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

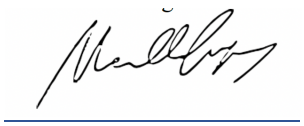
PhD Student: Giorgio Farina

Cycle: XXXVII

Training and Research Activities Report

Year: First

Tutor: prof. …



Co-Tutor:

Date: November 03, 2022

Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

Cycle: **Author:**

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**
- **Doctoral 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]
Real-Time Industrial Systems	Course	48	6	27/12/2021	Prof. Marcello Cinque	Y
Challenges towards Large-Scale Quantum Computers,	Seminar	1	0.2	01/12/2021	Prof. Giovanni Miano,	Y
Virtualization technologies and their applications	Course	20	5	04/03/2022	Dr. Luigi De Simone	Y
An Introduction to Deep Learning for Natural Language Processing	Seminar	1	0.2	3/04/2022	Prof. Francesco Cutugno	Y
Statistical data analysis for science and engineering research	Course	12	4	11/05/2022	Prof. Roberto Pietrantuono	Y
Software Security	Course	48	6	27/10/2022	Prof. Roberto Natella	Y
Explainable Natural Language Inference	Seminar	1	0.2	13/04/2022	Prof. Francesco Cutugno.	N
Using Delays For Control	Seminar	2	0.4	21/04/2022	Prof. Stefania Santini	Y

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	**6**	**0.2**	**3.8**		
Bimonth 2			**7**		
Bimonth 3	**5**	**0.8**	**6**		
Bimonth 4			**8**		
Bimonth 5			**6**		
Bimonth 6	**10**		**5**		
Total	**21**	**1.0**	**35.8**		
Expected	**30 - 70**	**10 - 30**	**80 - 140**	**0 – 4.8**	

3. Research activity:

My research activity is about Strategies for assessing fault and attack isolation in virtualized software systems.

Cloud is a computing paradigm aiming to provide reliable, customized, QoS-guaranteed dynamic computing environments for end-users.

Cloud providers offer (i) the setup of hardware resources to host general purpose Operating Systems (OSs) as Infrastructure as Service (IAAS), (ii) applications as Software as a Service (SAAS), or (iii) a common platform on which the users can execute their applications (PAAS). While most of the current cloud services operate on a best-effort basis and provide no timing guarantees, there is a growing interest in cloud applications for industrial and critical applications. However, a higher degree of determinism is desired for cloud technologies to be fully embraced by the industry. This calls for new techniques and methodologies to design predictable and reliable cloud applications.

Assuring a minimum memory bandwidth is paramount in building predictable cloud computing. During the first months of my PhD, I investigated the memory bandwidth guarantees of the modern Intel MBA hardware feature. However, our experiments prove that only some configurable parameters effectively limit the memory bandwidth of noisy neighbours. We mainly identify three issues in memory bandwidth partitioning: (i) the handling of asynchronous memory accesses, (ii) the need for last-level cache space partitioning, and (iii) the degradation of the average case. Hence, we propose the read pending queue occupancy to detect run-time interference and enable a detection and regulation algorithm to save the average case. In addition, we plan to build and design a new software solution that leverages hardware virtualization extensions to handle the last-level cache traffic transparently to the virtual machines. We believe this solution adds enough flexibility and predictability to current software-based solutions.

As memory bandwidth partitioning is essential in achieving predictability, assessing hardware-assisted virtualization is paramount for reliable cloud computing. During the first months of my PhD, I spent some time depicting the state of the art and the practice in assessing the security and the reliability of the hardware-assisted virtualization solutions.

The two aspects (reliability and security) are two sides of the same coin. They start by defining the requirements. Sometimes these requirements overlap. For example, both are interested in discovering faults in the hypervisor that lead to the crash/hang of the hypervisor and its virtual machines. However, security requires that the fault can be triggered by a virtual machine acting as an attacker. Once the requirements are defined, the standards require evidence that those requirements are not violated.
The process to generate such evidence at run time can be summarized in the following steps: (i) choose metrics that make it possible to detect a possible violation of the requirements, (ii) choose an efficient and effective method of exploration of the code. Once a good code exploration method has been identified, it can be reused later for new requirements.
My study identified a gap in recent (mostly security) methods of exploring hypervisor code. They do not include a method for recording and replaying nominal workloads in their solutions. In the case of virtualization, monitoring a nominal workload can have many benefits such as (i) learning hidden hypervisor state variables (ii) and effortlessly generating complex workloads that require a thorough understanding of the underlying hardware.
In the last months of my first year of PhD, I proposed and implemented an architectural solution that can enable the record and replay of nominal guest workloads. Enabling the record & replay of nominal guest workload requires defining which guest operations to monitor, as not all are useful workloads and a special architecture to reproduce the synthesized workload.

4. Research products:

"Assessing Intel's Memory Bandwidth Allocation for resource limitation in real-time systems,"
G. Farina, G. Gala, M. Cinque and G. Fohler,
IEEE 25th International Symposium On Real-Time Distributed Computing (ISORC 2022), Full Paper

"RunPHI: Enabling Mixed-criticality Containers via Partitioning Hypervisors in Industry 4.0"
M. Barletta, M. Cinque, L. De Simone, R. Della Corte, G. Farina, D. Ottaviano
33rd IEEE International Symposium on Software Reliability Engineering (ISSRE 2022), Fast Abstracts

"AID4TRAIN: Artificial Intelligence-Based Diagnostics for TRAins and INdustry 4.0.,"
Cinque, M., Della Corte, R., Farina, G., Rosiello, S.
EDCC 2022, Workshops.

"An unsupervised approach to discover filtering rules from diagnostic logs,"
Cinque, M., Della Corte, R., Farina, G., Rosiello, S.
33rd IEEE International Symposium on Software Reliability Engineering (ISSRE 2022), Industry Track

5. Conferences and seminars attended

"Assessing Intel's Memory Bandwidth Allocation for resource limitation in real-time systems,"
G. Farina, G. Gala, M. Cinque and G. Fohler,
IEEE 25th International Symposium On Real-Time Distributed Computing (ISORC 2022), Full Paper

6. Activity abroad:

7. Tutorship