Prof. Dr. Christoph Meinel
IT Security Engineering (Sec-Eng) Team
Internet Technologies and Systems Group

Vulnerability Database for Cyber Threat Intelligence - Proposal for a Master Project in SS2022

Background

The vulnerability information is one of the major and most important sources of cyber threat intelligence (CTI). The currently running HPI Vulnerability Database (HPI-VDB) provides a comprehensive and up-to-date repository, which contains a large number of known vulnerabilities of Software. The textual descriptions about each vulnerability entry are grabbed from the public portals of other vulnerability databases, software vendors, security forums, etc. and then normalized into a well-structured data model. Thanks to the high-quality vulnerability data, many analytical services can be provided, including browsing, searching, self-diagnosis, Attack Graph (AG), as well as other API-based ad-hoc analytics. With the increasing demand of data-driven threat detection, it makes sense to research and implement more efficient management of vulnerability information to achieve high-quality CTI data.

Objectives

The goals of this master project are:

- Exploration and study of state-of-the-art vulnerability modeling and management techniques as well as the organization and features of popular vulnerability databases (VDBs);
- Research and investigation on challenges and solutions to integrate vulnerability information in a hybrid Threat Intelligence Platform (TIP);
- Design and development of an enhanced version of HPI-VDB as well as the PoC version of HPI-TIP.

The results of this project intends to provide theoretical foundation and practices for integration of new vulnerability databases as well as high-performance collection, processing, validation, storage, and applications of vulnerability information.

Deliverables

The deliverables of this project include:

- an enhanced version of HPI-VDB
- a conceptual design and PoC of HPI-TIP, and
- a technical report.

Target Disciplines (sorted by priorities)

- **Cybersecurity**
- IT-Systems Engineering
- Data Engineering

Contacts

Prof. Dr. Christoph Meinel, Dr. Feng Cheng, Pejman Najafi, Wenzel Pünter
Email: security-analytics@hpi.de | Room: H-1.10/12 | Tel: +331-5509-519