Efficient and effective ransomware detection in databases

ACSAC ‘18, San Juan, Puerto Rico, USA

Christoph Hagen, Alexandra Dmitrienko, Lukas Iffländer,
Michael Jobst, Samuel Kounev
Contact: christoph.hagen@uni-wuerzburg.de

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Motivation

No dedicated solution against the increasing threat of ransomware targeting databases

- 5 billion USD of estimated damages through ransomware in 2017
- Attacks against thousands of MongoDB servers in January 2017
- MySQL, ElasticSearch, Cassandra, Hadoop, CouchDB ransomed as well

Challenges

Database ransomware is substantially different to client-side ransomware

- No malicious binaries to detect
- Individual queries are benign
- No cryptographic primitives used
- Attacks can be performed across multiple sessions/users

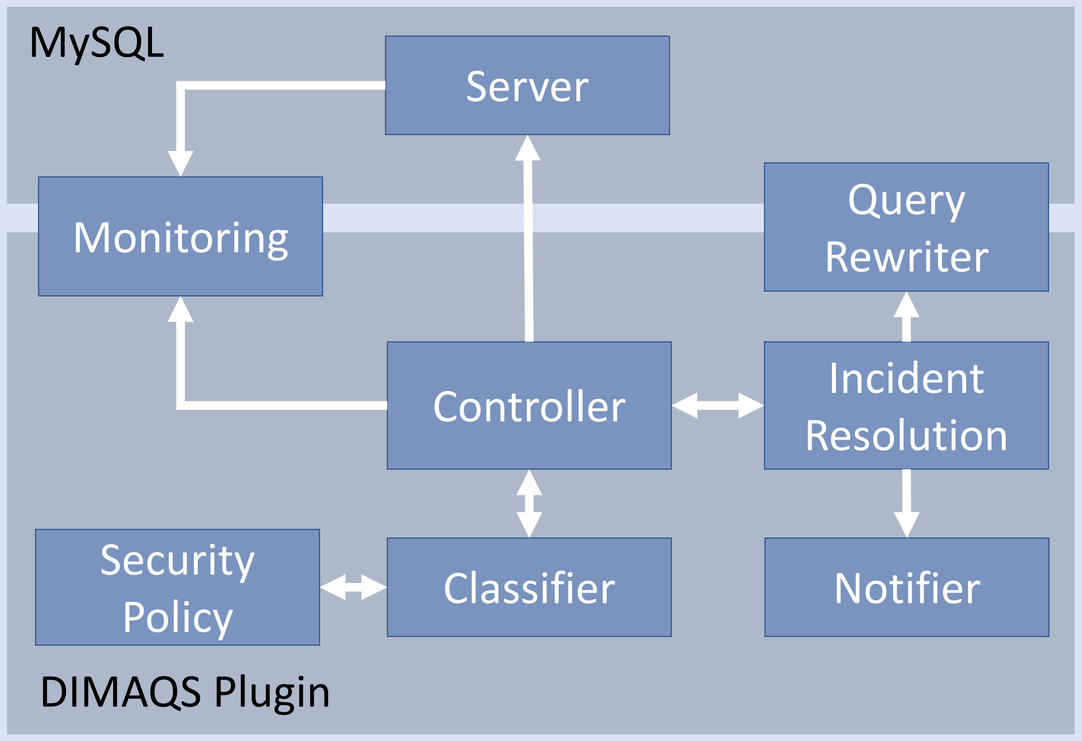
Approach

Ransomware detection through signature-based classifier

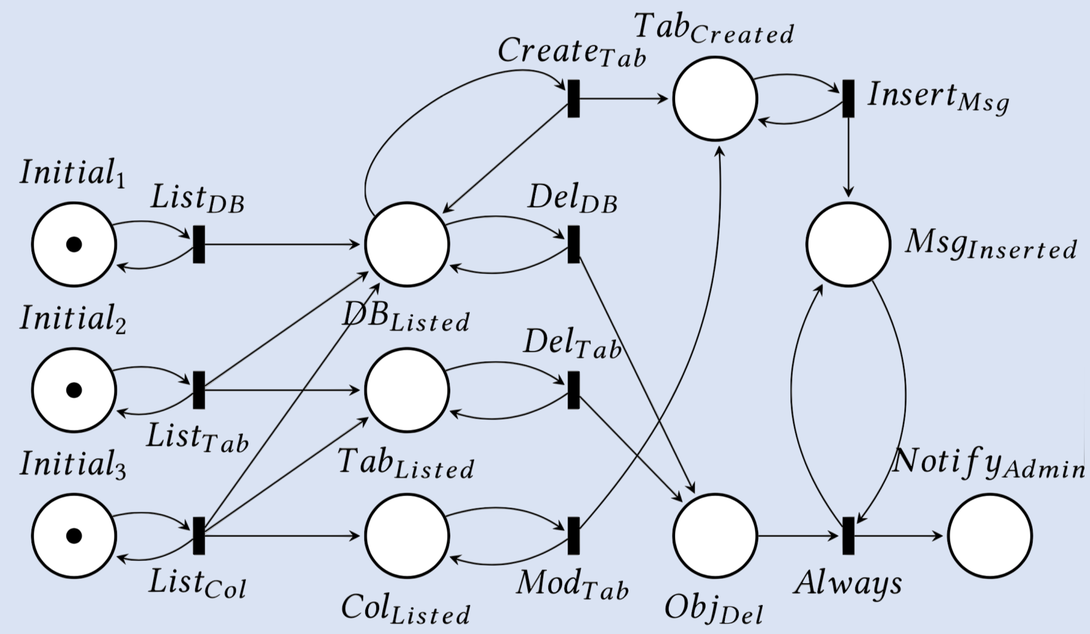
- Classify queries according to security policy derived from attack signatures
- Perform preemptive backups of modified data for later recovery
- Modify queries for full transparency of the system to the attacker
- Administrator notification per e-mail for detected incidents

Design & Implementation

Architecture



Classifier based on colored petri nets



Representation of the CPN used to detect current ransomware attacks. Potentially malicious queries trigger token transitions, leading to an alert, if all attack steps have been observed

Proof of concept implementation as a plug-in for MySQL server

Evaluation

Data set	Total queries	False positives	False negatives
Malicious set	53,940	0	0
BibSpace	52,085	0	0
MediaWiki	2,514,764	0	0

- Performance overhead ∽5 %