UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

itee PhD information technology electrical engineering

DIETI UNINA

Antonia Affinito

Using DNS for evaluating network status and security

Tutor: Alessio Botta

Cycle: XXXV

Year: First

itee PhD information technology electrical engineering

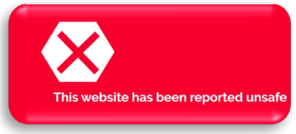
My background

- MSc degree: Computer Science Engineering
- First Year PhD: Academic Year 2019-2020
- Laboratory: ARCLab with Professor Alessio Botta
- Scholarship type: Unina

Research activity: Context

- A major issue in current networks is the scarce visibility of their status mainly in terms of security and performance

- **Security Issues**:
  - Detect new registered malicious domains;
  - Update blacklists;
  - Detect command and control servers.



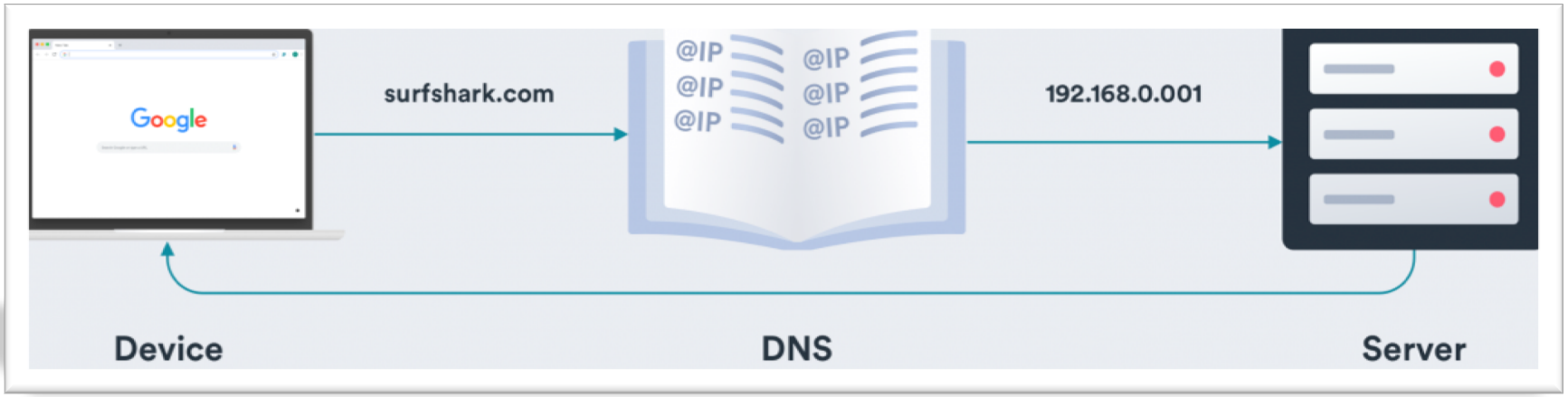
- **Network Performance**:
  - Detect the type of traffic of a network;
  - Analyze the speed of a network.

The existent solutions are based on the analysis at flow or packet level.

- Too much data;
- Unscalable.

The Domain Name System

The DNS represents an important observation point in order to study the main issues of current networks, including *performance* and *security.*



- Its ***main function*** is to translate the human-readable names in their IP addresses.
- It allows to analyze interesting information about the nature of domain names and network operation.

Research activity: Initial Contribution

- Analysis of the similar and different characteristics of the domain names:
  - Extracting the features from the zone files of the top-level domains;
  - Application of the clustering algorithms to investigate which characteristics are predominant in the similarity of the domain names
    - Including different classes of domains related to different kinds of applications;
    - Including malicious and benign domains.

Study Activities

- During the first year, my study activity focused on the deepening of the DNS system and its functions. Then, I also studied the security problems and the existent methodologies to detect new malicious domains.

- In order to deep this topic and its possible solutions I attended to the following courses and conferences:
  - Machine Learning; Intelligenza Artificiale; Scientific Programming and Visualization with Python; Virtualization Technologies and their Applications; Big Data Analytics and Business Intelligence; Intelligenza Artificale ed Etica.

  - *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks - CAMAD; Network Traffic Measurement and Analysis Conference - TMA Conference.*

My Products

[P1]	*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.*
[P2]	*Antonia Affinito, Alessio Botta, Giorgio Ventre; "The impact of Covid on network utilization: an analysis on domain popularity"; IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks- CAMAD; online conference; published; 2020.*

	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	

Thanks for the attention!