UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Dipartimento di Scienze Fisiche, Informatiche e Matematiche

Friend or Foe? On the Interplay between ML and Cybersecurity

Relatore: Dr. Giovanni Apruzzese
Affiliazione: University of Liechtenstein

Abstract. Machine Learning (ML) technologies have rapidly progressed from being a niche research topic to being widely deployed in real-world systems. Indeed, recent ML advancements have far exceeded the expectations of most experts: today, everyone can use---oftentimes for free and without requiring any sort of specialized expertise---some form of ML-based system to carry out a plethora of tasks.

Unfortunately, such quick progress and broad accessibility comes with risks. For instance, ML techniques are affected by a variety of security problems (e.g., the so-called "adversarial examples") for which no effective solution has been found yet. And while ML can enhance security systems (e.g., to detect cyber threats), such benefits can be exploited also by attackers (e.g., to compromise systems, or deceive human users).

In this talk, I will discuss the three areas in which ML and Cybersecurity intersect: first, how ML helps solve security problems; second, the security and privacy challenges of deploying ML in real-world systems; and third, how ML can be used offensively to cause harm. Drawing on both recent research findings and real-world incidents, the talk is designed for a broad audience and requires no prior ML expertise or mathematical background.

The expected outcome is that attendees will have obtained some understanding of the open issues that stem from the widespread deployment of (and accessibility to) ML technologies, so that proper remedies can be found in the years to come.

Time and location: October 24, 2025, 9.00 a.m.; Room M0.1, Building MO18 (Mathematics Building) Dept. FIM – Via Campi 213/b – Modena

Short bio. Giovanni Apruzzese is an Assistant Professor within the Hilti Chair of Data and Application Security at the University of Liechtenstein. He obtained the PhD in Information and Communication Technologies at the University of Modena and Reggio Emilia (Italy) in 2020. He authored over 30 peer-reviewed papers at internationally-recognized research venues. His research interests encompass a variety of themes, most of which revolve around cybersecurity and artificial intelligence. His primary expertise lies in network security and in phishing detection.

Host: Mauro Leoncini