Networks:Sustainable IoT: Link Performance: Customised Networks: Data-driven Optimisation and Management: and The New Operators: CONNECT researchers have vast expertise in test and experimentation in these areas.



MORE INFORMATION
WWW.spatial-h2020.eu

SPEAKERS



Aengus GOREY

Establishing Trust in the Data we use to drive automation & autonomous decision-making

ABSTRACT

In an environment where sensor data describing the real-world is increasingly being used to drive decisions which affect how we live. Establishing trust in data's origins are key to enabling trust in decisions made by autonomous systems. As intelligence moves to the edge & raw data made more intelligent earlier in its life-cycle, establishing a chain of trust, anchored at the point of origin gives assurance that as data migrates from its point of creation it can be traced back to its point of origin. With modern network systems protecting the communication medium, compromised data flows introduced to a system would be given a "free ride" through the system to a point of decision making. Not only does trusted data protect us from data poisoning, tampering or spoofing, it offers more useful outcomes when it comes to trust models for data reporting, such as ESG reports & other compliance metrics.

JOB TITLE

Security Systems Engineer

AFFILIATION

ANALOG DEVICES

BIO

Aengus Gorey has been working with Analog Devices since May 2021, focusing on the development of security capabilities & applications for the embedded market. Aengus previously worked as a Cyber Security Architect with Jaguar Land Rover, helping to implement Telematic ECUs using a grounds-up secure design life-cycle. Before that, Aengus took time out of Industry to complete a Masters Of Engineering in Information & Network Security at the University of Limerick. Aengus worked with Intel, primarily focusing on their embedded products division with a focus on embedded graphics, security & networking in their industrial & automotive product groups.



Bartlomiej SINIARSKI

JOB TITLE

PostDoctoral Researcher / Project Manager

AFFILIATION

UNIVERSITY COLLEGE DUBLIN

BIO

Bartlomiej Siniarski currently holds the position of a post-doctoral researcher and serves as a project manager for the EU H2020 SPATIAL project at University College Dublin. His academic journey commenced with undergraduate studies in Computer Science at both University College Dublin (Ireland) and the University of New South Wales (Australia). In 2018, he successfully earned his doctoral degree. His expertise lies in the field of IoT networks, with a particular focus on the design, data collection, storage, and analysis derived from intelligent sensors. Moreover, Bartlomiej has actively contributed to various projects, including MSCA-ITN-ETN, ICT-52-2020, and H2020-SU-DS-2020, which are dedicated to addressing challenges in network security, performance, and management within 5G and B5G networks.



Dan KILPER

JOB TITLE

Director of the CONNECT Centre, and Principal Investigator

AFFILIATION

TRINITY COLLEGE DUBLIN

BIO

Professor Dan Kilper is the Director of the CONNECT Centre, and Principal Investigator. He is a Professor of Future Communication Networks in the School of Engineering at Trinity College Dublin.

Professor Kilper received his PhD in physics from the University of Michigan in 1996. From 2000 to 2013, he was a member of the technical staff at Bell Labs. He is a senior member of IEEE, a topical area editor for the IEEE Transactions on Green Communications and Networking (TGCN) and chairs the optics working group in the IEEE International Network Generations Roadmap. He was recognized as a 2019 NIST Communications Technology Lab Innovator and holds eleven issued patents, and authored six book chapters and more than one hundred sixty-seven peer-reviewed publications. His research aims to solve fundamental and real-world problems in communication networks to create a faster, more affordable, and energy efficient Internet, addressing interdisciplinary challenges for smart cities, sustainability, and digital equity.



Edgardo MONTES DE OCA

Explainability for AI-based cybersecurity solutions

ABSTRACT

While AI demonstrates remarkable performance in detecting and mitigating cyber-attacks, the lack of interpretability and explainability inherent in many AI models poses significant challenges. This presentation will highlight the growing importance of explainability and emphasize the need to strike a balance between trust and efficacy in safeguarding digital assets. Various techniques and approaches will be discussed that aim to enhance the interpretability and transparency of AI-based cybersecurity solutions. These methods encompass model-agnostic techniques, such as LIME and SHAP, which provide post hoc explanations for AI predictions, as well as inherently interpretable models like decision trees and rule-based systems. Furthermore, the abstract delves into the advancements in neural network architectures, such as attention mechanisms and gradient-based attribution methods, which facilitate the introspection of complex deep learning models.

JOB TITLE

CEO Montimage

AFFILIATION

MONTIMAGE

BIO

Edgardo Montes de Oca graduated as an engineer in 1985 from Paris XI University, Orsay, both in electronics and computer science. He has worked as a research engineer at the Alcatel Corporate Research Centre in Marcoussis, France and at Ericsson's Research Centre in Massy, France. In 2004 he founded Montimage and is currently its CEO. His main interest is in building critical systems that require state-of-the-art fault-tolerance, testing and security techniques; developing software solutions with strong performance and security requirements; designing and building tools for monitoring the security and performance of networks; and building portable and secure 5G solutions.



Houda LABIOD

A Multi-layer trust framework for future communication systems

ABSTRACT

Future digital world will bring more complex behaviors and trust relationships between digital entities and stakeholders, it is thus necessary to re-build digital relationships between entities and set up new trust systems establishing universal digital trust. The heterogeneity, openness, pervasiveness and complexity of the future generation communication networks and human centric applications introduce additional cyber security threats and vulnerabilities that make security, safety, privacy and resilience even more challenging. Novel approaches for security, data protection, resiliency and trust assurance are required to secure and trust exchange of information between involved massive number of heterogeneous AI-based and non-AI computation and communication infrastructure elements. To meet this vision, we need to design new generation of trustworthy communication networks. How can we build a trustworthy Internet? How trustworthiness could be natively integrated in 6G? How could we make Cooperative ITS systems more trustworthy? This talk introduces the concepts and characteristics of trustworthy systems and identifies key challenges for realizing multi-layer trust frameworks while highlighting some recent standardization progress.

JOB TITLE

Team Leader

AFFILIATION

HUAWEI TECHNOLOGIES FRANCE, SHIELD LAB PARIS, PARIS RESEARCH CENTER

BIO

Houda Labiod (Senior Member, IEEE) is a Senior Expert and Team Leader in Shield Lab Paris at Huawei Paris Research Center. Before taking up this position, she received the H.D.R. (Habilitation à diriger les recherches) degree in 2005 in France and Full Professor with the Department INFRES (Computer Science and Network Department), Telecom Paris (previously named ENST), Paris, France for 20 years. She was the Head of the Research Group CCN "Cybersecurity for Communication and Networking" from 2015 to 2018. Before this, she held a research position with the Eurecom Institute, Sophia-Antipolis, France. Her current research interests include trust and security in a new generation of communication networks. She has published six books, eleven patents and more than 250 research papers. She is a Founder of IFIP NTMS Conference on New Technologies, Mobility and Security (NTMS2007). She was involved in major national and European projects focusing on security for connected and autonomous vehicles (SCOOP@F, InterCor and C-Roads). She was the Co-Leader of the Chaire C3S on Cybersecurity for connected and autonomous vehicles with French partners Renault, Valéo, Thales, Nokia and Wavestone.



Huber FLORES

JOB TITLE

Associate Professor

AFFILIATION

INSTITUTE OF COMPUTER SCIENCE, UNIVERSITY OF TARTU, ESTONIA

BIO

Huber Flores is an Associate Professor of Pervasive Computing at the Institute of Computer Science, University of Tartu, Estonia as well as a Docent at the University of Helsinki, Finland. He leads the Distributed and Pervasive Systems Group (<https://dps.cs.ut.ee>). Prior to that, he held the prestigious Academy of Finland Postdoctoral Fellowship and the competitive Faculty of Science Postdoctoral Fellowship of the University of Helsinki. He is also a former member of UBICOMP at the University of Oulu, Finland, and SyMLab at the Hong Kong University of Science and Technology, Hong Kong. He is also the recipient of the Jorma Ollila Award given by the Nokia Foundation. Besides this, Flores is also an active member of ACM (SIGMOBILE) and IEEE societies. His major research interests include distributed systems, pervasive and mobile computing, and AI. He has served as an organizer and a technical committee member of research venues, which includes MobiSys, IJCAI, ECAI, UMAP, IJCAI-PRECAI, WWW, PerCom, and IUI.



Madhusanka LIYANAGE

JOB TITLE

Assistant Professor / Ad Astra Fellow and Director of Graduate Research

AFFILIATION

SCHOOL OF COMPUTER SCIENCE, UNIVERSITY COLLEGE DUBLIN, IRELAND

BIO

Madhusanka Liyanage is an Assistant Professor/Ad Astra Fellow and Director of Graduate Research at University College Dublin, Ireland. He is also a Docent/Adjunct Professor at the University of Oulu, Finland, the University of Ruhuna, Sri Lanka, and the University of Sri Jarawardhenepura, Sri Lanka. He holds a Doctor of Technology degree from the University of Oulu, Finland (2016) and prestigious fellowships during 2018-2020. Madhusanka has been a Visiting Research Fellow at various renowned institutions globally. He received the "2020 IEEE ComSoc Outstanding Young Researcher" award and was ranked among the World's Top 2% of Scientists in 2021 and 2022. He has over 150+ publications, authored books, edited books, and two patents. Additionally, he serves as an expert consultant at European Union Agency for Cybersecurity (ENISA) and has secured over 5 Million Euro research funding. Currently, he leads three large EU H2020/Horizon Europe projects and is the director of the Netslab team at University College Dublin, Ireland. More info: www.madhusanka.com



Michael ZIMMER

Building Privacy and Ethics into Future Mobile Platforms

ABSTRACT

The enhanced speeds, connectivity, and optimization promised by future mobile will spark continued innovation in instant communications, mixed reality applications, ubiquitous internet of things devices, and ambient intelligence platforms. While security and privacy issues are a central focus for researchers developing such future mobile technologies, this talk highlights additional gaps in how we think about the privacy and ethical dimensions of this next phase of advanced wireless networking. Issues of ubiquitous monitoring and surveillance, fairness and equity, autonomy and control, and unintended consequences will be presented, and pathways for engaging in ethically-informed design will be shared for discussion.

JOB TITLE

Professor and Director of Center for Data, Ethics, and Society

AFFILIATION

DEPARTMENT OF COMPUTER SCIENCE, MARQUETTE UNIVERSITY, USA

BIO

Michael Zimmer, PhD, is a privacy and data ethics scholar whose work focuses on digital privacy & surveillance, the ethics of big data, internet research ethics, and the broader social & ethical dimensions of emerging digital technologies. Dr. Zimmer is Director of the Center for Data, Ethics, and Society at Marquette University, and is a Professor in the Department of Computer Science. He co-chairs the AoIR Ethics Working Group, serves on the SIGCHI Research Ethics Committee, and sits on numerous advisory and editorial boards. Dr. Zimmer currently is the ethics advisor for the European Commission-sponsored SPATIAL Project.



Neil HURLEY

JOB TITLE

Associate Professor, Head of School

AFFILIATION

SCHOOL OF COMPUTER SCIENCE UCD

BIO

Dr. Neil Hurley graduated with a M.Sc. in Mathematical Science from U.C.D. in 1988. In 1989, he joined Hitachi Dublin Laboratory, a computer science research laboratory based at Trinity College Dublin. He initially worked on knowledge-based environments for engineering design and was awarded a PhD in 1995. A patent for the system was granted in the US and Europe. His research focus switched to parallel and distributed computing, and he became the group leader of the parallel computing group in HDL in 1995. During this period, he worked on developing parallel simulation and optimisation software, such as parallel finite element analysis and dynamic load balancing. In 1998, he was appointed as manager of HDL. He became a lecturer in the UCD Computer Science department in 1999. He established the Information Hiding Laboratory in 2001, a research laboratory focused on technology for embedding information in digital content. He has won over €1 million euro in research funding from Enterprise Ireland, Science Foundation Ireland, the EU and industrial partners.



Nicolas KOURTELLIS

Harnessing the Power of Privacy: Advancing into the 6G era with AI

ABSTRACT

With the arrival of faster, more demanding (5G, 6G,...) networks and the envisioned applications they will support, traditional solutions for (telco) network management are reaching their limits, both with respect to performance and protection they can offer. Within Telefonica Research, we investigate how novel, beyond state-of-art methods based on privacy-preserving artificial intelligence, cloud, and edge computing, can enable more secure, private, and scalable systems and networks that will accommodate the needs of future networks and applications.

JOB TITLE

Co-Director Telefonica Research & Head of Systems AI Lab

AFFILIATION

TELEFÓNICA

BIO

Nicolas Kourtellis is Head of the Systems AI Lab (SAIL) and Co-Director of Telefonica Research, a 20+ researcher team based in Barcelona. He holds a PhD in Computer Science & Engineering from the University of South Florida, USA (2012) and has over 90 published peer-reviewed papers and 6 filed patents. Currently, he focuses on privacy-preserving AI and federated learning on the edge, modelling/detecting with AI user online privacy leaks, as well as inappropriate/fraudulent behaviour on social media. He executed several research visits in Argonne National Lab, INRIA, Yahoo, UCL, CUT, AUTH, FORTH, and others. He has served in many technical committees of top conferences and journals and presented his work in top academic and industrial venues, including Mobile World Congress 2021 and 2023. His work has been covered by major news outlets such as Nature, New York Times, The Atlantic, New Scientist, Washington Post, Wired, and others. In 2022, he was ranked among the World's Top 2% Scientists (2021) in the list prepared by Elsevier BV, Stanford University, USA.





Samuel MARCHAL

Security assessment of ML-based systems under realistic attacker capabilities

ABSTRACT

Securing ML-based systems often comes at the cost of compromising other desired capabilities such as performance, explainability or privacy. To select and deploy a sensible defense, which won't jeopardize these other capabilities, we must know the actual vulnerability of ML-based systems against adversarial attacks. We propose an empirical assessment method to quantify the vulnerability of ML-based systems against evasion attacks. This method is supported by vulnerability metrics, and it is implemented in a library enabling the empirical security assessment of ML-based systems. The library leverages state-of-the-art black-box evasion attacks and implements flexible constraints regarding the modifications that can be performed to the inputs of the ML model. These flexible constraints allow for an easy implementation of realistic attacker capabilities, enabling accurate vulnerability assessment in sensible attack settings.

JOB TITLE

Senior Data Scientist / Squad Lead (Machine Learning Security)

AFFILIATION

WITHSECURE CORP

BIO

Samuel Marchal is a Senior Data Scientist withing the CTO office at WithSecure Corp. where he leads the research on trustworthy AI, focusing mainly on security, reliability and bias aspects of ML systems. He is also a Research Fellow at Aalto University. He received his PhD in Computer Science from the University of Luxembourg and the University of Lorraine (France). Samuel's research focuses on the application of ML to improve system and network security, the security of ML-based systems and on AI-enabled cyberattacks.

He has published over 35 papers in top conferences and journals specialized in systems and security. Samuel has been part of two Intel Collaborative Research Institutes (ICRI-SC and ICRI-CARS <https://www.icri-cars.org/>) in which he led the "Security and Machine Learning" research pilar. He has been involved in several large research projects funded by the European Commission, Business Finland, the Luxembourgish FNR, the Academy of Finland and the US NSF.



Shen WANG

Robust Federated learning for 6G Networks

ABSTRACT

Federated learning (FL) is considered as one of the key enabling technologies for future AI-assisted 6G applications. Uniquely crafted to enhance data privacy, FL operates by exchanging only model updates between server and clients, rather than the training data itself. Despite its design to safeguard privacy, FL remains susceptible to a myriad of security and privacy risks, including the potential reconstruction of private data from model updates. This talk will embark on an introduction to the security and privacy challenges that arise when implementing FL within 6G networks. Special emphasis will be placed on the research being conducted at NetsLab, which includes the application of explainable AI technologies, that offers a nuanced perspective on resilience and the intricate balance between privacy and accuracy. The talk will conclude with discussions on other possible solutions that are worth exploring in the near future to make FL more robust for 6G networks.

JOB TITLE

Associate Professor

AFFILIATION

UNIVERSITY COLLEGE DUBLIN

BIO

Dr. Shen Wang is an Assistant Professor at the School of Computer Science, University College Dublin, Ireland. He received an M.Eng. degree from Wuhan University, China, and a Ph.D. degree from Dublin City University, Ireland. Dr. Wang has been involved with several EU projects as a co-PI, WP, and Task leader in big trajectory data streaming for air traffic control and trustworthy AI for intelligent cybersecurity systems. Some key industry partners of his applied research are IBM Research Brazil, Boeing Research and Technology Europe, and Huawei Ireland Research Centre. He is also a senior member of IEEE and the recipient of the IEEE Intelligent Transportation Systems Society Young Professionals Travelling Fellowship 2022. His research interests include connected autonomous vehicles, explainable artificial intelligence, and security and privacy for mobile networks.


AGENDA

11 September 2023

08:30 AM - 05:00 PM CEST

UCD University Club


UNIVERSITY COLLEGE DUBLIN
DUBLIN, IRELAND

- 
- 08:30-09:00 **REGISTRATION**
 - 09:00-09:20 **OPENING REMARKS AND INTRODUCTION TO NETSLAB**
 - 09:20-09:40 **WELCOME SPEECH ABOUT UCD AND CS**
 - 09:40-10:00 **PROJECT HIGHLIGHT - CONNECT**
 - 10:00-10:20 **PROJECT HIGHLIGHT - SPATIAL**

COFFEE

- 
- 10:45-11:15 **TALK 1** EDGARDO MONTES DE OCA *Montimage, France*
EXPLAINABILITY OF AI-BASED CYBERSECURITY SOLUTIONS
 - 11:15-11:45 **TALK 2** NICOLAS KOURTELLIS *Telefonica Research, Spain*
HARNESSING THE POWER OF PRIVACY: ADVANCING INTO THE 6G ERA WITH AI
 - 11:45-12:15 **TALK 3** MICHAEL ZIMMER, *Marquette University, USA*
BUILDING PRIVACY AND ETHICS INTO FUTURE MOBILE PLATFORMS

NETWORKING LUNCH AND POSTER SESSION

- 
- 13:30-14:00 **TALK 4** HOUDA LABIOD *Huawei Research, France*
A MULTI-LAYER TRUST FRAMEWORK FOR FUTURE COMMUNICATION SYSTEMS
 - 14:00-14:30 **TALK 5** SAMUEL MARCHAL *WithSecure, Finland*
SECURITY ASSESSMENT OF ML-BASED SYSTEMS UNDER REALISTIC ATTACKER CAPABILITIES
 - 14:30-15:00 **TALK 6** AENGUS GOREY *Analog Devices, Ireland*
ESTABLISHING TRUST IN THE DATA WE USE TO DRIVE AUTOMATION & AUTONOMOUS DECISION-MAKING!

COFFEE

- 
- 15:30-16:00 **TALK 7** SHEN WANG *UCD, Ireland*
FL SECURITY AND PRIVACY IN 6G
 - 16:00-16:45 **PANEL DISCUSSION** (ALL SPEAKERS)
 - 16:45-17:00 **CLOSING REMARKS & FUTURE PLAN**