Data-driven Vulnerability Analysis for Critical Infrastructures

Zhenlu Sun[1,*], Salman Toor[1,*], and André Teixeira[1,*]

[1]Department of Information Technology, Uppsala University, Uppsala, Sweden
[*]zhenlu.sun, salman.toor, andre.teixeira@it.uu.se

ABSTRACT

Software applications and reliable communication are key to offer regular and mission critical services online. Mission critical services are part of critical infrastructure sectors like healthcare, finance, communications, and power generation and distribution. To support a reliable, secure, and efficient offering of software services for critical infrastructures, the cybersecurity and trustworthiness of software and computing infrastructures are vital. In 2020, 56% of energy utility facilities reported cyberattacks on their installations, a number that is likely to increase as novel machine learning-based services are deployed within these critical infrastructures. Thus, it is of utmost importance to take all possible measures to secure the computing systems supporting critical infrastructures and ensure uninterrupted availability of services.

A possible way forward on secure these systems is to design and develop a comprehensive and proactive vulnerability analysis framework for software applications running on critical infrastructures. Effective vulnerability analysis is a highly challenging task requiring real-time processing of massive datasets based on millions of reported vulnerabilities available in public databases, traces coming from underlying software frameworks and libraries, and data based on application development and execution processes. Vulnerability analysis for critical infrastructures requires a focused, data-driven approach that covers all aspects that are crucial to ensuring a reliable, secure, and efficient offering of uninterrupted services. The proposed project, with its well-defined focus areas, is a cross-disciplinary effort within data science and cybersecurity to develop a firm understanding of the dynamics of the vulnerability landscape for critical infrastructures, to design explainable predictive vulnerabilities analysis frameworks, and to develop a methodology for knowledge transfer between different infrastructures.

Among the numerous techniques in the field of cybersecurity, the attack graph approach stands out as one of the most promising methods. It plays a crucial role in network security analysis and has garnered increasing attention in recent years. An attack graph is a directed acyclic graph that describes the potential attack paths that external or internal attackers could exploit. By identifying these attack paths, security professionals can prepare and deploy corresponding patches to mitigate possible attacks. The risk assessment generated from attack graph analysis can also assist in decision-making processes, striking a balance between security and economic considerations when designing a network. Generating an attack graph for specific systems typically involves collecting information on network topology, vulnerabilities, network configuration, network connections, and assets. However, the rapid growth in modern network presents several challenges to attack graph analysis, including issues of low scalability and high complexity. This project aims to harness the power of machine learning to address these challenges. Furthermore, the dynamic analysis of vulnerabilities in real-world systems, an area that has received limited attention in previous research, will be another focal point of this project.