Bachelor/Master/Praktikum

Ransomware Detection in Databases

Motivation

Ransomware is a popular form of malware, which was initially targeting PC (client) platforms, but moved on to servers recently. Client-side ransomware typically encrypts files in a file system and holds the decryption key until the victim pays a ransom. Server-side version, in contrast, encrypts or destroys data in a database through a remote connection. Hence, the same methods cannot be used to detect both ransomware types.

While previous research has developed countermeasures against client-side ransomware, the problem of server-side ransomware has received zero attention. The only solution developed so far is a DIMAQs framework for SQL servers, which was developed at our chair in a master thesis last year. DIMAQs is an intrusion detection framework which is based on colored Petri nets (CPN)-based classifier. It models malicious SQL query sequences and matches them against query sequences captured at runtime. The successful detection of ransomware attacks depends on proper CPN configuration, which needs to be done manually in the current design.

Goals

The goal of this project is to improve the initial design of DIMAQs and to extend it with automated approach to CPN configuration. In particular, the scope of the master thesis is to develop and implement the method to construct the CPN configuration automatically using machine learning techniques and from observing malicious traffic. We are also interested in porting the DIMAQs solution to other database types, such as MongoDB, ElasticSearch, Cassandra, Hadoop, and CouchDB – these tasks are more suitable for a Bachelor Thesis or a Master Practicum.

- Analyze current ransomware attacks on database servers
- Port and extend an existing database Intrusion Detection System to other database types (e.g. MongoDB, ElasticSearch, etc.)
- Develop an automated approach to security policy engineering using machine learning

Duration

6 months

Contact

Lukas Iffländer
lukas.ifflaender@uni-wuerzburg.de

Prof. Alexandra Dmitrienko
alexandra.dmitrienko@uni-wuerzburg.de