**PhD in Information Technology and Electrical Engineering**
**Università degli Studi di Napoli Federico II**

# PhD Student: Giorgio Farina

**Cycle: XXXVII**

## Training and Research Activities Report

**Academic year: 2022-2023 - PhD Year: Second**

**Tutor: prof. Marcello Cinque**

**Co-Tutor:**

**Date: October 23, 2023**

# Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

**Cycle:** XXXVII
**Author: Giorgio Farina**

## 1. Information:

- **PhD student: Giorgio Farina**
- **DR number: DR995861**
- **Date of birth: 03/05/1996**
- **Master Science degree: Computer engineering**
- **University: Università degli studi di Napoli, Federico II**
- **PhD Cycle: XXXVII**
- **Scholarship type: CINI**
- **Tutor: Marcello Cinque**
- **Co-tutor: N/A**

## 2. Study and training activities:

| Activity | Type[1] | Hours | Credits | Dates | Organizer | Certificate[2] |
|---|---|---|---|---|---|---|
| IoT Data Analysis | Course | 12 | 4 | 03/02/2023 | Dr. Raffaele della Corte | Y |
| Verification and Validation of Automated Systems' Safety and Security | Doctoral School | 18 | 6 | 18/07/2023 | VALU3S | Y |
| Threat Hunting & Incident Response | Seminar | 2 | 0.4 | 13/12/2022 | Prof. S.P. Romano, R. Natella | **N** |
| Cybercrime and Information Warfare: National and International Actors | Seminar | 2 | 0.4 | 18/11/2022 | Prof. S.P. Romano, | **N** |
| Ricerca e formazione nella società della transizione digitale | Seminar | 5 | 1 | 22/9/2023 | Prof. Stefano Russo | **N** |

1) Courses, Seminar, Doctoral School, Research, Tutorship
2) Choose: Y or N

### 2.1. Study and training activities - credits earned

| | Courses | Seminars | Research | Tutorship | Total |
|---|---|---|---|---|---|
| Bimonth 1 | | **0.8** | **9** | | **6.8** |
| Bimonth 2 | **4** | | **8** | | **12** |
| Bimonth 3 | | | **8** | | **8** |
| Bimonth 4 | | | **8** | | **8** |
| Bimonth 5 | **6** | | **6** | | **12** |
| Bimonth 6 | | **1** | **6** | | **7** |
| **Total** | **12** | **1.8** | **42** | | **53.8** |

| | | | | | |
|---|---|---|---|---|---|
| **Expected** | **30 - 70** | **10 - 30** | **80 - 140** | **0 – 4.8** | |

## 3. Research activity:

My research activity regards methods and tools for test automation and failure prevention in Mixed Criticality Systems.

In our container-everywhere vision [3], we imagine to spread the flexibility of containers in terms of simplified management and deployment, and quick reconfiguration, in all the stack of Industrial Internet of Things (IIoT), from cloud servers to things and edge devices, enabling unprecedented use cases. For instance, a containerized controller for a robotic arm might be deployed on the computing resources of the arm itself, if enough are available. Over time, the container could be migrated to an edge server and transmit wireless commands if needed, e.g., the controller becomes too complex to run on local resources. To enable this paradigm, we need new guarantees on the edge nodes, as they are going to host heterogenous applications (i.e., Mixed Criticality System), from real-time to general-purpose applications.

In continuous with the first year of PhD, I focused on preventing failures of real-time applications in edge servers.

In real-time systems, the correctness of a computation depends not only on the logical correctness of the result but also on the time at which the result is produced. Hence, a real-time application fails if has a deadline miss. Edge servers run on top of multi-core platforms, in which delays in task execution can occur due to shared resource interference, e.g., memory bandwidth, among co-executing applications. How to partition memory bandwidth without compromise the average performance is still an open research challenge. Detecting an error state can prevent a situation of interference from escalating into a system failure, i.e., a deadline miss. The mitigation is the action taken to avoid such escalation.

In [1], to enable the co-execution of critical and non-critical applications on the same multicore processor, we propose a “detection and regulation approach” that guarantees memory access time isolation for critical cores, while not jeopardizing the memory bandwidth of the non-critical ones. We identify the queue occupancy as an excellent observable metric to estimate the number of interfering cores co-accessing the memory, i.e., the error state, and, to mitigate the error, we regulate the memory accesses by using the indirect memory bandwidth limitation achievable by applying Intel’s Memory Bandwidth Allocation technology.

However, the correctness of a task can be compromised also from problems of isolation in terms of security among applications running on the same edge node. For this reason, in the second year of PhD, I focused more on providing tools to test problems of security isolation.

Hardware virtualization is an effective mean to build isolated environments. However, even if hardware virtualization is supported by several hardware extensions (i.e., Intel VT-x, AMD-V or ARM-VHE), software intervention by a hypervisor (i.e., the Virtual Machine Monitor VMM) is still possible for several reasons, such as missing hardware features, device emulation, resource usage optimization, or VM introspection. Since hypervisor intervention involves a change in a most privileged mode, hypervisor security can jeopardize the isolation of the hosted virtual machines CVE-2010-0435, CVE-2011-1936, CVE-2020-2732. Uncovering such isolation issues is still an open challenge, as it asks a not negligible manual effort to build the test cases. In [2], we propose IRIS, a framework to automate the test case generation to test hypervisor intervention. The framework records (learn) hypervisor interventions during the real guest execution (e.g., OS boot) and replay them as-is, in a synthetized form, to reach valid and complex hypervisor states. Finally, the IRIS can use them as valid seed to be mutated for enabling fuzzing solutions.

**Cycle:** XXXVII
**Author: Giorgio Farina**

## 4. Research products:

1] "Enabling memory access isolation in real-time cloud systems using Intel's detection/regulation capabilities", Giorgio Farina, Gautam Gala, Marcello Cinque, Gerhard Fohler, Journal of Systems Architecture, JSA, published, 2023, indexed by Scopus

2] "IRIS: a Record and Replay Framework to Enable Hardware-assisted Virtualization Fuzzing", Carmine Cesarano, Marcello Cinque, Domenico Cotroneo, Luigi De Simone, Giorgio Farina, The 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN, published, 2023, indexed by Scopus

a. Winner of DSN grant

3] "Partitioned Containers: Towards Safe Clouds for Industrial Applications", Marco Barletta, Marcello Cinque, Luigi De Simone, Raffaele Della Corte, Giorgio Farina, Daniele Ottaviano, 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume, DSN-S, published, 2023, indexed by Scopus

## 5. Conferences and seminars attended

I attended "The 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN" as a presenter author

## 6. Periods abroad and/or in international research institutions

## 7. Tutorship

## 8. Plan for year three

In the first two years, my focus was mainly on edge nodes. Instead, in the last year, my focus moves to the security and safety of the things, i.e., IoT devices. The software in each such device will have vulnerabilities and their implications have been well studied so far.
However, the novel aspect is that due to the connected nature of multiple of these devices, newer threats arise.
For example, the phone gets some input device from a wearable (such as heart rate) and automatically configures the IoT devices in the physical space (such as, increasing the rate of fresh air being brought in to the room through HVAC control, or reducing the temperature of the room through control of a smart thermostat).
Now, if there is a vulnerability in any of the applications on the interacting devices, the impact of that may spread.
Our goal in this project is to detect such a spread, as close to the start as possible, and then to mount some mitigation action.
I plan to do this work in collaboration with the Purdue University, which I visit as research scholar in the first eight months of my third PhD year.