UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

itee PhD
information technology
electrical engineering

DIETI. UNINA

Carmine Cesarano

Security Assessment and Hardening of Open Source and Off-The-Shelf Software

Tutor: prof. Roberto Natella

Cycle: XXXVIII Year: Second

itee PhD
information technology
electrical engineering

My background

- MSc degree in **Computer Engineering** (June 2022)
  - Thesis: “Assessing Isolation Properties in Partitioning Hypervisors”
- **Research group**: Dependable and Secure Software Engineering and Real-Time Systems (DESSERT – www.dessert.unina.it)
- **PhD start date**: 1st November 2022
- **Scholarship type**: UNINA

Summary of study activities

Ad hoc PhD courses / schools:

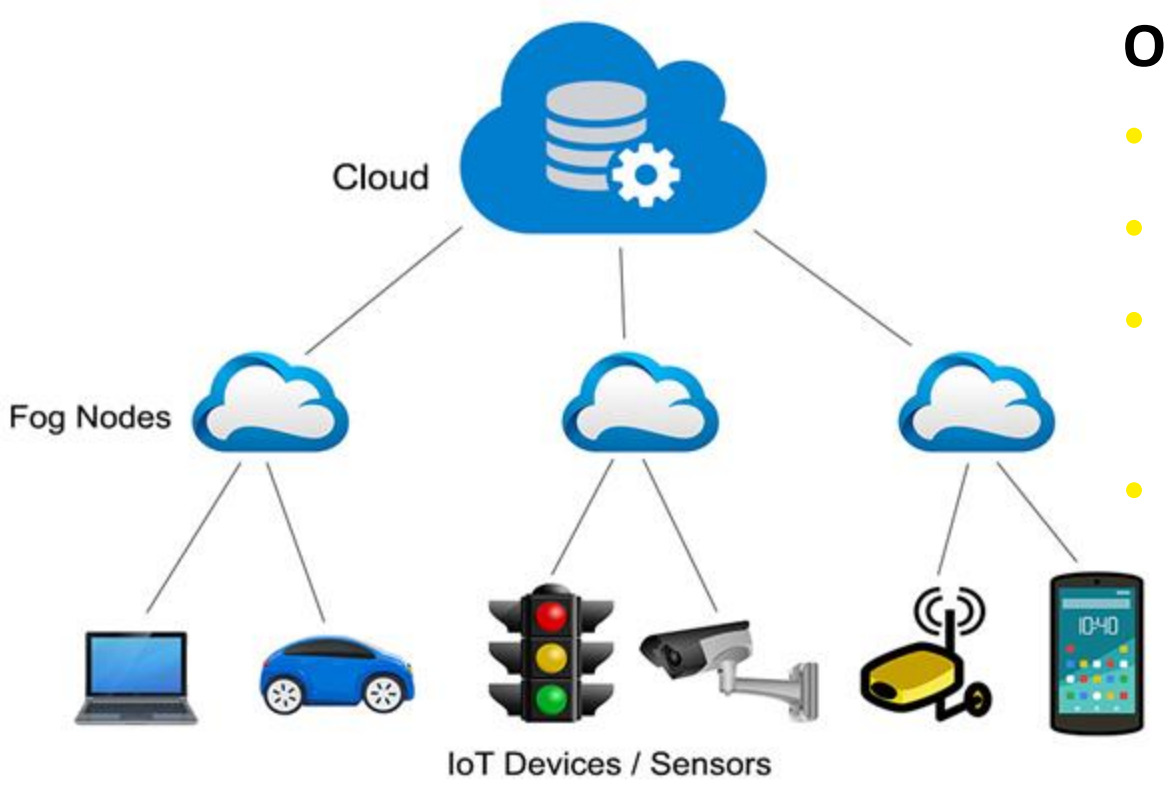
- Percorso per il rafforzamento delle competenze sulla progettazione europea
- Strategic Orientation for STEM Research & Writing
- Using Deep Learning Properly

Conferences / events attended

- 19th European Dependable Computing Conference (EDCC2024)
- ACM Conference on Computer and Communications Security (CCS2024)

Research field of interest

My research field concerns the security assessment and hardening of software stack employed in Fog Computing Systems



OSS, OTS software:

- Middleware
- Operating Systems
- Virtualization Platforms
- IoT Frameworks

Research activity: Overview

My research activity was focused on addressing the main problems related to:

Security Assessment

- Off-The-Shelf software
- Open-Source software

Security Enforcement

- Open-Source software

Security Assessment of OTS software

Problem: Lack of a systematic methodology for assessing Off-The-Shelf (OTS) components before integration into industrial products.

Solution: developed a security assessment methodology involving

- Collecting vulnerabilities (CVEs)
- Identifying families of weaknesses (CWEs)
- Designing attack scenarios based on CVE exploits
- Simulating attacks in a virtual environment

Case Study: industrial Application Layer Gateway

Security Assessment of OSS software

Problem: Lack of a comprehensive taxonomy for malicious code hiding in open-source packages.

Solution:

- Developed novel taxonomy of attack vectors for hiding the execution of malicious code in Go dependencies.

- Developed a static analysis tool that uses AST analysis to detect these vectors in source code.

Security Enforcement of OSS software

Problem: Existing sandboxing tools have limited capabilities for securely executing untrusted open-source packages.

Solution: Developed a dependency-aware sandboxing technique, for Go programming language:

1. Automatic capabilities allowlist configuration for third-party untrusted packages.

2. Runtime enforcement of denied capabilities through eBPF.

Products

[P1]	Cesarano, C.; Natella, R. Securing an Application Layer Gateway: An Industrial Case Study 19th European Dependable Computing Conference (EDCC2024) **Accepted**
[P2]	Cesarano, C.; Andersson, V., Natella, R., Monperrus, M. GoSurf: Identifying Software Supply Chain Attack Vectors in Go ACM Workhop on Software Supply Chain Offensive Research and Ecosystem Defenese (SCORED24) **Accepted**
[P3]	Cesarano, C.; Foggia, A.; Roscigno, G.; Andreani, L.; Natella, R. GENIO: Synergizing Edge Computing with Optical Network Infrastructures IEE Communication Magazine (COMMAG-IEEE) **Submitted**

Thank you for your attention