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

PhD Student: Gaetano Perrone

XXXIV Cycle
Training and Research Activities Report – Second Year

Tutor: Simon Pietro Romano

Summary

1 Information 3
2 Study and Training Activities 3
3 Research Activity 4
4 Products 5
4.1 Publications 5
4.2 Patents 5
5 Conferences and Seminars 5

1 Information

My name is Gaetano Perrone. I obtained Master Degree in Computer Engineering at the University Federico II in July 2017. Actually, I am attending PhD in Information Technology and Electrical Engineering without fundings. I am a PhD student that works in Epsilon S.R.L., a Consultant Company with a strong liason with the University and with the research field. My tutor is Professor Simon Pietro Romano. My research is mainly focused on Network Security field. Finally, I am cofounder of SecSI a cybersecurity startup, founded on 29/07/2019 and focused on SECurity Solutions for Innovation. SecSI has become an innovative startup on 10/11/2020.

2 Study and Training Activities

During my second year of the PhD I have followed different courses aimed at improving my knowledge in Software Security, Artificial Intelligence and Security By Default techniques.
I have attended the following 4courses:

- ***Secure System Design (Prof. Casola):*** I improved my knowledge in Cyber Security techniques used to protect against threats and the implementation of standard Authorization and Authentication protocols. As assignment of the course, I performed a lesson regarding a security by design architecture cluod-based (Amazon Web Services) implemented by Epsilon for an important customer; the customer required the compliance to Critical Security Controls for a public competitive call. The lesson illustrated an overview of security services in AWS and the coverage of Critical Security Controls by using these security services;
- ***Software Security per Sistemi Industriali (Prof Cotroneo):*** I increased my knowledge in secure code development, by looking at the main web application vulnerabilities and exploitation techniques of Buffer Overflow. As assignment of the course, I prepared a lesson regarding Threat Modelling and Risk Assessment techniques that can be used to implement a Security by Design approach in critical infrastructures. I illustrated all the process, starting from the Threat Modelling, detecting critical assets and security controls applied to the system, and risk evaluation according to OWASP Risk Methodology.

I have followed ML4Health2020 ***(Carlo Sansone, Marco Aiello, Anna Carrozza, Diego Gragnaniello, Francesco Isgrò, Roberto Prevete, Francesco Raimondi)*** module aimed at improving my skills in machine learning and Artificial Intelligence world. The module was very interesting as it was focused on Healthcare systems. I was interested at it as these systems require great safety and cybersecurity requirements.

Student: Gaetano Perrone (gaetano.perrone@unina.it) **Tutor:** Simon Pietro Romano (spromano@unina.it)

	Credits year 1								Credits year 2							
		1	2	3	4	5	6			1	2	3	4	5	6	
	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary
Modules	18	1,4	1,2	6	0,4		9,6	**18,6**	9		3		3.6	6		**12,6**
Seminars	13	0	0			0	5	**5**	6							**0**
Research	34	6	6	6	6	5	7,4	**36,4**	42							**47,4**
	65	7,4	7,2	12	6,4	5	22	**60**	57	0	3	0	0	6	0	**60**

Year	Lecture/Activity	Type	Credits	Certification	Notes
2	Software Security per Sistemi Industriali	MS Module	3	X	
2	Secure Systems Design	MS Module	6	X	
2	ML4Health2020	MS Module	3.6	X	

3 Research Activity

Main area of my research is Network Security.
I continued my research on the topics of the first year:

- The application of Artificial Intelligence to develop an intelligent agent able to use hacking techniques to detect web application vulnerabilities.
- The application of virtualization techniques to create network security scenarios for educational purposes.

As extension of the first year of research in the first topic, we developed a Reinforcement Learning models by using a multi-agent objective system that can be used to find Cross-Site-Scripting vulnerabilities.
Regarding the second topic, we refined the basic idea by improving the abstraction of design concept, and by providing a microservices-based heterogeneus environment to implement capture the flag events. This allowed us to publish the work on an International Conference
During the second year, I have explored new topics:

- The optimization of website structure discovery by using Semantic Clustering algorithms.
- The formal definition of the attacker behaviour during a Penetration Test activity
- The realization of a Generic Testing approach to find injection vulnerabilities in Web Applications
- Automatic Recheck of a Penetration Test activity by using Natural Language Processing techniques

My research is conducted in collaboration with Francesco Caturano. We have created a working group focused on network security field called SecSI.

4 Products

4.1 Publications

Published Papers

- *F.Caturano, G.Perrone, S.P. Romano, Hacking Goals: a goal-centric attack classification framework, , published to 28th 32th IFIP International Conference on Testing Software and System IEEE (ICTSS 2020)*
- *F.Caturano, G.Perrone, S.P. Romano, Capturing flags in a dynamically deployed microservices-based heterogeneous environment, 13th IEEE Principles, Systems and Applications of IP Telecommunications (IPTComm2020)*

Submitted Papers

- *F.Caturano, G.Perrone, S.P.Romano, "Discovering reflected Cross-Site Scripting vulnerabilities using a Multiobjective Reinforcement Learning environment", submitted to Computers & Security (2020) under second review*
- *D.Antonelli, R. Cascella, G. Perrone, S.P. Romano, A. Schiano, Leveraging AI to optimize website structure discovery during Penetration Testing, IEEE Transactions on Network and Service Management*

In Preparation

- *C.Brandi, F.Caturano, G.Perrone, S.P.Romano Generic Testing to find injection vulnerabilities in Web Applications*
- *F. Caturano E. De Martino G.Perrone S.P.Romano, Leveraging Knowledge Graphs to model Attackers' Behaviors*
- *F. Caturano A. Ferraiuolo M. Perna G. Perrone S.P.Romano, Recheck Through Ansible: a declarative-based approach to vulnerability fix validation*

4.2 Patents

We registered "Docker Security Playground" (https://github.com/giper45/DockerSecurityPlayground)to SIAE (Società Italiana degli Autori ed Editori) in date 10/06/2020. It is the software that allowed us to convert SecSI in an **innovative startup** on 10/11/2020.

5 Conferences and Seminars

IPTComm2020 Conference, Virtual Conference, Chicago, October 13-15