

Vulnerability Research: Modeling and Honeypot

Background

Along with the rapid development of Hardware and the overall IT-Infrastructures, e.g., faster and many/multi-core supported CPU, larger and more reliable main memory, etc., Computer Software as well as attacks and countermeasures of the Software become more and more complicated. It leads to an increasing amount of complex vulnerabilities as well. To identify, reproduce, analyze, confirm, specify, organize and later make use of the vulnerability is challenging but necessary research work.

Description and Concrete Tasks

HPI-VDB portal is the result of research work being conducted by IT-Security Engineering Team in the chair "Internet Technologies and Systems" at HPI. It is a comprehensive and up-to-date repository which contains a large number of known vulnerabilities of Software. Till now, it includes about 57,000 well-structured vulnerability entries. The proposed bachelor project aims to:

- 1) further improve the existing HPI-VDB with providing higher quality data and more add-on services;
- 2) explore the general methodologies and workflow of vulnerability analysis;
- 3) implement vulnerability analysis toolkits with focus on SAP software

We propose to build a virtualized SAP Software platform (with some typical SAP software installed and a self-contained scenario running). Based on this environment, such approaches as simulation, honeypot, penetration testing, attack modeling, and HPI Security Analytics Lab (SAL) will be deployed to gather the security-relevant event information. It is expected that this platform can integrate most popular and useful security auditing and analytics methods and be further used to analyze and evaluate the SAP software and its vulnerabilities. The project task can be divided into four parts:

- 1) General vulnerability research and HPI-VDB optimization;
- 2) Research and development of attacks and honeypots for SAP software;
- 3) Deployment of a SAL-monitored SAP platform;
- 4) Integration of analysis methods for vulnerabilities of SAP software

Deliverables

- An optimized version of HPI-VDB
- A running prototype of SAP software vulnerability assessment platform (incl. honeypot/attack/analytics/model/archive/....)
- A technical report about the general vulnerability research as well as modeling and honeypot methodologies for exploring SAP software vulnerabilities

References

- SAL: <http://sal.hpi-web.de/>
- HPI-VDB: <https://www.hpi-vdb.de/>

Contact

- Prof. Dr. Christoph Meinel, Dr. Feng Cheng, Andrey Sapegin (HPI)
- Industrial Partner: SAP AG