



UNIVERSITÀ  
DI PAVIA

**Ph.D. Program in Electronics, Computer Science and Electrical Engineering**

## **SEMINAR**

# **Information Hiding: Attack Models and Defense Challenges**

***Luca Caviglione***

**IMATI – CNR, Genova**

**December 11, 2025 - h. 14:30**

**Classroom A1, A Floor**

**Department of Electrical, Computer and Biomedical Engineering**

**Abstract:** The increasing complexity of networks and computing platforms magnifies opportunities for concealing arbitrary data. An established offensive trend takes advantage of *information hiding* techniques, which aims at making the detection of attacks harder. Among the various mechanisms, two major offensive paradigms are becoming popular. The first takes advantage of *covert channels*, i.e., abusive communication paths hidden within legitimate network traffic or software components. Covert channels demonstrated their effectiveness to exfiltrate sensitive information, avoid detection, retrieve malicious payloads, or bypass execution enclaves. The second exploits *steganography* for cloaking a payload within a digital object, primarily a multimedia artifact. Alas, mitigation of malware endowed with information hiding capabilities is a poorly generalizable process since it strictly depends on the deployed cloaking technique. Moreover, even a successful eradication of the malicious content may lead to additional pitfalls, which require to partially rethink countermeasures. This talk presents the main attack scenarios and countermeasures characterizing the most recent examples of *steganographic malware*.

**Bio:** Luca Caviglione (male) is a Research Director at the Institute for Applied Mathematics and Information Technologies of the National Research Council of Italy (CNR). He holds a Ph.D. in Electronic and Computer Engineering from the University of Genoa, Italy. His research interests include optimization of large-scale computing frameworks, network security, and analysis of threats targeting the software supply chain. Currently, he is the principal investigator for CNR within Project PERUN - Protecting Sensitive Cyber Ecosystems from Upcoming Next Generation and AI-generated Malware Threats (Grant N. 101225653) funded by the Horizon Europe Program. He is also a contract professor for the course "Foundations of Cybersecurity" at the University of Pavia and a board member for the PhD program in Security, Risk and Vulnerability of the University of Genoa (Cybersecurity and Reliable AI).

**Organizer**

**Prof. L. Massari**

**Ph.D. Coordinator**

**Prof. Ilaria Cristiani**