HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Attack Graph and Graph Analytics for Cybersecurity (Proposal for a Master Project in WS2020/21)

Background

Attack graph is a well-known method to model, analyze, and evaluate the security of complicated computer systems or networks. To construct an attack graph, runtime information about the target system or network environment is monitored, collected, and evaluated together with existing descriptions of known vulnerabilities. The outputs are visualized into a graph structure for further analytics and theoretical measurements. With recent development of modern hardware, powerful computing diagrams, and innovations on AI and Big Data, graph and graph-based technologies have drawn great attention from both academia and industry, evolving many promising approaches to solve or mitigate new challenges in Cybersecurity.

Objectives

The goals of this master project are:

(1) study and evaluate the state-of-the-art theories and practices of graph and graph analytics;
(2) investigate and showcase feasibilities and benefits to apply graph and graph analytics in the domain of cybersecurity;
(3) propose and conceptualize methods to enhance existing cybersecurity solutions using new techniques of graph modeling and analytics.

The results of this project intends to provide theoretical foundation and direction for the integration of the latest graph theories and practices in current cybersecurity landscape of the large enterprise network, enabling more efficient collection, processing, storage, and analysis of security relevant data, as well as advanced threat detection capabilities.

Deliverables

The deliverable of this project is supposed to be a technical report and several running prototypes of use cases.

Requirements

Knowledge and experiences/skills on 1) Network/software security as well as IT operations and management, and 2) (Big) Data science and engineering, are expected.

Contacts

Prof. Dr. Christoph Meinel, Dr. Feng Cheng, Pejman Najafi
Email: security-analytics@hpi.de
Room: H-1.13 | Tel: +331-5509-519