Graph Analytics for Cybersecurity

-- Proposal for Master Thesis in 2021/2022

IT Security Engineering (Sec-Eng) Team
Prof. Meinel's Chair „Internet Systems and Technologies"
Hasso Plattner Institute, Potsdam, Germany

Motivation

- To Model as much as possible Security-relevant Data into Graph, e.g., Attack Graph, CTI Knowledge Graph, etc.
  - Environmental (infrastructure) data: networks, hosts, applications, users, ...
  - CTI/OSINT: e.g., vulnerabilities, weaknesses, attack Techniques and Tactics, IOCs, …
  - Runtime data: alerts, logs, traffics, memory snapshots, process lists, ...

- To Establish effective **Graph Analytics** for Threat Detection/Hunting:
  - Graph-based Reasoning, Partitioning, Clustering, Machine Learning, Outlier/Anomaly Detection, ……

Goals

- study and evaluate the **state-of-the-art theories and practices** of Graph Modeling & Analytics;
- investigate and **showcase** the feasibilities and benefits to apply Graph Modeling & Analytics in the domain of cybersecurity;
- propose and conceptualize methods to **enhance existing cybersecurity solutions** (e.g., some mainstreaming SIEM systems) using new graph modeling & analytics techniques

Research Topics

- Topic 1: **Attack Graph** and Graph modeling of security relevant data
  - Newly available data sources
  - Graph representation of heterogeneous data
  - Efficient Graph construction

- Topic 2: Recent advancements on **graph theories and techniques**
  - Graph-based data structures and Graph specific algorithms
  - Graph data engineering: database, operations, visualization, SIEM built-in Graph capabilities, ...

- Topic 3: **Graph analytics for advanced threat detection**
  - reasoning, correlations, partition, mining,....
  - performance, scalability, ...

Organization

- Requirements:
  - M.Sc. Programs: **Cybersecurity**, IT Systems Eng., or Data Eng.
  - (**Expected**) knowledge and experiences/skills on
    - Network/System/Application security, IT/Security operations and management, (Big) Data science and engineering, etc.

- Deliverables:
  - Master Thesis
  - running prototype
  - Scientific publications on international conferences/journals (**expected**)

- Supervision:
  - Sec-Eng@HPI: Dr. Feng Cheng, Pejman Najafi
  - Cybersecurity/Data Engineering experts from our project partners

Thank you for your attention!

HPI IT Security Engineering (Sec-Eng) Team
Hasso-Plattner-Institut at University of Potsdam
Campus Griebnitzsee, 14482 Potsdam, Germany
Email: security-analytics@hpi.uni-potsdam.de
Online Services: https://sec.hpi.de