Université Bretagne Sud

UNIVERSITÉ LIBRE DE BRUXELLES

UNIVERSITÉ DU LUXEMBOURG

Co-funded by the European Union

Schedule

	Monday April 7, 2025	Tuesday April 8, 2025	Wednesday April 9, 2025	Thursday April 10, 2025	Friday April 11, 2025
9h30-10h00		Chairman: Mohamed El Bouazzati **Smart Cryptography: Applying Machine Learning for Stronger Protection** Vesna Dimitrova Room: Amphi	Chairman: Guy Gogniat **Introduction to Anonymous Communication Networks** Iness Ben Guirat Room: Amphi	Chairman: Guy Gogniat **Program Analysis: Challenges and Opportunities** Jordan Samhi Room: Amphi	Chairman: Guy Gogniat **Cryptographic screaming-channel attacks** Jérémy Guillaume **Room: Amphi**
10h00-10h30					Chairman: Guy Gogniat **Wireless Security for the Internet of Things: Threats and Intrusion Detection System** Mohamed El Bouazzati Room: Amphi
10h30-11h00		**30' Coffee break**	**30' Coffee break**	**30' Coffee break**	**60' Coffee break & Poster session**
11h00-11h30		Chairman: Mohamed El Bouazzati **Post-quantum cryptography** Sedat Akleylek Room: Amphi	Chairman: Guy Gogniat **An Introduction to Formal Methods for Cyber Security** Achim Brucker Room: Amphi	Chairman: Guy Gogniat **Mobile Security: years of improvement, yet challenges remain** Jordan Samhi Room: Amphi	
11h30-12h00					**CTF Award ceremony & closing session** Room: Amphi
12h00-13h30		**Lunch break**	**Lunch break**	**Lunch break**	
13h30-14h00		Online session with CYBERUS Alumni	Social event Visit to Port Louis	Chairman: Philippe Tanguy & Adam Henault **Embedded systems CTF** Rooms: 107 & 108	
14h00-14h30	**Opening session** Room: Amphi				
14h30-15h00	Chairman: Philippe Tanguy & Adam Henault **Embedded systems CTF** Rooms: 107 & 108	Chairman: Philippe Tanguy & Adam Henault **Embedded systems CTF** Rooms: 107 & 108			
15h00-16h00					
16h00-17h00					
17h00-18h00					
18h00-19h0			Free evening		
19h00-20h00	Welcome cocktail Room: 009	Free evening		Free evening	
20h00-21h00					

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

WELCOME TO THE CYBERUS SPRING SCHOOL 2025

The CYBERUS Spring School 2025 will be held at Université Bretagne Sud, Lorient, France, from April 7 to 11, 2025. This year's programme is very rich: cryptography, mobile security, communication security, data privacy to name but a few.

Pr. Guy GOGNIAT
Université Bretagne Sud

The CYBERUS Spring School will also be an opportunity to test your level of expertise by taking part in the embedded systems CTF. Just as in 2024, this year’s edition will include students from other universities in Turkey, North Macedonia, Germany and the UK. Students will compete in teams. The challenge runs through the week, with an awards ceremony on Friday April 11.

The CYBERUS Spring School is a unique opportunity to meet international experts in the field and delve into the fascinating world of cybersecurity. You will a have a chance to hear presentations from junior and senior researchers, to discuss poster presentations with PhD candidates and also to share your experience with CYBERUS alumni.

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

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

PhD Student | UBS | LabsTICC team ARCAD

Adam HENAULT is a PhD student in hardware security in the ARCAD team of the Lab-STICC. He has a Master degree on embedded systems security at the University of South Brittany in Lorient. As an reverse engineer enthusiast, he enjoys unravelling the intricacies of various software and hardware components, which has led him to game hacking, CTFs, Windows internals, and hardware such as FPGAs.

Philippe TANGUY

Associate Professor | UBS | LabsTICC team ARCAD

He teaches at the Université 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.

SCIENTIFIC SESSION

TUESDAY, APRIL 7

09:30 TO 10:30

Smart Cryptography: Applying Machine Learning for Stronger Protection

In today's rapidly evolving digital technology, the integration of machine learning (ML) into cryptography offers promising advancements in securing data and communication systems. This presentation explores the intersection of ML and cryptography, highlighting how machine learning techniques are being applied to enhance cryptographic protocols, improve key generation, optimize random number generation, and strengthen intrusion detection systems; what is the role of machine learning in cryptanalysis, demonstrating how it is used to detect weaknesses in encryption algorithms and recover cryptographic keys; and how ML can optimize the performance of privacy-preserving methods like homomorphic encryption and federated learning, ensuring the confidentiality of sensitive data while enabling powerful computations. This presentation offers a comprehensive overview of these applications and discusses the potential challenges and future directions of this intersection.

Prof. Vesna DIMITROVA

Faculty of Computer Science and Engineering, "Ss. Cyril and Methodius" University in Skopje, R. N. Macedonia

Vesna Dimitrova is currently a Full Professor at the Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University, where she is also the Head of Department for Theoretical Foundations of Informatics and Computational Engineering and the Coordinator of the Master studies of Security, Cryptography and Coding. Also, she is the local coordinator of Erasmus Mundus project titled CyberMACS, which stands for a Master's Program in Applied Cybersecurity She participated/managed more than 30 international/national projects (Erasmus Mundus, Erasmus Plus from the H2020 program, COST actions, bilateral project with the People's Republic of China, etc.). She was a chair of two International Conference and a member of program/scientific committee at more than 40 conferences. She has published over 80 scientific papers. She participated in more than 100 conferences/workshops in the country and abroad. She is the editor of several books/proceedings and appears as an expert reviewer of two books in the field of Cryptography. She was vice-dean of Finance at the Faculty of Computer Science and Engineering, vice-president of the ICT-ACT Association, head of the FCSE Career Center, a member of the Management Committee of seven international projects and a member of several other committees. The main areas of scientific interest are: information security, cryptography, cryptanalysis, risk information security management, application of ML and DL in cybersecurity.

Scientific session

Tuesday, April 11
11:00 to 12:00

Recent Advances in Post-Quantum Cryptography

In this talk, we will give a brief survey on the importance of post-quantum cryptography by describing current approaches. Then, we will discuss the computationally hard problems used in post-quantum cryptographic schemes focusing on lattice-based cryptography (key encapsulation mechanisms and digital signature schemes). The focus will be given to the NIST Post-Quantum Cryptography Standardization Project. We will also discuss the open problems in post-quantum cryptography.

Prof. Sedat AKLEYLEK

Institute of Computer Science, University of Tartu, Tartu, Estonia

Sedat Akleylek received the B.Sc. degree in mathematics majored in computer science from Ege University, Izmir, Türkiye, in 2004, and the M.Sc. and Ph.D. degrees in cryptography from Middle East Technical University, Ankara, Türkiye, in 2008 and 2010, respectively. He was a Postdoctoral Researcher at the Cryptography and Computer Algebra Group, TU Darmstadt, Germany, between 2014 and 2015. He worked as a Professor at the Department of Computer Engineering, Ondokuz Mayıs University, Samsun, Türkiye till 2022. He has started to work at the Chair of Security and Theoretical Computer Science, University of Tartu, Tartu, Estonia, since 2022. His research interests include post-quantum cryptography, algorithms and complexity, blockchain, architectures for computations in finite fields, applied cryptography for cyber security, malware analysis, IoT security, and avionics cyber security. He is the co-chair of IEEE Türkiye Blockchain Group. He is a member of the Editorial Board of IEEE Access, Turkish Journal of Electrical Engineering and Computer Sciences, Peerj Computer Science, and International Journal of Information Security Science.

Scientific session

Wednesday, April 9

09:30 to 10:30

Introduction to 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 currently a postdoctoral researcher, working with Prof. Jean-Michel Dricot and Prof. Jan-Tobias Mühlberg at the intersection of privacy and security. She also serves as the Officier de Liaison for the CyberExcellence project. She earned her PhD in 2024 from COSIC, KU Leuven, under the supervision of Prof. Claudia Diaz, focusing on privacy, with a particular emphasis on mixnets.

SCIENTIFIC SESSION

WEDNESDAY, APRIL 9

11:00 TO 12:00

An Introduction to Formal Methods for Cyber Security

Our modern life depends on the correctness of security protocols such as OAuth or TLS, which are used for establishing authentic and confidential communication channels in public networks, such as the Internet. Hence, it is crucial that these protocols achieve their security objectives.

While security protocols are often perceived as “small”, designing and implementing them correctly is a challenge: they are highly distributed systems that need to establish their security guarantees also when operating in a (partially) untrustworthy environment and in the presence of threat actors.

In this lecture, I will give a general introduction to security protocols and demonstrate selected attacks on them. Furthermore, using security protocols as an application domain, I will provide an introduction into formal methods in general and their application in security-critical applications in particular.

Prof. Achim BRUCKER

Department of Computer Science, University of Exeter, UK

Professor in Computer Science (Chair in Cybersecurity) and Head of the Cybersecurity Group at the University of Exeter, UK. He has over 20 years of professional experience in cybersecurity in general, and, in particular, in research and development of safety and security critical systems. In his work, he particularly focuses on techniques, methods, and tools for ensuring the safety, security, correctness, and trustworthiness of advanced systems. His industry experience includes being a Security Architect and Security Testing Strategist for SAP SE. In this role, he defined the risk-based security testing strategy of SAP that combines static, dynamic, and interactive security testing methods and integrates them deeply into SAP’s Secure Software Development Life Cycle. He also led the team implementing this new security testing strategy across all development locations of SAP—a world-wide effort supporting over 25000 developers. He continues to work closely with industry, e.g., as technical advisor and member of the Advisory Board of Anzen Technology Systems Ltd. His research interests cover broad areas of Formal Methods (Verification, Computational Logic), Cybersecurity (including Privacy, Information Security, Software Security, Hardware Security), and Software Engineering (e.g., Program Verification, Semantics of Programming or Specification Languages). He is interested in both, theoretical/foundational and applied research and innovation. His work experience in both industry and academia reflects his unique combination of applied and theoretical work. He is supporting security initiatives and events that build bridges industry, academia, and local communities. Amongst others, he is a member of the Steering Committees of the South West Cyber Security Cluster and BSides Exeter.

Online session with CYBERUS Alumni

Wednesday, April 9
13:30 to 14:30

Mashal ZAINAB

PhD Student, SerVal, Interdisciplinary Centre for Security, Reliability and Trust, Luxembourg

Biplab GAUTAM

Security Research Engineer, NEC Laboratories Europe, Heidelberg, Germany

Paweł BORSUKIEWICZ

PhD Student, TruX, Interdisciplinary Centre for Security, Reliability and Trust, Luxembourg

Ribiea RAMZAN

Security Engineer, Fujitsu, Luxembourg

Amarilda KOKA

Information Security Analyst @ SES Satellites, Luxembourg

Scientific Session

Thursday, April 10

09:30 to 10:30

Program Analysis: Challenges and Opportunities

Automated program analysis enables developers and researchers to systematically examine code to verify correctness, detect defects, identify security vulnerabilities, optimize performance, and ensure compliance with coding standards. Researchers have been devising many different types of program analysis techniques: (1) static analyses, where the code of a given software is scanned but not executed; (2) dynamic analyses, where a given software is executed and monitored to observe its behavior at runtime; (3) hybrid techniques combining both static and dynamic analyses; and (4) AI-based techniques. However, all these approaches come with inherent and practical limitations. The considerable progress in machine learning in recent years, notably the emergence of Large Language Models (LLMs), has demonstrated impressive effectiveness in code-related tasks such as code completion, bug/vulnerability detection, program synthesis, and more. These successes pose the question: to what extent can LLMs replace traditional program analysis techniques? In this talk, I will present an overview of different program analysis techniques, discuss their respective strengths and limitations, and explore emerging trends.

Jordan SAMHI

Research Scientist | University of Luxembourg - SnT

Jordan Samhi is a Research Scientist working in Software Security and Software Engineering at the University of Luxembourg. His research is about automating software security with static code analysis. More particularly, he has a strong interest to improve the comprehensiveness of software analysis towards ensuring the security and reliability of software systems. Currently, he is focusing on Android systems

Scientific Session

Thursday, April 10

11:00 to 12:00

Mobile Security: years of improvement, yet challenges remain

Today, mobile devices are ubiquitous in daily life, used for various operations such as banking, communication via messaging and social media, storing health data, shopping, and more. As a result, they handle vast amounts of personal and confidential information, making them prime targets for attackers. This has been a persistent issue, as demonstrated by the continuous discovery of new mobile malware—even within official app stores like Google Play. A simple search for “Android malware” in the news highlights the scale of the problem. To address these security threats, researchers have developed various techniques for detecting and mitigating security issues in mobile software. In this talk, I will present an overview of existing security mechanisms and discuss approaches to combat mobile threats using techniques such as static and dynamic analysis, behavioral monitoring, and AI-driven detection methods. I will then discuss some of the remaining challenges in mobile security.

Jordan SAMHI

Research Scientist | University of Luxembourg - SnT

Jordan Samhi is a Research Scientist working in Software Security and Software Engineering at the University of Luxembourg. His research is about automating software security with static code analysis. More particularly, he has a strong interest to improve the comprehensiveness of software analysis towards ensuring the security and reliability of software systems. Currently, he is focusing on Android systems

SCIENTIFIC SESSION

FRIDAY, APRIL 11

09:30 TO 10:30

Cryptographic screaming-channel attacks

This talk discusses cryptographic side-channel attacks, i.e., the recovery of a secret cryptographic key by analyzing physical leakage (e.g., electromagnetic emanation) produced by a victim electronic device, such as a processor. The presentation will focus on a particular case of side-channel attacks, called the screaming-channel attack. This attack is made possible by mixed-signal devices, like IoTs, which integrate an RF module on the same die as the processor. In such a scenario, side channels can be unintentionally modulated, amplified and transmitted by the RF module, making a side-channel attack possible at a distance of several meters.

Jeremy GUILLAUME

Postdoctoral Researcher | Lab-STICC, UBS, Lorient

Jeremy Guillaume is a postdoctoral researcher at Université Bretagne Sud (UBS), working with Dr. Vianney Lapotre and Prof. Guy Gogniat at the Lab-STICC laboratory in the ARCAD team.After his thesis on screaming-channel attacks, his research focuses on micro-architectural attacks, in particular on the development of countermeasures.

SCIENTIFIC SESSION

FRIDAY, APRIL 11

10 TO 10:30

Wireless Security for the Internet of Things : Threats and Intrusion Detection System

The rapid expansion of Internet of Things (IoT) applications has led to a significant increase in the number of connected devices and the deployment of diverse IoT protocols. While these advancements enhance connectivity, they also expose devices to security threats, particularly wireless attacks that exploit vulnerabilities in communication units. In this talk, we begin with an overview of common attack vectors and vulnerabilities in wireless communications, focusing on LoRa/LoRaWAN, BLE, and IEEE 802.15.4 protocols. We then introduce a Host Intrusion Detection System (HIDS) specifically designed to mitigate wireless attacks on IoT end-devices. This HIDS utilizes a hardware-assisted approach, employing hardware performance counters (HPCs) to monitor both microarchitectural and network metrics on a 32-bit RISC-V-based wireless connectivity unit. Experimental evaluation demonstrates its effectiveness in detecting packet injection and jamming attacks. The FPGA implementation incurs a logic overhead of approximately 14.30%, with less than a 1% impact on design frequency and code size for the RISC-V processor.

Mohamed EL BOUAZZATI

Postdoctoral Researcher | Lab-STICC, UBS, Lorient

Mohamed EL Bouazzati is a postdoctoral researcher in the ARCAD team at Lab-STICC, Lorient, France. He earned an engineering degree in embedded systems and wireless communications from ENSEM, Casablanca, Morocco. He then joined an international exchange program in electronic systems for biomedical engineering (ESYBIO) at ENSEIRB-MATMECA, Bordeaux, France, and completed an MSc degree at the University of Bordeaux in 2020. Furthermore, he received his PhD from the University of Southern Brittany in December 2023. In 2022, he took part in a research exchange at the University of Massachusetts, Amherst, USA. His research focuses on Wireless attacks detection in IoT, FPGA-based hardware intrusion detection systems (IDS), radio frequency fingerprinting for device identification, and IoT dataset collection from commercial off-the-shelf (COTS) devices for security applications.

Poster session

Friday, April 11

10:30 to 11:30

Etienne LEMONNIER | IRISA

Towards a Decentralized and Dynamic Approach of Data-Centric Security

Adam HENAULT | Lab-STICC

LiteInjector: A fault emulator framework for LiteX System on Chip

Hongwei ZHAO | Lab-STICC

Fault attack on the communication architecture of a RISC-V based system

Gwenn LE GONIDEC | Lab-STICC

Internal Power-Management-based Fault Attacks

Tianxu LI | Lab-STICC

Hardware-Based Intrusion Detection System for IoT Gateway Against Wireless Attacks

LOCAL ORGANIZING COMMITTEE

Prof. Guy GOGNIAT

CYBERUS Scientific and Academic coordinator

Prof. Jean PEETERS

CYBERUS Director

Dr Philippe TANGUY

Associate Professor, CTF Supervisor

Adam HENAULT

PhD Student, CTF Supervisor

Corinne NEVEU

Administrative Manager

Yanira GAVILÁN

Administrative Assistant