Ph.D. in Information Technology
Thesis Defense

July 16th, 2026
at 3:00 pm
Room Schiavoni – building 20A

Alessandro BERTANI – XXXVIII Cycle

Novel Methodologies for the Security Analysis of Firmware and Hardware Components

Supervisor: Prof. Stefano Zanero

Abstract:

The security of firmware and hardware components has become increasingly important in recent years, due to the widespread distribution of embedded devices and specialized processors. Weaknesses in these layers can undermine the entire system's security and enable sophisticated attacks.
However, their analysis remains challenging due to the diversity of architectures, limited observability, and the lack of mature tools.
This thesis addresses these challenges by proposing novel techniques for the systematic, automated security analysis of both firmware and hardware components, following the lifecycle of a device: from verifying the correctness of a design, through analyzing the firmware that runs on it, to attacking the protection mechanisms it exposes once deployed.
At the design stage, we show how to systematically analyze processor designs to identify bugs and underspecifications, reducing the manual effort that dominates hardware verification.
At the firmware level, we present static and dynamic analysis techniques applied to firmware images, including a methodology for recovering structural information (the target instruction-set architecture and the boundaries between code and data regions) from raw images, and a concolic-execution-based approach to improve the accuracy of peripheral modeling during firmware re-hosting.
Finally, we demonstrate how hardware debug interfaces and hardware-based control-flow protections can expose residual attack surfaces that undermine the isolation and control-flow integrity guarantees on which the platform relies.
These contributions advance the state of the art in hardware and firmware security analysis, providing tools and methodologies for the security assessment of low-level components.

PhD Committee

Prof. Davide Zoni, Politecnico di Milano

Prof. Davide Balzarotti, Eurecom

Prof. Marius Muench, University of Birmingham