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

PhD Student: Antonia Affinito

Cycle: XXXV

Training and Research Activities Report

Year: First

student signature

Tutor: prof. Alessio Botta

Date: October 21, 2020

1. Information:

- **PhD student: Antonia Affinito**
- **DR number: DR993885**
- **Date of birth: 10/08/1992**
- **Master Science degree: Computer Engineering**
- **University: University of Napoli "Federico II"**
- **Doctoral Cycle: XXXV**
- **Scholarship type: *Unina***
- **Tutor: Alessio Botta**
- **Co-tutor:**

2. Study and training activities:

Activity	Type[1]	Hours	Credits	Dates	Organizer	Certificate[2]
"Intelligenza Artificiale ed etica: La ricerca in IA alla prova delle sfide etiche"	Course	8	1.6	06/12/2019	Dr. Roberto Prevete-DIETI	N
"Introduction to CERN and wakefield measurements at CLEAR"	Seminar	2	0.4	18/11/2019	Prof. Arpaia Pasquale	Y
"Blockchain for beginners"	Seminar	3	0.6	12/11/2019	Prof. Pierluigi Rippa	Y
"Deep Learning Onramp"	Seminar	2	0.4	21/11/2019	Prof. Carlo Sansone	Y
"Marked point processes for object detection and tracking in high resolution images: application to remote sensing data"	Seminar	1	0.2	2/12/2019	Prof. Giuseppe Scarpa	Y
"Lo spazio cibernetico come dominio bellico"	Seminar	2	0.4	15/11/2019	Prof. Guglielmo Tamburrini	Y
"Safety Critical Systems for Railway Traffic Management"	Course	20	3.3	10/01/2020 - 27/01/2020	Prof. Antonino Mazzeo; Prof.	Y

					Nicola Mazzocca	
"Cybersecurity and fuzzing for robots, blockchain and more"	Seminar	1	0.2	13/01/2020	Dr. Roberto Natella	Y
"Scientific Programming and Visualization with Python"	Course	20	2	27/02/2020 - 4/03/2020	DIST-Prof. Alessio Botta	Y
"Elettromagnetismo e salute"	Seminar	1	0.2	09/04/2020	Prof.ssa Rita Massa	N
"Computational Biology: Large scale data analysis to understand the molecular bases of human diseases"	Seminar	1	0.2	09/04/2020	Prof. Michele Ceccarelli-DIETI	Y
"How to get published with IEEE"	Seminar	2	0.4	20/04/2020	Dott.ssa Alessandra Scippa	Y
"Innovation Management, entrepreneurship and intellectual property"	Course	20	5	05/05/2020 - 19/06/2020	Prof. Pierluigi Rippa; StartCupCampania2020	Y
"Virtualization technologies and their applications"	Course	20	4	06/04/2020 - 30/04/2020	Prof. Domenico Cotroneo	Y
"Big Data Analytics and Business Intelligence"	Course	-	6	II Semester	Prof. Vincenzo Moscato	Y
"Large Scale training of deep neural networks"	Seminar	2	0.4	06/05/2020	Prof. Carlo Sansone	Y
"Design e nuove tecnologie. Possibili scenari per fronteggiare l'emergenza"	Seminar	1	0.2	11/05/2020	Innovation Village 2020	Y
"Access the eLearning library on IEEE Xplore"	Seminar	1	0.2	04/05/2020	Dr.ssa Alessandra Scippa	Y
"Health 4.0 – La rapidità della medicina e la velocità del cambiamento del nostro mondo organizzato da	Seminar	2	0.4	14/05/2020	Innovation Village 2020	N

Università degli Studi di Napoli Federico II"						
"Planning 5G under EMF constraints: challenges and opportunities"	**Seminar**	**2**	**0.4**	**18/05/2020**	**Prof. Luca Chiaraviglio; Dr.ssa Cacciapuoti; Dr. M. Caleffi**	**N**
"Virtual Seminars on sensing"	**Seminar**	**4**	**0.8**	**20/05/2020**	**Prof. Carlo Forestiere - Plasmonica**	**Y**
"La programmazione Europea e la ricerca. Nuovi scenari della programmazione europea dopo il 2020 – La gestione di un progetto di ricerca"	**Seminar**	**2**	**0.4**	**13/05/2020**	**Innovation Village 2020**	**N**
"Joint Design of Optics and Post-Processing Algorithms Based on Deep Learning for Generating Advanced Imaging Features"	**Seminar**	**2**	**0.4**	**19/05/2020**	**Part of the Signal Processing and Computational imagE formation (SPACE) by IEEE SPS**	**N**
"Exploring Autonomy in Robotic Flexible Endoscopy"	**Seminar**	**2**	**0.4**	**12/06/2020**	**Prof. Funny Ficuciello**	**Y**
"Machine Learning"	**Course**	**20**	**4**	**6/07/2020-17/07/2020**	**ITEE-ICTH**	**Y**
"Intelligenza Artificiale"	**Course**	**-**	**6**	**II Semester**	**Prof.ssa Flora Amaro**	**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	**1.6**	**2**	**6.4**	**0**	**10**
Bimonth 2	**3.3**	**0.2**	**6.5**	**0**	**10**
Bimonth 3	**2**	**0.8**	**7.2**	**0**	**10**
Bimonth 4	**15**	**3.6**	**4**	**0**	**22.6**
Bimonth 5	**10**	**0**	**5**	**0**	**15**
Bimonth 6	**0**	**0**	**7**	**0**	**7**
Total	**31.9**	**6.6**	**36.1**	**0**	**74.6**
Expected	**30 - 70**	**10 - 30**	**80 - 140**	**0 – 4.8**	

3. Research activity:

The Domain Name System, more simply DNS, plays an important role in Internet services. Its main function is to convert human-readable names (ex: example.com) in their corresponding IP addresses (ex: 93.184.216,34), and so it is considered as the phonebook of the Internet. If the DNS can be stopped, the majority of communications on the Internet are effectively interrupted.
The DNS represents an important observation point in order to study the main issues of current networks, including performance and security. In the scientific literature, several solutions have been developed to detect intrusions in a network or to evaluate its performance. Most of these work at the flow or packet level, but, in today high-speed networks, they suffer from scalability problems. For this reason, the DNS is currently considered a valid tool that it allows to analyze a lower percentage of traffic and to extract interesting information about the network operation.
In the security field, domain names are also popular for malicious use. For example, domain names are increasingly playing a role for the management of botnet command and control servers, download sites where malicious code is hosted, and phishing pages that aim to steal sensitive information from unsuspecting victims [1].
In addition, to remotely control an infected host, attackers need to build a command and control channel for sending command and transferring data. This channel is typically built on the DNS protocol, and so, observing the DNS traffic, it is also possible to detect infected hosts.
The DNS queries can be also useful to detect the performance of a network, in terms of network operation looking, for example, the response time of the queries. In fact, if the value of the response time is very high implies that the time to reach the requested domain is higher and therefore the network performance is low. Another interesting perspective on network performance, analyzing the DNS traffic, is to estimate the predominant type of traffic in a network or host. For example, if DNS queries for real-time video applications travel through this network, we can infer that a video call is made on one or more hosts.
During the first year, my study research focuses on the deepening of the DNS system and its functions. In particular, I focused on the security side and on the study of the existent methodologies to detect new malicious domain names [1],[2],[3],[4]. One of the primary techniques for protecting people from malicious domains is the use of the blacklists: continuously updated lists that contain detected malicious domain names. A large number of organizations maintain a blacklist (like Cisco Umbrella, VirusTotal). But blacklist platforms detect harmful entities only after they become active. Firstly, we have not focused only on the malicious domains, but we wanted to study the domain names and their common and different characteristics. In fact, the understanding of their common and distinctive characteristics allows identifying such domains (e.g. Malware, Streaming, Real-Time, etc.) without referring to a list but rather to their characteristics. For this purpose, we have adopted clustering techniques to investigate which characteristics are predominant in the similarity of the domain names.
The features related to the domain names are extracted from OpenINTEL, a platform developed by researchers of the University of Twente to create a high-performance scalable infrastructure of large-scale active DNS measurements.
We have also adopted two blacklists provided by Cisco Umbrella and VirusTotal to verify if each cluster contains malicious or benign domains and, in general, to understand the nature of the clusters.

Preliminary results show that some characteristics can be used to group together domains referring to the same (benign) applications as well as domains referring to malicious behaviors.

[1] DNS Traffic Analysis for Malicious Domains Detection; Ibrahim Ghafir and Vaclav Prenosil; 2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN).

[2] L. Bilge , E. Kirda, C. Krugel , and M. Balduzzi; EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis; ACM Transactions on Information and System Security; 2014.

[3] Antonakakis, M., Perdisci, R., Lee, W., Vasiloglou, N., and Dagon, D. 2011. Detecting malware domains at the upper DNS hierarchy. In Proceedings of the 20th Usenix Security Symposium.

[4] Felegyhazi, M., Kreibich, C., and Paxson, V. 2010. On the potential of proactive domain blacklisting. In Proceedings of the 3rd USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET'10).

4. Research products:

- *Antonia Affinito, Alessio Botta, Luigi Gallo, Mauro Garofalo, Giorgio Ventre; "Spark-based Port and Net Scan Detection"; The 35th ACM/SIGAPP Symposium on Applied Computing-ACM SAC; published; 2020.*
- *Antonia Affinito, Alessio Botta, Giorgio Ventre; "The impact of Covid on network utilization: an analysis on domain popularity"; IEEE CAMAD 2020; online conference; published; 2020.*

5. Conferences and seminars attended

- *The 35th ACM/SIGAPP Symposium on Applied Computing; ACM SAC; online conference; 30 March- 3 April; I presented the paper "Spark-based Port and Net Scan Detection";*
- *Network Traffic Measurement and Analysis Conference; TMA Conference; online conference;*
- *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks; IEEE CAMAD 2020; online conference; 14-16 September 2020; I presented the paper "The impact of Covid on network utilization: an analysis on domain popularity".*

6. Activity abroad:

7. Tutorship