UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

DOTTORATO DI RICERCA / PHD PROGRAM IN
INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

Ad hoc course announcement

Title: Practical Network Intrusion Detection with Machine Learning and Generative AI

Lecturer: Dr. Giampaolo Bovenzi, PhD

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

***CV**: Giampaolo Bovenzi 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 May 2022 and his MS Degree in Computer Engineering in October 2018, 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/giampaolo.bovenzi/*
***Email**: giampaolo.bovenzi@unina.it*

Credits: 4

Overview

The course addresses the design, implementation, and evaluation of Network Intrusion Detection Systems (NIDSs) aimed at protecting networks against malicious attacks. In particular, it explores how Machine Learning (ML) and Deep Learning (DL) techniques—with a special focus on Generative Artificial Intelligence (GenAI)—can be effectively leveraged to build such systems. The course introduces the fundamentals of the most common network attacks as well as the ML, DL, and GenAI models used to mitigate them. Students will acquire methodological guidelines to identify the most suitable models and input data depending on the task at hand (e.g., anomaly detection, attack classification), the type of information available (e.g., supervised vs. unsupervised learning), the specific threats to address (e.g., DDoS, BotNet). Adopting a practical approach, the course guides students through the hand-on design, implementation, and performance evaluation of NIDSs using state-of-the-art Python frameworks (e.g., Scikit-learn, PyTorch, HuggingFace), . Case studies based on real-world attack data (e.g., targeting IoT or Android devices) will be extensively employed to provide realistic scenarios for the systems under study. The final assessment consists of the presentation of a paper on one of the covered topics.

Schedule

Lecture	Date	Time	Classroom	Topics	Lecturer
1	01/10/2025	16:30 - 18:30 (2 hours)	C2A *Build. 3/A*	Essentials of Network Intrusion Detection Systems	Giampaolo Bovenzi
2	02/10/2025	10:00 - 13:00 (3 hours)	Seminari (ex Softel) *Build. 3/A*	Methodologies for Designing and Evaluating NIDSs via ML and GenAI	Giampaolo Bovenzi
3	07/10/2025	16:30 - 19:30 (3 hours)	C2A *Build. 3/A*	Designing NIDS via Hierarchical Learning	Giampaolo Bovenzi
4	08/10/2025	16:30 - 19:30 (3 hours)	C2A *Build. 3/A*	Evolving NIDS for Rare and Novel Attacks	Giampaolo Bovenzi
5	09/10/2025	10:00 - 13:00 (3 hours)	Seminari (ex Softel) *Build. 3/A*	Recap and Assessment Project: Presentation of a selected paper	Giampaolo Bovenzi

Content Details

Lesson 1 - Essentials of Network Intrusion Detection Systems. Fundamentals of network attacks, overview of NIDSs, and key methodological principles for ML, DL, and GenAI-based detection systems.

Lesson 2 - Methodologies for Designing and Evaluating NIDSs via ML and GenAI. Frameworks, tools, and workflows for building and evaluating ML/DL-based NIDSs, with practical examples using Python libraries such as Scikit-learn, PyTorch, and HuggingFace.

Lesson 3 - Designing NIDS via Hierarchical Learning. Practical exercises comparing ML vs. DL approaches, hierarchical vs. flat traffic classifiers, and case studies on real Android malware traffic.

Lesson 4 - Evolving NIDS for Rare and Novel Attacks. Challenges of catastrophic forgetting and intransigence, with strategies such as fine-tuning, fixed-representation, and model-growth combined with few-shot learning for adaptive detection.

Lesson 5 - Recap and Assessment Project. Presentation of a selected paper on one of the topics covered in the course, summarizing practical and methodological insights.

Important Notes

Participants are requested to join the following MS Teams group:

https://teams.microsoft.com/l/team/19%3AI03Q74tcfGKSFUhVL1XAMeHNdGrkVq7rDnsuY3TgM-o1%40thread.tacv2/conversations?groupId=f2decd1a-3e8d-4a33-8768-b0bc400308e8&tenantId=2fcfe26a-bb62-46b0-b1e3-28f9da0c45fd

Team Code: bawbmhm

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-PracticalNetworkIntrusionDetectionwithMac/ESRoz9CY8IdKmAEV5az3yg4BbUjQn_CZf0iIgRkIX210IQ?e=IsXkXM

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. Giampaolo Bovenzi (DIETI, UniNA) – giampaolo.bovenzi@unina.it