Università degli Studi di Napoli Federico II

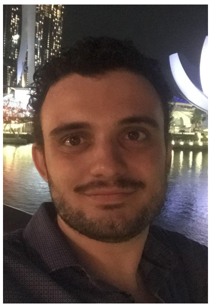
Dottorato di ricerca / PhD program in
Information Technology and Electrical Engineering

Ad hoc course announcement

Title: Hands-on Network Intrusion Detection via Machine and Deep Learning

Lecturer: **Dr. Antonio Montieri, PhD**

Università degli Studi di Napoli Federico II,
Department of Electrical Engineering and Information Technologies (DIETI)



***CV**: Antonio Montieri is an Assistant Professor (RTD-A) at the Department of Electrical Engineering and Information Technology of the University of Napoli Federico II. He received his Ph.D. degree in Information Technology and Electrical Engineering in April 2020 and his MS Degree in Computer Engineering in July 2015, both from the same University. He is a member of the Traffic and COMICS (COMputers for Interaction and CommunicationS) departmental research groups. His research interests concern network security, network measurements, (encrypted and mobile) traffic classification, traffic modeling and prediction, and eXplainable Artificial Intelligence (XAI) approaches for networks.*

***Website**: http://wpage.unina.it/antonio.montieri/*
***Email**: antonio.montieri@unina.it*

Credits: 4

Overview

The course covers topics regarding the design, realization, and evaluation of Network Intrusion Detection Systems (NIDSs) used for protecting networks against attacks. Specifically, the course details how Machine Learning (ML) and Deep Learning (DL) approaches can be properly exploited to develop these detection systems. The course briefly provides the basics on the most common attacks against networks and on ML and DL models used to counteract them. The students will learn methodological guidelines to determine which are the most suitable models and input data based on, for instance, the problem to face (e.g., anomaly detection, attack classification), the information available (e.g., supervised vs. unsupervised), and the attacks to deal with (e.g., DDoS, BotNet). The course follows a "hands-on" approach that will guide the students toward the actual design, implementation, and performance evaluation of NIDSs, exploiting the tools provided by state-of-the-art (Python) frameworks (e.g., Scikit-learn, Keras, PyTorch). The course will make extensive use of actual case studies based on data from real network attacks (e.g., attacks against IoT or Android devices) to provide the operational scenarios for the detection systems. There will be a final assessment concerning the realization of a basic prototype and a report describing its design and evaluation.

Schedule

Lecture	Date	Time	Topics	Lecturer
1	09/01/2024	10:00 - 12:00 (2 hours)	Introduction to Network Intrusion Detection	Antonio Montieri
2	11/01/2024	10:00 - 13:00 (3 hours)	Design, implementation, and evaluation of NIDSs	Antonio Montieri
3	16/01/2024	10:00 - 13:00 (3 hours)	Hands-on detection and classification of Android malware traffic	Antonio Montieri
4	17/01/2024	10:00 - 13:00 (3 hours)	Hands-on attack traffic classification in IoT environments	Antonio Montieri
5	18/01/2024	10:00 - 13:00 (3 hours)	Hands-on cross-evaluation of NIDSs in different network contexts	Antonio Montieri
			Assessment project: realization of a basic prototype along with a report describing its design and evaluation	

Content Details

Lesson 1 - Introduction to Network Intrusion Detection. Introduction and basics of attacks against network environments. Methodological key points for the design of a Network Intrusion Detection System (NIDS) based on Machine Learning (ML) and Deep Learning (DL): datasets, algorithms, input data, and evaluation benchmark.

Lesson 2 - Design, implementation, and evaluation of NIDSs. Frameworks and tools for the design, implementation, and evaluation of NIDSs based on ML and DL. Examples using Scikit-learn, Python Keras, and PyTorch.

Lesson 3 - Hands-on detection and classification of Android malware traffic. ML vs. DL approaches. Hierarchical vs. flat malware traffic classifiers.

Lesson 4 - Hands-on attack traffic classification in IoT environments. Input-data selection and optimization. Single-modal vs. multimodal solutions. Investigation of NIDS input importance via occlusion analysis.

Lesson 5 - Hands-on cross-evaluation of NIDSs in different network contexts. Training and operational strategies for cross-evaluation of ML/DL-based NIDSs. How to improve the robustness of NIDSs when changing the network context.

Important Notes

Participants are requested to join the following MS Teams group:

https://teams.microsoft.com/l/team/19%3a0sBXSWIpKiaWF9DrgTM9m02rFNEdKdNYQoUWkLbfQDI1%40thread.tacv2/conversations?groupId=b142bcee-3089-4e9c-8c4d-3cf7b6da9755&tenantId=2fcfe26a-bb62-46b0-b1e3-28f9da0c45fd

Team Code: j4sn9o2

Once accepted in the Teams group, students have to fill the following .xlsx file with their information (the .xlsx file can also be found within the Files of the Teams group):

https://communitystudentiunina.sharepoint.com/:x:/s/AdhocITEEPhDcourse-Hands-onNIDSviaMLandDL-Dr.A.Montieri/EZedWSLR_b1ArkUSNvd9q4oB-lhL8GEKtQCzFh5B6rToQg?e=3C8odQ

The course is conducted on-site. However, students pursuing their PhD period abroad (for research purposes) have the option to request remote attendance for classes via MS Teams.

There will be a final assessment.

For information: Dr. Antonio Montieri (DIETI, UniNA) – antonio.montieri@unina.it