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

PhD Student: Simona De Vivo

Cycle: XXXVII

Training and Research Activities Report

Academic year: 2022-23 – PhD Year: Second

Simona De Vivo

Tutor: prof. Domenico Cotroneo

Date: December 4, 2023

1. Information:

- **PhD student:** Simona De Vivo
- **PhD Cycle:** XXXVII
- **DR number:** 996112
- **Date of birth:** 22/07/1997
- **Master Science degree:** Master’s degree in Computer Engineering (cum laude)
- **University:** University of Naples Federico II
- **Scholarship type:** PhD student grant (Grant Type: MUR PON)
- **Tutor:** Prof. Domenico Cotroneo

2. Study and training activities:

Activity	Type[1]	Hours	Credits	Dates	Organizer	Certificate[2]
RTA – REAL TIME ANALYTICS MOD. C	Course	32	3	20-23-27/02, 02/03	CY4GATE ACADEMY, link: https://www.cy4gate.com/it/formazione/academy/	Y
RTA – REAL TIME ANALYTICS MOD. D	Course	40	3	20-23-30/03, 03/04	CY4GATE ACADEMY, link: https://www.cy4gate.com/it/formazione/academy/	Y
Multi-robot Control of Heterogeneous Herds	Seminar	1	0.2	16/02/23	Dr. Simone Mancini, Dr. Giacomo Ascione, Dr. Francesco Bajardi.	Y

Machine Learning and Security	Seminar	2	0.4	01/03/23	Sapienza Università di Roma	N
L'AI Generativa e il futuro della scrittura di codice	Seminar	1	0.2	04/04/23	CRIT S.r.l.	Y
How to Publish Under the CARE-CRUI Open Access Agreement with IEEE	Seminar	1.5	0.3	05/04/23	CARE-CRUI and IEEE	Y
Traffic Engineering with Segmented Routing: optimally addressing popular use cases	Seminar	1	0.2	23/06/23	Prof. Valerio Persico	Y
Comprehensive Exploration of Sparse Accumulator for SpGEMM	Seminar	1	0.2	25/08/23	Prof. Dong Dai, Ing. Hasanur Rashid (UNCC)	Y
Accelerating Serverless Computing via Intelligent Resource Harvesting	Seminar	1	0.2	08/09/23	Prof. Dong Dai (UNCC)	Y
Uncovering Bottleneck in HPC I/O Stack through Instrumenting Low-level System Stats	Seminar	1	0.2	20/10/23	Prof. Dong Dai (UNCC)	Y
Computational Design of Mechanically Flexible Organics	Seminar	1	0.2	03/11/23	Prof. Dong Dai (UNCC)	Y
DGAP: Efficient Dynamic Graph Analysis on Persistent Memory	Seminar	2	0.4	10/11/23	Prof. Dong Dai (UNCC)	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		0.6	5		5.6
Bimonth 2	3	0.6	10		13.6
Bimonth 3	3	0.5	6		9.5
Bimonth 4		0.2	6	0.5	6.7
Bimonth 5		0.2	6		6.2
Bimonth 6		0.4	6		6.4
Total	6	2.5	39	0.5	48
Expected	30 - 70	10 - 30	80 - 140	0 – 4.8	

3. Research activity:

Title: *Enhancing IoT Security and Efficiency Through Green AI Techniques*

The 5G mobile network has revolutionized the IoT landscape. Indeed, with multi-gigabit data speeds, lower latency, and network slicing, it supports diverse IoT services, leading to the number of internet-connected devices quickly increment. The growth of IoT devices poses two critical concerns: i) environmental impact and ii) attack surface enlargement.

Green Internet of Things (GIoT) – The Green IoT (GIoT) aims to reduce the environmental impact of IoT. It focuses on eco-friendly products, energy-efficient facilities, and decentralized processing at the network edge. Techniques like fog and edge computing minimize latency, improve bandwidth, and avoid unnecessary data transmission to the cloud. However, limited computational resources and power can affect security capabilities, making IoT devices susceptible to several security threats. Real-time monitoring and adaptive security measures are needed to safeguard IoT devices. Efficient computational resources and advanced solutions for data analysis are crucial to extracting value from the uninterrupted flow of data generated by connected objects.

AI Integration – AI algorithms are critical in managing the security threats and vast volume of data generated by IoT devices. They help detect faults, identify patterns, and enable predictive models. ML integration with IoT networks, particularly in edge computing, improves the filtering of relevant data, leading to energy-efficient decision-making. However, IoT current intrusion detection solutions based on AI inadequately consider the limitations of IoT devices' computing power and memory requirements.

To deal with the problems just highlighted, during the second year of my Ph.D., I delved into innovative topics within the realm of cybersecurity, focusing on the Internet of Things (IoT), Fog/Edge Computing, Intrusion Detection System (IDS), Security Information and Event Management (SIEM), and the Carbon Footprint of cybersecurity solutions. Particularly, I selected valid scientific papers from relevant conference proceedings held between 2016 and 2023. The outcomes of this research include a deep understanding of i) the vulnerability and risks of IoT devices, the most frequent attacks committed against IoT systems, and the commonly used datasets to support the intrusion detection analysis; ii) the most used AI-based solution for intrusion detection in IoT context, higher performance machine learning algorithms for intrusion detection, as well as their security and sustainability issues; iii) and

finally, Green AI solution for Intrusion Detection in IoT context (e.g., Lightweight IDS, Distributed Learning, and Federated Learning), the Federated Learning state-of-the-art and its relevance for sustainable intrusion detection practices combined with AI techniques.
The theoretical knowledge of this information was strengthened by hands-on sessions carried out at the DigitalPlatforms SpA ("DP") company, where I had the opportunity to practice with regular expression and correlation rules and where I did practical detection activity with the Real Time Analytics (RTA) SIEM, a cyber security monitoring and incident response solution, and LimaCharlie, a cybersecurity platform designed for endpoint detection and response (EDR) and threat hunting.
Currently, I spent four of the six months foreseen by my research project as a training period at DP company.

Thanks to the wealth of knowledge acquired, to face the state-of-the-art issues I carried out by the research study, I gave the following main research contributions: i) I implemented a lightweight Intrusion Detection System (IDS), analyzing it in terms of performance and power consumption through a simulated IoT environment. I showed that the constraints on the CPU and memory limit the performance of the IDS but help to limit the power consumption; ii) moreover, I introduced an environment for performance and energy consumption evaluation of Intrusion Detection Systems (IDS), which could be crucial in the IoT context since it ensures robust security without compromising operational integrity; iii) I also developed DDoShield-IoT, a simulation testbed capable of generating real-world benign and malicious traffic. It operates in two phases, utilizing lightweight models for immediate traffic analysis subsequently aggregating packet features over time for in-depth analysis. The machine learning algorithms used for DDoS botnet traffic detection within this framework include Support Vector Machines (SVM), Kmeans, and Variational Autoencoders (VAE). DDoShield-IoT performance was evaluated based on accuracy, precision, recall, and F1 score parameters, showing considerable results. Additionally, resource consumption metrics, including CPU and memory usage, highlight the system's suitability for IoT environments with limited resources.

4. Research products:

In this second year, I had the following product:

4.1 Publications

Conference Paper

1. **Simona De Vivo**, Pietro Liguori, 2023 IEEE 34th International Symposium on Software Reliability Engineering Workshops (ISSREW), published, 2023.
2. **Simona De Vivo**, Islam Obaidat, Dong Dai, Pietro Liguori, 2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), under revision.

5. Conferences and seminars attended

...

6. Periods abroad and/or in international research institutions

I am still spending my period abroad at the University of North Carolina at Charlotte (UNCC). It started on June 8th, 2023, and will end on February 1st, 2024. Here, Dr. Bojan Cukic and Dr. Dong Dai oversee my work.

During this time, I focused my research study on the green cybersecurity in IoT field, developing an environment for performance and energy consumption evaluation of Intrusion Detection Systems (IDS). I also learned how to use DDoSim, a simulation testbed for mimicking real-world, large-scale botnet DDoS attacks, starting a collaboration with Dr. Islam Obaidat, a research and teaching assistant in Software and Information Systems (SIS) at UNCC, for the implementation of an enhanced version of DDoSim, i.e., DDoShield-IoT framework. This framework is designed for resource constrained environment of IoT and can generate real-world benign and malicious traffic. It also provides an Intrusion Detection Component capable of online detection, i.e., the detection in real-time during traffic generation.

Currently I spent at the UNCC seven of the eight months of the abroad period foreseen by my research project.

7. Tutorship

...

8. Plan for year three

During the third year of my Ph.D., I will be concluding my period abroad at the University of North Carolina at Charlotte. Then, I will continue the DigitalPlatforms SpA (DP) company collaboration for two months. For this partnership, I plan to execute sustainable security experiments, collect relevant data for my research activity, and support the company in the adoption of new green security technologies.

I will delve deeper into the Federated Learning approach to intrusion detection in IoT. Leveraging this Green AI solution, I plan to implement a lightweight FL-based network intrusion detection system suitable for resource and power consumption constraint systems. Moreover, I will study the IPv6 protocol security vulnerability, enhancing the DDoShield-IoT framework to detect the wide variety of cyber threats including those related to IPv6 weakness.