Efficient and effective ransomware detection in databases

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

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

<table>
<thead>
<tr>
<th>Data set</th>
<th>Total queries</th>
<th>False positives</th>
<th>False negatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious set</td>
<td>53,940</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BibSpace</td>
<td>52,085</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MediaWiki</td>
<td>2,514,764</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- Performance overhead ≈5%