Modeling and Detecting AI-based Cyber Threats

Context and Motivation

Dynamic cyberattacks, characterized by their adaptability and sophistication, represent an evolving challenge in cybersecurity. Unlike traditional threats which often rely on predefined patterns, dynamic attacks can change tactics to evade detection mechanisms. This evolution means the shift from manual threat orchestration to a more automated and intelligent attack system, making them increasingly difficult to predict and mitigate.

The integration of artificial intelligence (AI) in the execution of cyberattacks allows attackers to automate their decision-making processes, and even adapt their attack strategies in real time according to the defensive measures they encounter. This not only increases the speed and scale of attacks, but also allows for a level of customization that was previously unattainable, making AI-assisted cyberattacks a significant challenge for even the most advanced defense solutions.

This joint PhD project between the University of Lorraine, France, and the International University of Rabat, Morocco, is a collaborative project that aims to develop an in-depth analysis of dynamic and AI-assisted cyberattacks, and to develop approaches to detect and mitigate them.

Objectives

The objectives of this PhD thesis are:

- **Attacker behavior analysis**: Understand attackers' tactics, techniques, and procedures by analyzing data from past and ongoing attacks. This includes studying the mechanisms used in AI-based attacks.
- **Predictive model development**: Designing advanced predictive models using machine learning (e.g., dynamic spatiotemporal graph neural networks) to identify patterns and signatures of dynamic and AI-based attacks. These models will help anticipate this type of attack and improve detection systems in near real-time.
- **Building Countermeasures and Mitigation Strategies**: Develop and test response and mitigation strategies to neutralize dynamic attacks, minimizing potential damage.
- **The development of game theory-based models**: Explore the use of game theory models, such as Markovian dynamic games, to evaluate the effectiveness of defensive methods against AI-assisted attackers. This involves quantifying the values of the game model for decision-making in scenarios in which attackers use AI techniques to launch advanced attacks.

Work Environment

This thesis project is co-supervised by the University of Lorraine (UL), Nancy, France, and the International University of Rabat (UIR), Rabat, Morocco. The host laboratories are TICLab (UIR) and LORIA (UL). The thesis is spread over 36 months. The doctoral student will ideally spend 18 months at the UIR and 18 months at the UL, in total.

Compensation and Benefits

The doctoral student will benefit from a LUE "Lorraine University of Excellence" excellence scholarship. Travel costs between the two countries are covered. The doctoral student will benefit from several facilities in both campuses (swimming pool, sports hall, catering, etc.).