CYBERUS Summer School

1st edition | online

July 3 – 7, 2023

MONDAY, JULY 3: Opening Session

14:00 – 14:15 Jean PEETERS and Guy GOGNIAT

TEAMS link to follow the session here

Remote access is open to the public but please register beforehand by following this link

MONDAY, JULY 3: SESSION 1

Fault attacks and countermeasures

Moderator: Vianney LAPÔTRE, UBS

TEAMS link to follow the session here

14:15 – 15:00 DE PAUW Cédrick, ULB

How to evaluate your countermeasures against fault injections with Unicorn

Faults may be injected in a system either by an attacker or from a stressful environment. In both cases, the introduction of these faults may lead to a change in the control flow of a program, e.g. skipping a branching. Countermeasures against fault injections may be implemented, however testing them may require a certain expertise, expensive materials or a lot of time. This part will introduce Unicorn, a CPU emulator based on QEMU, and how it may be used to easily emulate fault injections for specific CPU architectures.

Cédrick De Pauw was awarded the Master's degree in Computer Science and Engineering from the Université Libre de Bruxelles (ULB) and he is completing a complementary Master's degree in Cybersecurity from the ULB.
He is a PhD student from the "Embedded Systems Design and Security" department, under the supervision of Professor Jean-Michel Dricot, at the ULB and his current research topic concerns physically unclonable functions (PUFs), related protocols and their application.software and physical attacks.

15:00 – 15:45 PENSEC William, UBS

Fault Injection Attacks Against an In-Core DIFT Mechanism

Internet of Things (IoT) devices manipulate sensitive data leading to strict security needs. They face both software and physical attacks due to their network connectivity and their proximity to attackers. These devices are usually built around low-cost and low-power processors. In this paper, we study the impact of Fault Injection Attacks (FIA) on the D-RI5CY processor integrating a Dynamic Information Flow Tracking (DIFT) mechanism against software threats. Our results highlight the high sensitivity of the target to multiple fault types at multiple spatial and temporal locations.

William PENSEC received his MSc in Computer Science with a specialisation in Software for Embedded Systems from Université de Bretagne Occidentale (UBO), in Brest, France in 2021. He joined the ARCAD team at the Lab-STICC laboratory in France starting his PhD in 2021 in Hardware Security at the Université Bretagne Sud in Lorient, France.
His area of research focuses on embedded system security, RISC-V core, Dynamic Information Flow Tracking, and fault injection attacks, in order to protect a RISC-V core against both software and physical attacks.

TUESDAY, JULY 4: SESSION 2

Wireless and software security

Moderator: Jacques KLEIN, UL

TEAMS link to follow the session here

14:00 – 15:00 EL-BOUAZZATI Mohamed and LI Tianxu, UBS

Wireless security and hardware assisted Intrusion Detection System

In this presentation we will first give an overview of attacks on wireless communications LoRa/LoRaWAN, BLE and IEEE 82.15.4. Secondly, we will detail a solution we are developing to detect attacks on an IoT node and a gateway.

Mohamed EL BOUAZZATI (PhD student, Lab-STICC) completed his engineering degree in embedded systems and telecommunications at ENSEM, Casablanca, Morocco. He then pursued an international exchange program in electronic systems for biomedical (ESYBIO) at ENSEIRB-MATMECA, Bordeaux, France. In 2020, he obtained an M.Sc. degree from the University of Bordeaux, France. Afterward, he joined the ARCAD team at the Lab-STICC in France and commenced his PhD studies at the University of Southern Brittany. During the summer of 2022, he was a guest researcher at the Reconfigurable Computing Group at the University of Massachusetts, Amherst, MA, USA.
His research interests include RISC-V ISA-based wireless connectivity processors, wireless attack detection in low data rate and low power Internet of Things (IoT), hardware performance monitoring for security issues, and the implementation of hardware intrusion detection systems (IDS).

Tianxu LI, PhD student in Lab-STICC. He received his licence diplome in Electronic Information at XIDIAN University, China in 2020. Then he came to Polytech Montpellier in France for future studies, pursuing an engineering degree in Microelectronics and Automation. He discovered his interest in research while working on a research engineer program, and an internship in medical embedded systems got him thinking about security. So he started to seek more knowledge on cyber security and conduct his doctoral research at University of Southern Brittany, in the ARCAD team of Lab-STICC.
Now his research focuses on the security of IoT gateways based on RISC-V processors and intrusion detection systems against wireless attacks.

15:00 – 16:00 REBATCHI Hocine, UL

Dependabot and Security pull requests: a large empirical study

Modern software development is a complex engineering process where developer code cohabits with an increasingly larger number of external open-source components. Even though these components facilitate sharing and reusing code along with other benefits related to maintenance and code quality, they are often the seeds of vulnerabilities in software supply chains leading to attacks with severe consequences. It is thus important to keep dependencies updated in a software development project. Unfortunately, several prior studies have highlighted that, to a large extent, developers struggle to keep track of dependency updates, and do not quickly incorporate security patches. Therefore, automated dependency-update bots have been proposed to mitigate the impact and the emergence of vulnerabilities in open-source projects.

In our study, we investigate the appropriateness and the limits of the current tools and security measures related to dependency updates and the management of security vulnerabilities in GitHub that lead to threatening the software supply chain. We also attempt to identify the factors and the features that motivate the adoption of such tools. In addition, our study aims to provide a better understanding of the practices used by developers and security experts with regards to mitigating the threat of security vulnerabilities, as well as discovering the dominance and lifetime of these vulnerabilities in dependencies. Our main discoveries show that bots have enabled an improvement in the monitoring of outdated dependencies, alleviating the difficulty of handling them manually. Yet, developers use different strategies to identify and fix vulnerabilities in dependencies. Besides, even though some tools enable quick reaction to vulnerable dependencies after their disclosure, threat remains unknown in GitHub for 512 days, and patches are disclosed after 362 days from 0-day, leading to a huge window of exposure, especially that vulnerabilities with serious severity levels are the most occurring.

Hocine REBATCHI is a PhD Candidate in the Department of Software and IT Engineering at École de Technologie Supérieure (ÉTS) in Montreal, Canada. He graduated from the National Computer Science Engineering School in Algeria in 2020 with a Double Degree (State Engineering Degree + Master's Degree) in Software Engineering. He is currently a PhD Candidate with Applied Research Profile at École de Technologie Supérieure (ÉTS) in Montreal, Canada with a collaboration with the SnT Group at the University of Luxembourg since January 2021. His research topic focuses on mining software updates to prevent Software Supply Chain Attacks (SSCAs), as well as the use of Deep Representation Learning to detect vulnerabilities that lead to SSCAs.
His field of research and interest: Software Engineering, Software Security, and Machine Learning..

WEDNESDAY, JULY 5: SESSION 3 ante

Embedded systems security

Moderator: Guy GOGNAT, UBS

Zoom link to follow the session here

Meeting ID: 923 7428 0442
Passcode: k9Qk8h

09:00 – 10:00 GUILLEY Sylvain, TELECOM-ParisTech

Embedded cyber-security: from requirements to technological solutions

Cyber-security has become ubiquitous, from IoT end points to datacenters. In such open and broad ecosystem, the protection of data is a major concern; Indeed, some business activities are at risk. In this regard, "certification" aims at controlling and reducing the extent of cyber-physical attacks. Fortunately, many technological solutions can be leveraged to mitigate all identified threats. In this talk, I'll show how the embedded cyber-security industry is working to map requirements into viable protection technologies, in order to reach the expected level of security.

Sylvain GUILLEY is co-founder and CTO at Secure-IC. Sylvain is also professor at TELECOM-ParisTech, associate research at Ecole Normale Supérieure (ENS), and adjunct professor at the Chinese Academy of Sciences (CAS). His research interests are trusted computing, cyber-physical security, secure prototyping in FPGA and ASIC, and formal / mathematical methods.
He has co-authored 300+ research papers and filed 40+ invention patents. He is member of the IACR, and senior member of the IEEE and the CryptArchi club. He is an alumnus from Ecole Polytechnique and TELECOM-Paris.

WEDNESDAY, JULY 5: SESSION 3

Deep learning for software repair and systems of systems security

Moderator: Philippe TANGUY, UBS

TEAMS link to follow the session here

14:00 – 14:45 KABORÉ Abdoul Kader, UL

Learning to Automatically Repair Vulnerable Programs

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 output 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.

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.

14:45 – 15:30 SADOU Salah, UBS

Security of systems of systems

Modern society is critically dependent on a wide range of systems, and in particular Systems of Systems (SoS). SoS are made from a collaboration of existing systems. As any system, they are developed to meet their functional requirements while ensuring correctness as well as safety, reliability, and performance, among other -ilities, it is equally fundamental to ensure their security.

However, traditionally, security has only been considered after the design and more often the implementation and even the deployment of software-reliant systems, meaning that security is fitted into pre-existing designs or code or executable. In practice, a fit-all solution is habitually assumed where security mechanisms are inserted into the system with very little consideration of the implications of inserting such mechanisms into the existing system design. As a result, security may conflict with the system requirements and this can raise problems, which most of the times translate into security vulnerabilities.

In this presentation, I will define SoS and describe the raised challenges in security perspective. By the way, I will present some of our team's work on these challenges.

Pr. Salah Sadou is a full professor in Computer Science. He leads the interdisciplinary research of the Cybersecurity Center of UBS and the Trustworthy computing department of ENSIBS engineering school. He obtained a PhD degree in 1992 at Ecole Centrale de Lyon, France. He has about 30 years of experience in research and education in software engineering science. His past research interests were centered on languages, processes and tools for designing and engineering systems where the evolution acts as a first class entity. He was also involved in research concerning architectural description language with non-functional properties as first class entities, software restructuring (from object-oriented to component-oriented), component-based description languages and software quality. He directed 12 PhD students (mean time to completion 3 years and 3 months) and currently supervising 5 PhD students most of them related to Cybersecurity domain. He published more than 70 academic publications, mainly ranked A in international ranking (eg. Australian CORE). His current research interest focus mainly on secure by design approach for System of Systems and Socio-technical System construction.

THURSDAY, JULY 6: SESSION 4

Post-quantum cryptography and statistics for big data

Moderator: Olivier MARKOWITCH, ULB

TEAMS link to follow the session here

14:00 – 14:45 GILCHRIST Valerie, ULB

The state of post-quantum cryptography

Post-quantum cryptography has been an increasingly popular research topic due to the looming threat of quantum computers. In this talk we will review what post-quantum cryptography is and its current main branches. We will assess the main contenders for standardization, and what a post-quantum world might look like.

Valerie GILCHRIST is a PhD student at ULB studying post-quantum cryptography, with particular emphasis on a branch called "isogeny-based cryptography". Her research includes both cryptanalysis and algorithmic improvements of these cryptosystems.

14:45 – 15:30 DURRIEU Gilles, UBS

Nonparametric statistics for Big Data

This talk is devoted to the estimation of the derivative of the regression function in fixed and random design nonparametric regression. We establish the almost sure convergence as well as the asymptotic normality of our estimates. We provide concentration inequalities. We also illustrate our nonparametric estimation procedure on simulated data and high-frequency real data.

Since 2010, Gilles Durrieu is professor at the University Bretagne Sud where, since 2021, he holds an 'exceptional professorial rank'. Additionally, he was professor at the University of New Caledonia in Oceania from 2017 to 2019 and associate professor at the University of Bordeaux before 2010. Gilles Durrieu's work includes nonparametric statistical modeling, sequential and robust statistics, extreme value theory, machine learning and computational statistics and studying the asymptotic properties of statistical models. Gilles Durrieu is working mostly on applications of its mathematical learning developments in ecology, genomics, and cybersecurity.

FRIDAY, JULY 7: SESSION 5

New technologies and attacks on microcontrollers

Moderator: Guy GOGNIAT, UBS

TEAMS link to follow the session here

14:00 – 14:45 MILOJEVIC Dragomir, ULB

Advanced CMOS & 3D packaging technologies for future integrated circuits and systems

New transistor architectures and scaling boosters will enable CMOS technology to reach & go beyond 1nm node. Despite further enablement of scaling, 2D system integration faces limitations due to memory wall (bandwidth, energy per transferred bit, capacity, etc.), cost-effective integration of big dies (many-core SoCs), poor scaling of SRAM technology (inefficient memory hierarchy) to name a few. To overcome these limitations, 3D system integration has been proposed with various technology options to allow different die-to-die interconnect schemes. In this talk we will investigate different 3D technologies options, their properties, system integration options and how they will shape future System-on-Chip design.

Dragomir MILOJEVIC received his master's and PhD degrees in Electrical Engineering from Ecole Polytechnique de Bruxelles (EPB), Université libre de Bruxelles (ULB), Belgium. Between 1999 and 2006 he worked at ULB as a teaching assistant in the field of digital logic circuits. In 2005 he joined IMEC where he first worked on multi-processor and Network-on-Chip architectures for low-power multimedia systems. Since 2008 he is working on design enablement and characterization of advanced CMOS technologies (<10nm) & 3D stacked integrated circuits. Today, part of INSITE & 3D integration programs at IMEC, he is working on system architecture and design technology co-optimization.
Since 2006, Dragomir MILOJEVIC holds the position of a professor at EPB, where he co-founded Parallel Architectures for Real-Time Systems (PARTS) multi-disciplinary research group.

14:45 – 15:30 GAUDIN Nicolas, UBS

Thwarting Timing Attacks in Microcontrollers using Fine-grained Hardware Protections

Timing side-channels are an identified threat for security critical software. Existing countermeasures have a cost either on the hardware requirements or execution time. We focus on low-cost microcontrollers that have a very low computational capacity. Although these processors do not feature out-of-order execution or speculation, they remain vulnerable to timing attacks exploiting the varying latencies of ALU operations or memory accesses. We propose to augment the RISC-V ISA with security primitives that have a guaranteed timing behavior. These primitives allow constant time ALU operations and memory accesses that do not alter the state of the cache. Our approach has a low overhead in terms of hardware cost, binary code size, and execution time both for the constant time secure program and other programs running concurrently on the same hardware.

Nicolas GAUDIN is a PhD student at Lab-STICC, Université de Bretagne Sud (UBS), France. He graduated in the field of embedded systems in engineering in Montpellier, France. His PhD thesis relates to hardware security of embedded systems. He focuses on protections against software attacks using timing side-channels. These considered timing leaks are presents on the micro-architecture and caches of RISC-V cores.

FRIDAY, JULY 7: Closing Session

15:30 – 15:45 Guy GOGNIAT

Contact: cyberus@listes.univ-ubs.fr