Intrusion Recovery in Cloud Computing

David R. Matos
Advised by
Miguel L. Pardal  Miguel Correia

Abstract

• A novel approach to remove the effects of intrusions in cloud applications
• Does not require modifications to the source code of the application
• Can be deployed in public Cloud offerings
• Use of machine learning algorithms and other techniques to undo the effects of intrusions

Step 1 – Finding Intrusion Effects

• Each intrusion causes specific effects in the state of the application
• It is possible to identify the one operation that triggered the corruption of the state
• However, calculating the effects of such intrusion is time-consuming and delicate.

Database recovery: NoSQL Undo

• NoSQL databases are widely used in cloud applications due to their scalability capacity and simplicity
• However, like any other database, it is vulnerable to intrusions
• NoSQL Undo is capable of undoing intrusions from a NoSQL database without requiring it to go offline and preserving every valid operation
• No software modifications are required to the database or application

Step 2 – Reverting Intrusion Effects

• Once every malicious state modification was identified it is necessary to undo them
• It is also necessary to undo malicious operations in such a way that the consistency of the application is preserved
• Valid state modification should be kept

Application recovery: Rectify

• Uses machine learning algorithms to find the effects of intrusions
• Can be deployed alongside web applications in any PaaS
• No software modifications are required

Results – Time to recovery

Results: Overhead

Backup

Backup vs Recovery

Backup

• Undoes everything that happened after the intrusion
• Intrusions detected too late will require older backups
• System is offline during recovery

Recovery

• Only the effects of the intrusion are undone
• No valid data is lost
• Does not require the system to be offline to recover

Backup

Recovery

Website

Defaced

Website

Recovered

Application

rectify

Protected App DB

Compensating DB Statements

DB Statements Matching

Signature Record

Signature Matching

HTTP Log

Knowledge Base

DB Log

HTTP Request

Malicious

Signature

HTTP Request

Malicious

HTTP Request

Malicious

Rectify

System

Administrator

Query

Router

Intrusion Detector

NoSQL Undo

NoSQL Database Instance

Shard 1

Shard 2

Config Servers

Config

Config

Secondary

Secondary

Primary

Secondary

Secondary

Primary

Secondary

Secondary

Config

Support Layer

Global Log

Backup Service

NoSQL Undo

Rewritten

Figure

With Rectify

Wordpress

LimeSurvey

MediaWiki

Number of operations to undo

Time to Recover (s)

Throughput (ops/s)