



POST MASTER DEGREE

IN SECURITY IN COMPUTER SYSTEMS AND COMMUNICATIONS

EXAMPLES OF STUDENT PROJECTS

Part of the curriculum of EURECOM Post Master's degree (Diplôme d'Ingénieur de Spécialisation) is made of supervised Projects based on real case studies. At the beginning of each semester, a list of topics is published and students need to choose one topic among this list.

Semester Projects are all based on real-case studies of industrial relevance. Industrial partners can be involved. They allowed students to gain hands-on training and gain new skills, by developing prototypes, working with cutting-edge and new technologies, testing vulnerabilities, assessing current safety solution and proposing new tools...

Students can work individually or in group of 2/3. The expected workload is 90 hours of individual work per semester. Regular meetings are organized with the supervisor (professor) and a Phd student to monitor and follow-up on the progress made the students. A defense is organized at the end of each semester.

Students can work on the same project topic throughout the 2 academic semesters or choose a different topic each semester.

Please find a few recent examples of project topics:

Infection risks of a Samsung gear fit watch Track

Wearables are currently among the most fashionable items. Their security though hasn't been studied much, yet. Thus, this project focuses on the risks of a smart watch with regards to malware infection. Can a smart watch be infected? Can a compromised watch infect another device? The student(s) will be supplied with a Samsung Gear Fit and, if needed, an Android device..

Security aspects of Amazon S3

"Big Data" is the nowadays' buzzword to describe the on-going revolution in IT that brings about increasing storage space and computing power for tremendous amounts of data. Many organizations deem crucial the analysis of this huge data to optimize their business operations. In this perspective, EURECOM is involved in the collaborative industrial project eBOB (e-Business Optimization with Big Data) that develops a new technology for Big Data analytics. In a first step, the students will explore Amazon S3 and learn how Amazon S3 works, how it stores data, etc. In a second step, the students will study, design and implement security functions for data protection in Amazon S3.

Studying and Testing a Security Technology for Intel Processors

Within most currently deployed cloud solutions, cloud administrators can spy at data being stored in the local memory of the computer node executing the process, or can corrupt the Operating System to access to these data. Intel's Software Guard Extensions (SGX) is the last breakthrough among the technologies providing cryptographic proofs of strong software memory isolation in presence of a powerful adversary that may have corrupted the operating system, hypervisor, and that can spy the external memory content. Your work is to choose an application that will run on an SGX platform (or an emulator) and study how it could be attacked from the OS or the hardware standpoint.

Secure Data Storage for autonomous system

This project deals with the development of security functionalities for protecting the storage of the information sensed during an autonomous system mission. You will first design a cryptographic protocol dedicated to protect data. This protocol should for instance support and protect the integrity of telemetry information. You will then design cryptographic mechanisms for protecting the mission-long storage of the data sensed during the mission despite potential physical attacks.

Explore low level bits in Intel Edison board

The goal of this project is to better understand intel Edison board. Edison is a module that contains a dual core atom processor (running linux) and a quark x86 micorcontroller (running a proprietary kernel). This platform is designed for IoT applications but unfortunately lacks a good documentation. The goal of the project is to: - get hands experience with this board, - understand the hardware and low level software better (secure boot, communications between the 2 processors, OS on the quark CPU). - find if a user can take ownership of the platform (or has to run code signed by someone else, which has to be trusted)

Automated Forensic Analysis

The goal of this project is to automate part of the forensics analysis. In particular, the student will develop a framework to group existing computer forensics tools (like volatility, log2timeline, ...) and external data sources and perform an analysis of their results in order to find suspicious events. By correlating and aggregating different information, the tool should be able to provide a better picture of what happened in the target system and to automatically detect both consistent and inconsistent scenarios.

Verifiable Keyword Search

As an increasingly number of databases and applications are moved to cloud computing platforms, ensuring that cloud servers process clients' outsourced data and operations as expected is a challenging issue that still makes companies reluctant to adopt cloud technologies. EURECOM is involved in a European Research project named TREDISEC and its work within this project focuses on the design of new verifiability solutions for cloud storage and processing. Our security research group proposes some novel verifiable computations solutions for some dedicated operations such as word search or polynomial evaluation. The aim of this project is to design, implement and benchmark the proposed mechanisms. This semester project will be tightly coupled with EURECOM's latest research on Cloud Computing Security, involving various industrial partners..

Privacy for Big Data

EURECOM is involved in a European Research project named User-Centric-Networking (UCN) which aims at leveraging massive user information in order to deliver dedicated content recommendation. Since such information is considered as being highly sensitive. as part of this project, EURECOM is designing new privacy preserving primitives in order to give back some control to the users. In order to demonstrate the feasibility of these primitives EURECOM is also developing a proof-of-concept implementation. The aim of this project is to investigate specific cryptographic building blocks to optimize the performance of the proposed primitive; implement an optimized version of the proposed primitive.

Baseband attacks

The goal of this project is to perform some attacks on a smartphone baseband. The student will be integrated in a larger project and a well-defined task will be given to him. This could include for example static analysis of some embedded system kernel or to some functionality of the baseband. Note: low level software skills (ARM asm) needed or to be acquired. Requires some personal involvement, a lot of help will be provided to students motivated to learn. Access to required hardware will be provided.

Creating a multichannel ieee 802.15.4 sniffer Track

IEEE 802.15.4 (zigbee physical layer) is the 802.11/wifi for small embedded systems. It's used in many diverse systems such as smart light bulbs, fireworks remote controllers, or building automation. There are several tools for sniffing IEEE 802.15.4, but most rely on one single receiver, which hops on channels for detection of communications. Some are based on software defined radios but have low sensitivity and are a lot more cpu intensive. The goal of this project is to design a receiver from discrete components Requirements (or skills that will be acquired) : - PCB design, Radio Frequencies basics, hands on electronics skills. Notes: - a lot of help will be provided to students motivated to learn and build stuff. All required hardware will be purchased/lent. - this project has potential for being published/open sourced