Ph.D. in Information Technology
Thesis Defense

March 14th, 2025
At 11:00 a.m.
Aula BIO 1 – Building 21

Fabio PALMESE – XXXVII Cycle

FORENSIC-AWARE SOLUTIONS FOR THE INTERNET OF THINGS IN THE HOME GATEWAY
Supervisor: Prof. Alessandro Enrico Cesare Redondi

Abstract:

The widespread integration of Internet of Things (IoT) devices is transforming modern households by automating tasks like lighting, security, and communication. However, this convenience introduces significant privacy and security challenges. IoT devices also hold potential as valuable sources of digital evidence, giving rise to IoT forensics, a field dedicated to identifying, acquiring, and analyzing data from these devices to aid investigations.

However, the limited hardware capacity typical of IoT devices complicates the application of traditional digital forensic techniques, as data may be lost, overwritten, or stored in complex cloud environments. Given these challenges, IoT forensics increasingly focuses on the network layer to extract meaningful data from traffic patterns derived by the communication of such devices. Many limitations are encountered due to the transient nature of network traffic, requiring a proper collection and analysis pipeline as the traffic is encrypted. This work fills the gaps in IoT network forensics introducing Feature-Sniffer, a framework that leverages Wi-Fi access points to gather and analyze IoT traffic, providing real-time communication insights that can serve as forensic evidence. Through statistical features derived from packet headers, even encrypted data can reveal useful contextual information about devices and users. We evaluate Feature-Sniffer on consumer-grade Wi-Fi access points, proving effective in environments with numerous IoT devices. Application use cases, such as device identification and human activity recognition via machine learning, showcase its versatility in revealing insights for forensic investigations. To extend potential sources of evidence, we integrate Wi-Fi Channel State Information (CSI) collection and analysis for human sensing, revealing presence or movement within indoor spaces only relying on physical propagation of the signal from IoT devices.

To handle high data volumes and resource constraints of consumer access points, we propose an adaptive resource allocation model for efficient feature collection, balancing forensic needs with CPU and storage limits. Additionally, a blockchain-based solution ensures data immutability for evidence preservation.

We conclude the work with a focus on the user privacy issue in home environments by proposing a machine-learning module that can detect and block non-essential destinations by only referring to network traffic characteristics.

This work lays a foundation for IoT forensics by addressing key challenges in evidence collection, preservation, and analysis, advancing toward an intelligent forensic-ready IoT gateway for smart homes.

PhD Committee

Prof. Matteo Cesana, **Politecnico di Milano**

Prof. Francesco Gringoli, **Università degli Studi di Brescia**

Prof. Martino Trevisan, **Università di Trieste**