UNIVERSITÀ DI PISA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Dottorato di Ricerca in Ingegneria dell'Informazione

Doctoral Course

"Principles of Cybersecurity and the Role of Hardware in Security"

Luca Crocetti, Ph.D.

Department of Information Engineering, University of Pisa – Italy

E-mail address: luca.crocetti@unipi.it

Short Abstract:

In the last decades, cybersecurity has emerged as a critical and pressing concern. With the proliferation of technology and the interconnectedness of our world, the protection of computer systems, networks, and data has become a fundamental aspect that may impact everyday life and the safety of people. Indeed, security attacks can threaten the most variegates fields and applications, and, if not properly counteracted, the consequences can be severe, causing injuries or even death. One of the most immediate and straightforward examples can be a hacker that takes the remote control over brake and/or steering system of a vehicle, or an attacker that manipulates the information about the state of charge of a battery causing its explosion.

This course aims to give the basic principles of cybersecurity, providing knowledge on the main security threats common to almost all application contexts and the main techniques to counteract them. All the fundamental aspects concerning the implementation of security modules (both hardware and software) are presented, including the references and the validation methodologies to evaluate the security properties according to the desired level of security. Finally, a focus on the importance of cybersecurity in some application fields and some examples on the future trends of security applications are provided. In addition, some highlights on the role of hardware in security are given.

During the lectures some exercitations will be held to get more familiarity with the illustrated concepts and to make some practical experiments.

After the participation to this course, the attendee will have a basic but comprehensive knowledge of which are the main security threats and the main techniques to counteract or mitigate them. The matured knowledge will constitute a useful instrument that can be used to evaluate also other aspects of its research activities and improve them by integrating security mechanisms or developing solutions that are more suitable for later integration of security mechanisms.

Course Contents in brief:

1. Principles of Cybersecurity. [7.5 hours]
    - Overview of the security threats and attacks.
    - Overview of the fundamental security services to protect data and assets.
    - Overview of cryptographic primitives and algorithms to implement security services.
    - Ad-hoc solutions to implement security services without cryptography.
    - Exercitation(s).
2. Basic guidelines for the development of HW/SW security modules: security services, interface security policies and physical implementation. [4 hours]
    - Concept of security strength, long-term security protection and introduction to Post-Quantum Cryptography (PQC).
    - Focus on verification/validation systems for the developed modules.
    - Focus on interface security policies.
    - Focus on physical implementation: Side-Channel Attacks (SCAs) – Principles and examples.
    - Exercitation(s).
3. On the importance of cybersecurity in automotive, space, Battery Management Systems (BMSs), and server applications. [1.5 hours]
    - Examples of attacks and consequences.
    - Future trends: assets encryption in general-purpose processors for servers and battery passport.
4. The Role of Hardware in Security. [2 hours]
    - Focus on the concepts of Hardware Secure Module (HSM), Root-of-Trust and Chain-of-Trust.
    - Physically Unclonable Functions (PUFs).
    - Focus on Secure Boot routines.

Final Exam (multiple choice questions). [1 hour]

Total # of hours of lecture: 16 (15 + 1 for final exam)

References:

* The lectures will be held via projection of slide, and the course' slides will be available via e-mail or a team dedicated to the course on the Microsoft Team platform.

CV of the Teacher

Luca Crocetti is currently an Assistant Professor at the Department of Information Engineering of the University of Pisa. Since its Master's Degree in Electronic Engineering at the University of Pisa (May 2015), its research activities focused on the development of digital modules, hardware modules, and embedded systems for cybersecurity services in different applications (automotive, low-power, High-Performance Computing, Datacenter and, lately, Battery Management Systems), working with several companies such as Intel, Magneti Marelli, and Renesas. He received the Ph.D. degree (cum laude) in Information Engineering from the University of Pisa in June 2022, and he participated in the first 3-year phase of the *European Processor Initiative* (*EPI*) project, contributing

to the development of a cryptographic co-processor for High-Performance Computing applications for the first generation of EPI chips. Actually, he is concentrating his research activities on the development of security modules and services for Battery Management Systems to protect lithium-ion batteries from security threats such as counterfeiting, Denial-of-Service, and others.

During his academic career, Luca Crocetti also participated in the project *CyberChallenge.it* as an instructor of the module '*Hardware Security*' in the years 2020, 2021, 2022, and 2023. His teaching activity covers the topics of basic analog and digital electronics for the Bachelor's Degree Programme in Electronic Engineering and the development of hardware security modules in Hardware Description Language (HDL) for the Master's Degree Programme in Cybersecurity.

Luca Crocetti co-authored 15 papers in international journal and conference, and he holds 1 patent.

Final Exam: Multiple choice test (11 questions) via Google Forms or Microsoft Forms application integrated in the team dedicated to the course on the Microsoft Teams platform. The test will take place in presence, during the last hour of the course schedule.

Room and Schedule

Room: *Aula Riunioni del Dipartimento di Ingegneria dell'Informazione, Via G. Caruso 16, Pisa – Ground Floor*

Schedule:

26/02/2024 – 9:30 /13:00, Lecture #1 – first part (2.5 h) + Exercitation (1 h)

27/02/2024 – 9:30 /13:00, Lecture #1 – second part (2.5 h) + Exercitation (1 h)

28/02/2024 – 9:30 /13:00, Lecture #2 (2.5 h) + Exercitation (1 h)

29/02/2024 – 9:30 /13:00, Lecture #3 (1.5 h) + Lecture # 4 – first part (1 h) + Exercitation (1 h)

1/03/2024 – 15:00 /17:00, Lecture #4 – second part (1 h) + Final Exam (1 h)