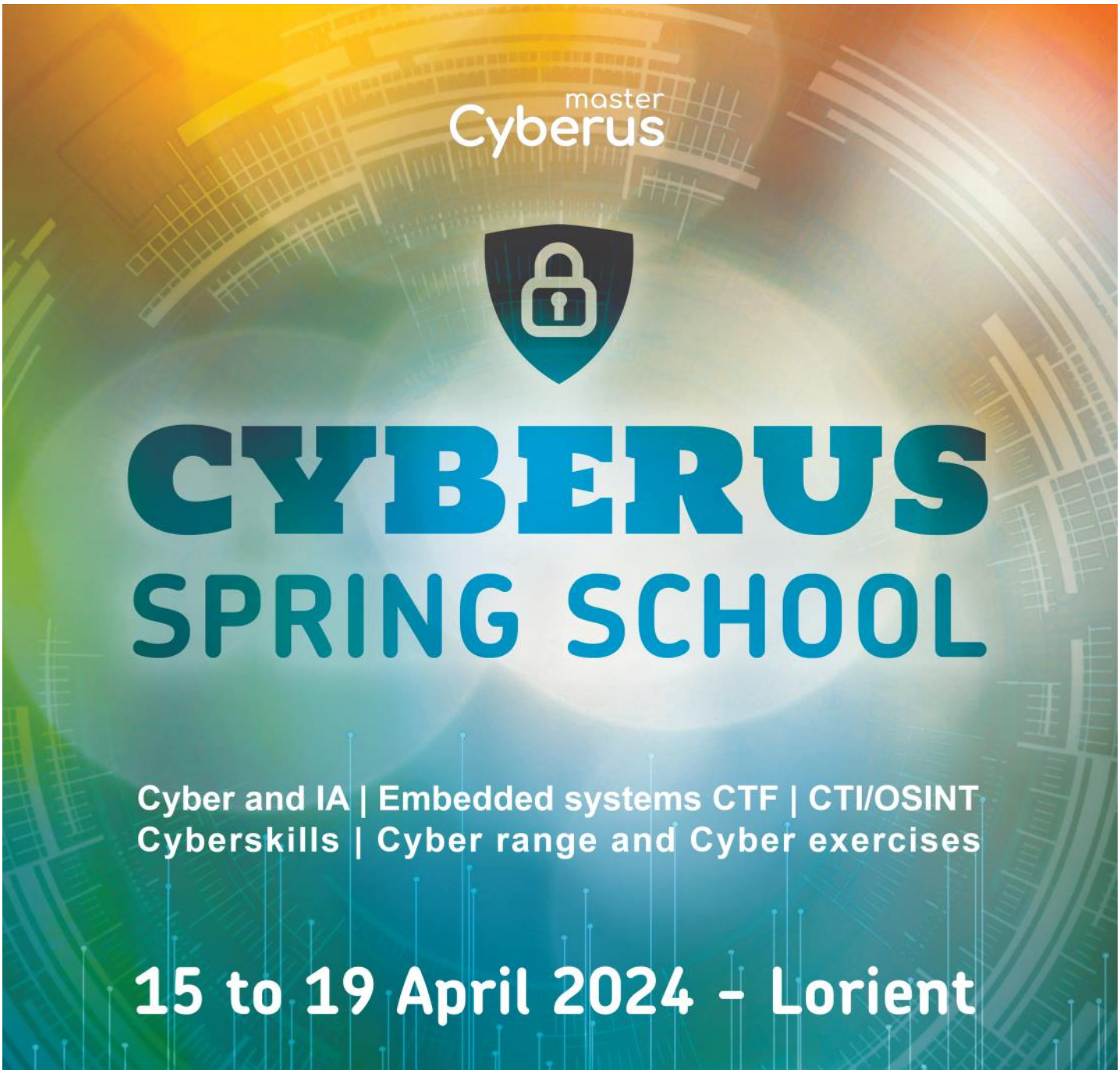

Co-funded by
the European Union

SCHEDULE

	Monday April 15, 2024	Tuesday April 16, 2024	Wednesday April 17, 2024	Thursday April 18, 2024	Friday April 19, 2024
8h30-9h30			Transfer to UBS Campus in Vannes	Chairman: Guy Gogniat **Oral poster presentation** Room: Amphi	Chairman: Guy Gogniat **Software and Communication security** Room: Amphi
9h00-9h30		Chairman: Jean Peeters **Cyberskills** Room: Amphi			
9h30-10h30			Chairman: Jack Noel **Cyber range and Cyber exercises**	Chairman: Guy Gogniat **NTNU session** Room: Amphi	
10h30-11h00		**Coffee break** Room: 009	**Coffee break**	**Coffee break** Room: 009	**closing session** Room: Amphi
11h00-12h00		Chairman: Jean Peeters **Cyberskills** Room: Amphi	Chairman: Jack Noel **Cyber range and Cyber exercises**	Chairman: Guy Gogniat **Poster session** Room: Front of Amphi	**Coffee** Room: 009
12h00-13h00 13h00-13h30	**Welcome coffee and brunch** Room: 009	**Lunch** Room: 009	**Lunch**	**Lunch** Room: 009	
13h30-14h00	**Opening session** Room: Amphi				
14h00-15h00	Chairman: Guy Gogniat **Cyber and IA** Room: Amphi	Chaiman: Jamal El Hachem **CTI/OSINT** Room: Amphi	Vannes and Discovery Trip in Gulf of Morbihan	Chairman: Guy Gogniat **Cyber and IA** Room: Amphi	
15h00-16h00				Chairman: Philippe Tanguy **Embedded systems CTF** Room: 108	
16h00-16h30	**Coffee break** Room: 009	**Coffee break** Room: 009			
16h30-17h00	Chairman: Philippe Tanguy **Embedded systems CTF** Room: 108	Chaiman: Jamal El Hachem **CTI/OSINT** Room: Amphi			
17h00-17h15					
17h15-17h30					
17h30-18h30		Chairman: Philippe Tanguy **Embedded systems CTF** Room: 108	Transfer to Lorient		
18h30-19h30			Free evening		
19h30-20h30	Welcome cocktail Room: 009	Free evening		**CTF Award ceremony** Room: Amphi	
20h30-21h30				Free evening	

Faculty of Sciences and Engineering Sciences in Lorient
2 Rue le Coat Saint-Haouen, 56100 Lorient

Welcome to CYBERUS spring school 2024

Pr. Guy GOGNIAT
Université Bretagne Sud

The CYBERUS Spring School 2024 will be held from April 15 to 19, 2024. This year's programme is very rich, with sessions addressing cybersecurity and AI, threat analysis, cyber crisis management, software vulnerability and communications systems, to name but a few.

The CYBERUS spring school will also be an opportunity to test your level of expertise in cybersecurity by taking part in the embedded systems CTF. The challenge runs through the week, with an awards ceremony on Friday April 19.

The question of training will also be at the heart of this event, with speakers from the main European players in the field.

The CYBERUS Spring School is a unique opportunity to meet international experts in the field and delve into the fascinating world of cybersecurity.

We wish you an excellent The CYBERUS Spring School and hope you enjoy the exceptional programme.

Session Cyber & AI

Monday, April 15

14 to 15:00

Security and Privacy Challenges in Large-Language Models and Generative AI

This talk explores the evolving landscape of generative AI and large language models, spotlighting the security and privacy challenges they introduce. As these technologies advance, they present unique vulnerabilities, including the potential for generating misleading content and leaking sensitive information. We delve into various mitigation strategies, such as differential privacy and federated learning, aimed at safeguarding data integrity and user privacy. Additionally, the discussion emphasizes the necessity of ethical considerations in AI development and suggests future research directions to fortify the security and privacy frameworks of generative AI systems, ensuring their responsible and secure application in diverse domains.

Prof. Constantine DOVROLIS

The Cyprus Institute and Georgia Tech

Dr. Constantine Dovrolis is the Director of the centre for Computational Science and Technology (CaSToRC) at The Cyprus Institute (CyI) as of 1/1/2023. He is also a Professor at the School of Computer Science at the Georgia Institute of Technology (Georgia Tech). He is a graduate of the Technical University of Crete (Engr.Dipl. 1995), University of Rochester (M.S. 1996), and University of Wisconsin-Madison (Ph.D. 2000). His research is highly interdisciplinary, combining Network Theory, Data Mining and Machine Learning. Together with his collaborators and students, they have published in a wide range of scientific disciplines, including climate science, biology, and neuroscience. More recently, his group has been focusing on neuro-inspired architectures for machine learning based on what is currently known about the structure and function of brain networks. According to Google Scholar, his publications have received more than 15,000 citations with an h-index of 56. His research has been sponsored by US agencies such as NSF, NIH, DOE, DARPA, and by companies such as Google, Microsoft and Cisco. He has published at diverse peer-reviewed conference and journals such as the International Conference on Machine Learning (ICML), the ACM SIGKDD conference, PLOS Computational Biology, Network Neuroscience, Climate Dynamics, the Journal of Computational Social Networks, and others.

The Cyprus Institute
RESEARCH·TECHNOLOGY·INNOVATION

Session Cyber & AI

Monday, April 15

15 to 16:00

Requirements for applying Artificial Intelligence to Network Security: Identification of Self and Nonself and avoiding Profiling Attacks

In this presentation, we will first introduce the Wirid Lab, a connected remote laboratory with both development and research capabilities. Following this, we will explore the prerequisites for the potential integration of artificial intelligence (AI) into the domain of network security, drawing inspiration from the intricate defense mechanisms found in the natural immune system. Our discussion will delve into the conceptualization of telecommunications networks as complex systems that demand vigilant protection against a myriad of threats. Furthermore, we will examine practical applications within the context of LoRa systems, illustrating how AI could potentially be exploited by attackers to profile vulnerabilities. Lastly, we will address the requirements for enhancing IoT designs in light of these emerging challenges.

Edward GUILLÉN

Research Professor

Military University Nueva Granada –UMNG

University of Rennes 1

Professor Edward Guillen is an electronic engineer with a master's degree in teleinformatics and a doctorate in engineering with a focus in telecommunication networks and cybersecurity fields. He has worked as a professor and researcher in the fields of telecommunications and network security for nearly 22 years. Throughout his research and teaching experience, he has been involved in training and research programs at various universities in Colombia, France, and the United States. He leads the Security and Telecommunications Systems Research Group (GISSIC) at UMNG. He served as the director of the doctoral school in applied sciences at UMNG and as the director of the Telecommunications Engineering Department at UMNG. Currently, he is also affiliated as researcher with the University of Rennes 1.

Universidad Militar Nueva Granada

Embedded systems CTF

All week long

The embedded systems CTF is a CTF (capture the flag) type of computer security competition conceived by Lab-STICC researchers and CSSE Master students from the University Bretagne Sud.
Compared to other CTFs, the challenges are focused on embedded systems and hardware. Each team is provided with an embedded system and the necessary equipment to solve the challenges. More traditional challenges (software, cryptography, etc.) will also be proposed.
The CTF will be run as a team competition.

Adam HENAULT

Student | master UBS/CSSE

Adam HENAULT is a student in hardware cybersecurity in the CSSE Master's program at the University of South Brittany in Lorient. As an reverse engineer enthusiast, I enjoy unravelling the intricacies of various software and hardware components, which has led me to game hacking, CTFs, Windows internals, and hardware such as FPGAs.

Philippe TANGUY

Associate Professor | UBS | LabsTICC team ARCAD

He teach at the Université de Bretagne Sud in the UFR SSI. He is the study director of the Master of Cybersecurity of Embedded Systems (CSSE) at UBS. He performs his research activities at Lab-STICC in the ARCAD team.
Currently, his research activities are dedicated to IoT system with a focus on the Cyber Security issues.

Session Cyberskills

Tuesday, April 16

9:00 to 9:45

Empowering European Cybersecurity Professionals: An Overview of the European Cybersecurity Skills Framework (ECSF)

This presentation provides a high level overview of the European Cybersecurity Skills Framework (ECSF). The ECSF serves as a practical aid in defining and understanding the tasks, competences, skills, and knowledge essential for European cybersecurity professionals. It acts as the official EU guidepost for defining and evaluating pertinent skills, as outlined in the Cybersecurity Skills Academy, a recent initiative by the European Commission. Comprising 12 distinct profiles, the ECSF thoroughly dissects each role, delving into their respective responsibilities, skills, synergies, and interdependencies. By doing so, it fosters a unified comprehension of these roles, competencies, skills, and knowledge crucial within the cybersecurity realm.

Anna SARRI

Cybersecurity Officer in Capacity Building Unit
European Union Agency for Cybersecurity

Anna Sarri is a Cybersecurity Officer at the European Union Agency for Cybersecurity (ENISA), where she spearheads capacity-building initiatives and fosters community empowerment by sharing best cybersecurity practices. With a focus on Cybersecurity for Small and Medium Size Businesses (SMEs), she champions diversity in cybersecurity endeavors and devises indicators to track the European market's evolution, addressing the cybersecurity talent gap. Anna brings extensive expertise in developing capabilities to bolster National Cyber Security Strategies for EU Member States and supporting the implementation of NIS Directives. Previously, she accrued over a decade of experience in the telecom sector, holding various roles including IT Security engineer and technical support team leader. Anna holds a B.Sc. in Computing, an M.Sc. in Information Security and Computer Crime from the University of South Wales, UK, and a certificate in Managing Cybersecurity Risk from Harvard University.

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Session Cyberskills

Tuesday, April 16

9:45 to 10:30

Cyber competencies : not just for specialists !

Presentation of work on cyber competencies :

- inside the dedicated working group of the national cyber campus, with the aim of creating a common matrix of cyber competencies for learners, training centres, businesses and administrations.
- for the "CyberEdu" label, which advises training managers at national and local level on how to integrate contextualised cyber skills into training courses for non-specialist cyber users.

Julien BREYAULT

Cyber defense teacher | ENSIBS, UBS

Head of teaching for cyber defence vocational training
Chairman of the CyberEdu association for ANSSI
Member of the EBIOS Club and Campus Cyber training working groups

Session Cyberskills

Tuesday, April 16

11:00 to 12:00

Boosting competitiveness, participation and talent : the European perspective and actions for a skilled workforce in cyber.

Today, private and public organisations are paying the price of the increasing exposure to cyber threats and a lack of skilled workforce. Moreover, the introduction of new policies (NIS2, Cyber Resilience Act…) will require more skilled professionals in this field. It is time to propose and implement new ideas.

EU perspective (initiatives at the EU level): How can we ensure that the needs of the labour market are reflected in public policy and public/private partnership initiatives ? How can we connect industry and universities? There are several policy framework and initiatives to encourage efforts to attract skilled people in the field. (The Cyber Skills Academy, CyberHead, the European Cybersecurity Skills Framework.

ECSO contributes towards a cybersecurity capability and capacity-building effort for a cyber resilient next generation (NextGen) digital Europe, through increased education, skills development, access to trainings and jobs, as well as actions on awareness-raising and gender inclusiveness. (Road2Cyber, European HR Community, Youth4Cyber, Cyber Ranges Checklist, Policy angle and recommendations).

Arnaud de VIBRAYE

Manager - skills & human factors | ECSO

Arnaud de Vibraye is Manager for Skills and Human Factors at the European Cyber Security Organisation, in the Working Group to develop a European cyber security education & skills ecosystem. As part of ECSO's mission to strengthen the digital strategic autonomy of Europe and a educate professionals and citizens, he manages the European HR Community for cyber to boost the recruitment process, monitors EU policies and initiatives on skills, and contributes to the creation and launch of the platform Road2Cyber to encourage career paths in the field and increase workforce in Europe.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Session CTI / OSINT

Tuesday, April 16

14 to 17:30

"Why did I decide to write cyber thrillers ? Because we've gone from the Cold War to the Code War"

Threat analysis has been a key issue for companies and state institutions for decades. With the development of the cyber threat since the 2000's, the emergence of Cyber Threat Intelligence (CTI) has been gaining increasing enthusiasm among intelligence services, security teams and so forth. Through this class, we will discover different aspects of CTI. Combinated with Open Source Intelligence (OSINT), let's discover how to produce his own intelligence and get useful insight to protect companies against cyber threat actors.

Thibaud MAGNE

Cyber Threat Intelligence Analyst | ANSSI / CERT-FR

Through cybersecurity and geopolitics classes of ENSIBS, Thibauld MAGNE became passionate about Cyber-defense mecanisms. Thanks to a four years of apprenticeship in EDF Security Operation Center, he has the possibility to discover technical aspect of cyber threat intelligence. Nowadays, his mission in ANSSI leds him to discover other aspect of CTI, as strategical CTI.

Session Cyber range and Cyber exercises

Wednesday, April 17

9:30 to 13:00 | Vannes Campus

Wednesday's session is devoted to crisis management, with a particular focus on cyber. As soon as 2013, UBS has been using a tool - a Cyber Range - to develop and play out realistic exercises. The most recent exercise took place a few weeks ago and applied to the agri-food industry. As a Cyber Lab, this tool can also be used for innovation and research. The session will feature a presentation of the UBS's experience in setting up this type of exercise (Mawloud), as well as two specific focuses that contribute to it: forensics (Pavel) and Planning Penetration Testing of Cyber-Physical Systems (Shaymaa).

Shaymaa MAMDOUH KHALIL

is a PhD candidate and early-stage researcher at the Center for Digital Forensics and Cyber Security at Tallinn University of Technology, Estonia. She holds a Bachelor of Science degree in Electronics and Communication Engineering from Cairo University (2006) and an MBA from the University Paris Dauphine and the University Paris 1 Panthéon-Sorbonne (2013). In 2020, Shaymaa received a Master of Science degree with honors in Cyber Security, specializing in Digital Forensics, from Tallinn University of Technology and the University of Tartu. Her research interests lie in cyber-physical systems security and digital forensics.

Pavel TSIKUL

is a Ph.D. candidate and early-stage researcher at the Center for Digital Forensics and Cyber Security at Tallinn University of Technology, Estonia. His academic journey began with a Bachelor of Science degree in Applied Informatics from Tallinn University of Technology, followed by a Master of Science in Cyber Security (Digital Forensics), which he received in 2019 from Tallinn University of Technology and the University of Tartu. His research interests revolve around cyber-physical systems security and digital forensics. Specifically, he is intrigued by the challenges posed by cyber-physical systems and the methodologies for forensic analysis in distributed environments. In addition to his research endeavors, he is actively involved in teaching. He leads lectures for the ITX8200 System Forensics course, where he blends theoretical insights with practical skills to prepare students for the intricacies of real-world challenges in digital forensics.

Mawloud OMAR

is a Full Professor at ENSIBS - University of South Brittany and a member of the IRISA laboratory. He leads the specialty in information systems security. He got his Ph.D. and Magister degrees in Computer Science from the University of Bejaia, Algeria, and his habilitation to supervise research from the University Paris-Est. Previously, he served as an Associate Professor at ESIEE Paris - University of Gustave Eiffel and as a Senior Researcher at IRT SystemX. He has also held positions as a Lecturer and Researcher at the University of Technology of Compiegne and the University of Bejaia. His teaching and research focuses primarily on cybersecurity, with particular interest in challenges related to networks of new generation, the Internet of Things, connected vehicles, and industrial environments.

Oral poster presentation

Thursday, April 18

8:30 to 9:30

Ehtesham Hashmi | NTNU

Multilingual Hate Speech Detection

Arne Roar Nygård | NTNU

Leveraging Hardware Reverse Engineering to Improve the Cyber Security and Resilience of the Smart Grid

Aida Akbarzadeh | NTNU

Dependency based risk analysis in Cyber Physical Systems

Mohamed El Bouazzati | UBS

Diwall: Lightweight Host-based Intrusion Detection System for Wireless Attacks on IoT Devices

Ahmed Elmarkez | UBS

Security-by-design for a secure industrial control system design

Kamel Aizi | UBS

Deep-Learning-Based Side-Chanel Attack

Nicolas Gaudin | UBS

SCRATCHS : Side-Channel Resistant Applications Through Co-designed Hardware/Software

Kévin Quénéhervé | UBS

Characterizing Clock Glitching Attacks on CVA6 PMP Configuration Flow

William Pensec | UBS

Automating Fault Injection through CABA Simulation for Vulnerability Assessment

NTNU
Norwegian University of Science and Technology

Université Bretagne Sud
ubs

Session organized by NTNU

Thursday, April 18

09:30 to 10:30

Building World Class Cyber Security Training Facilities Experience in researching and building a cyber range -NCR

Rome wasn't built in a day, but its destruction in six shows the inevitability of fire without proper safeguards. Similarly, our digital world, lacking robust security measures, faces countless compromises. Efforts to train for secure digital operation are ongoing, yet cyber-attacks persist. Traditional methods, like classroom teaching, fall short in delivering practical cybersecurity skills due to complexity and cost. Attempts to automate training processes have seen limited success, lacking standardized scenarios. Addressing these challenges, a novel approach using domain-specific language for scenario modeling offers efficiency, realism, and standardization in cybersecurity exercises. Tested in various settings, including national competitions, this method shows promise in enhancing cybersecurity readiness.

Muhammad Mudassar Yamin

Associate Professor | Norwegian University of Science and Technology (NTNU)

Dr. Muhammad Mudassar Yamin is currently working as an Associate Professor at the Department of Information and Communication Technology at the Norwegian University of Science and Technology (NTNU). He is a member of the system security research group, and the focus of his research is on system security, penetration testing, security assessment, and intrusion detection. Before joining NTNU, Mudassar worked as an Information Security consultant and served multiple government and private clients. He holds multiple cybersecurity certifications, such as OSCE, OSCP, LPT-MASTER, CEH, CHFI, CPTE, CISSO, and CBP.

NTNU
Norwegian University of Science and Technology

Session organized by NTNU

Thursday, April 18

10 to 10:30

Theories and Methods from Economics and Finance for Information Security Risk Management

The presentation navigates through the complex cyber risk landscape, introducing the integration of economic and financial theories into cybersecurity risk management, which offers a sophisticated framework for understanding and mitigating cyber threats. This presentation delves into the various economic and financial models that can be leveraged to enhance decision-making processes in cybersecurity investments and policy formulation. Beginning with an overview of cybersecurity economics, it outlines the critical need for adopting economic perspectives in managing cyber risks, highlighting the intersection between economics, finance, and cybersecurity.

Pankjaj Pandey

Researcher | Norwegian University of Science and Technology (NTNU)

Dr Pandey is a Research Scientist at the Center for Cyber and Information Security, Norwegian University of Science and Technology, Campus - Gjovik, Norway. He is managing a significant European Commission-funded research and innovation project called ENFIELD: European Lighthouse to Manifest Trustworthy and Green AI, where 30 European partners from 18 countries representing academia, SMEs, and industry are participating. Dr Pandey holds a PhD in Information Security and a second PhD in Applied Economics. He also holds an LLM in international law. Dr Pandey is a Certified Senior Lead Risk Manager (ISO 31000), Senior Lead Auditor (ISO 27001), and Senior Lead Crisis Manager (ISO 22361).

NTNU
Norwegian University of Science and Technology

Poster session

Thursday, April 18

11 to 12:00

Ehtesham Hashmi | NTNU

Multilingual Hate Speech Detection

Arne Roar Nygård | NTNU

Leveraging Hardware Reverse Engineering to Improve the Cyber Security and Resilience of the Smart Grid

Aida Akbarzadeh | NTNU

Dependency based risk analysis in Cyber Physical Systems

Mohamed El Bouazzati | UBS

Diwall: Lightweight Host-based Intrusion Detection System for Wireless Attacks on IoT Devices

Ahmed Elmarkez | UBS

Security-by-design for a secure industrial control system design

Kamel Aizi | UBS

Deep-Learning-Based Side-Chanel Attack

Nicolas Gaudin | UBS

SCRATCHS : Side-Channel Resistant Applications Through Co-designed Hardware/Software

Kévin Quénéhervé | UBS

Characterizing Clock Glitching Attacks on CVA6 PMP Configuration Flow

William Pensec | UBS

Automating Fault Injection through CABA Simulation for Vulnerability Assessment

NTNU
Norwegian University of Science and Technology

Université Bretagne Sud
ubs

Session Cyber & AI

Thursday, April 18

14 to 16:00

Machine learning for cybersecurity and its challenges

The use of data-driven methods in the field of cybersecurity has been a hot research topic in the last years. The talk will review, with some examples, the most common applications of machine learning in threat detection and identification. Promising future research directions will be discussed, as well as the main challenges that need to be addressed to achieve practical applicability, such as data collection, concept drift and domain adaptation.

Miguel A. PRADA

Associate Professor | Universidad de León

Miguel A. Prada was born in 1981. He received his degree in computer engineering and his Ph.D. from the Universidad de León, León, Spain, in 2003 and 2009, respectively. He has worked at the Aalto University, Finland, and the Universidad de León, Spain. He is currently an Associate Professor at the Department of Electrical and Systems Engineering of the Universidad de León. His research interests include machine learning and its industrial applications, cybersecurity of industrial control systems, and innovation of education in control engineering and automation.

universidad de león

Automated Test-free Repair of Vulnerable Programs

Most program repair techniques rely on test cases as a key ingredient for driving patch generation and validation. Test cases have been successfully leveraged to automate the repair of many bug classes, but relying on them has hindered progress in repairing vulnerabilities. Their scarcity, exacerbated by the fact that, for vulnerabilities, test cases are also exploits, forms a “sound” barrier that we propose to break in this work. To this end, we introduce Nerve, a novel deep learning -based approach for automating vulnerable software repair. Instead of tests, Nerve leverages the signal in the vulnerability detection and fix suggestions of static analysis security testing (SAST) to learn to repair vulnerable code. Nerve’s learning architecture relies on CodeT5 pre-trained model for source code representation, augmented with a mixed learning objective. This involves, first, the use of triplet loss to build an embedding space that brings each vulnerable code closer to good fixes while keeping it away from incorrect fixes. The second learning objective incorporates cosine similarity into its loss function to align its repair candidates with SAST fix suggestions.

We assess Nerve on over 3,000 real-world vulnerable code samples in C/C++, C#, Python, and Java programs. We show that NERVE advances the state of the art in neural vulnerability repair, outperforming VulRepair, the incumbent, by 7.5% points in sequence accuracy, 5% points in CodeBLEU, and 3% points in Normalized Discounted Cumulative Gain (NDCG) for the repair of C/C++ programs. For the other programming languages in the dataset, we provide baselines for future work. Finally, we present a comparison of NERVE with large language model (LLM) using prompts that include different inputs. Our results show that NERVE performed better on some samples compared to LLMs, but also demonstrate that, as with NERVE, SAST results have a positive impact on the performance of these LLM.

Abdoul Kader KABORÉ
Doctoral Researcher | University of Luxembourg

Abdoul Kader KABORE is a Doctoral Researcher in Software Security and Software Engineering at the University of Luxembourg. He is part of the Interdisciplinary Centre for Security, Reliability and Trust and member of the TruX research Group.
His research interests are machine learning applied to software engineering and software security. His PhD topic is about automatic vulnerability repair.

Software and Communication security

Friday, April 19

9:30 to 10:30

Anonymous Communication Networks

This talk delves into Anonymous Communication Networks, focusing on Tor and mixnets, to examine their distinct designs and how they defend against various adversaries. We explore what does anonymity means and how to quantify it. Attendees will gain insights into the myriad of design decisions and the necessary trade-offs concerning practicality, performance, and the degree of anonymity. The presentation will highlight key topics, including metrics for anonymity, its properties, potential attacks, and the strategies for counteracting these threats. Additionally, the talk will showcase some of the proposed and already implemented mixnet projects.

Iness BEN GUIRAT
Postdoctoral Researcher | Université Libre de Bruxelles

Iness Ben Guirat is a postdoctoral researcher at the Université Libre de Bruxelles (ULB), working with Prof. Jean-Michel Dricot and Prof. Jan-Tobias Mühlberg. Her research is focused on Privacy, with a specific focus on mixnets. Iness has a keen interest in exploring the intersection of technology, privacy and their broader impact on society.

ULB UNIVERSITÉ LIBRE DE BRUXELLES