Project PCAS: Secure Personal Devices backed by the Cloud

Miguel Pupo Correia
Confraria de Segurança, June 2015

Project PCAS at a glance

• 2013-16
• Funded by the European Commission, FP7
• Consortium:

<table>
<thead>
<tr>
<th></th>
<th>INESC ID - INSTITUTO DE ENGENHARIA DE SISTEMAS E COMPUTADORES, INVESTIGACAO E DESENVOLVIMENTO EM LISBOA</th>
<th>INESC ID - INSTITUTO</th>
<th>Portugal</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>k't's v's/e w^2^/s</td>
<td>IS</td>
<td>Israel</td>
</tr>
<tr>
<td>3</td>
<td>UNIVERSIDAD POLITECNICA DE MADRID</td>
<td>UPM</td>
<td>Spain</td>
</tr>
<tr>
<td>4</td>
<td>NORSK REGNESENTRAL STIFTELSE</td>
<td>NORSK REGNESENTRAL S</td>
<td>Norway</td>
</tr>
<tr>
<td>5</td>
<td>COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES</td>
<td>CEA</td>
<td>France</td>
</tr>
<tr>
<td>6</td>
<td>MAXDATA-INFORMATICA LDA</td>
<td>Maxdata</td>
<td>Portugal</td>
</tr>
<tr>
<td>7</td>
<td>AFCON CONTROL &amp; AUTOMATION LTD</td>
<td>AFCON CONTROL &amp; AUTO</td>
<td>Israel</td>
</tr>
</tbody>
</table>
Schedule

1. Secured Personal Device
2. Shuttle: cloud intrusion recovery
Motivation: smartphones

- Smartphones are convenient to store personal data & authentication
- but security is weak and storage capacity is limited

Secured Personal Device (SPD)

- The Secured Personal Device is the main outcome of PCAS
  - a smartphone add-on (or “sleeve”)
  - recognizes the user using biometric sensors
  - high storage capacity
  - physically isolated from smartphone (except USB conn.)
- Use:
  - allows users to authenticate themselves
  - allows users to securely store data
Role of the smartphone

• SPD has to communicate with trusted (cloud) services
• Smartphone provides the SPD:
  – communications (e.g. Internet connection)
  – a user interface
Access control with SPD/biometrics

usual scheme  
with SPD/biometrics

1. Access request  
   Identification request  
   Identification in Progress  
   Access granted

1. Access request  
2. Identification request  
3. Identification  
4. Access granted

Scenarios

- **Electronic health**
  - SPD used for storing lifelong health information (exams...)
  - SPD as access point to Electronic Health Record (EHR)
  - Supports normal use (visit to doctor, surgery) and emergency

- **University campus**
  - SPD used for (physical) access control and
  - authentication into campus services (canteen, library, web site,...)
2. SHUTTLE: CLOUD INTRUSION RECOVERY

Shuttle’s objective

- Recover PaaS applications’ state integrity when there are intrusions
Backups?

- Works but removes both bad and good operations
- Shuttle: removes bad (tainted) operations but keeps good operations

Platform as a Service (PaaS)

- Cloud service = to run applications
- Consumer develops application to run in that environment, using
  - Supported languages, e.g., Java, Python, Go, PHP
  - Supported components, e.g., SQL/noSQL databases, load balancers
Shuttle intrusion recovery service

• Features:
  – Supported by the cloud: available without setup
  – Removes the intrusion effects in the applications’ state
  – Supports applications deployed in various instances
  – Avoids application downtime
  – Cost effective
  – Recovers fast

Shuttle architecture

User requests

Legend:
- Scanning
- User Requests
- Replay Requests
- Control Messages
Replay Process

1. Identify the malicious operations (not part of Shuttle)
2. Start new application and database instances
3. Load a snapshot previous to intrusion instant
   Create a new branch; keeps the application running in previous branch
4. Replay requests in new branch
5. Block incoming requests; replay last requests
6. Change to new branch; shutdown unnecessary instances

Replay Modes

- **Full-Replay**: Replay every operation after snapshot
- **Selective-Replay**: Replay only affected (tainted) operations
- **Serial**: Replay all dependency graph sequentially
- **Clustered**: Independent clusters can be replayed concurrently

<table>
<thead>
<tr>
<th>Clustering Method</th>
<th>Full-Replay</th>
<th>Selective-Replay</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Cluster (Serial)</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Clustered</td>
<td>✔</td>
<td>✗</td>
</tr>
</tbody>
</table>
Evaluation Environment

- Amazon EC2, c3.xlarge instances, Gb Ethernet
- WildFly (formely JBoss) application servers
- Voldemort database
- Ask Q&A application; data from Stack Exchange

Performance overhead evaluation

- in normal execution

<table>
<thead>
<tr>
<th></th>
<th>Workload A</th>
<th>Workload B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shuttle</td>
<td>6325 ops/sec [5.78 ms]</td>
<td>15346 ops/sec [3.62 ms]</td>
</tr>
<tr>
<td>No Shuttle</td>
<td>7148 ops/sec [5.07 ms]</td>
<td>17821 ops/sec [3.01 ms]</td>
</tr>
<tr>
<td>overhead</td>
<td>13% [14%]</td>
<td>16% [20%]</td>
</tr>
</tbody>
</table>
Recovery time

• for 1 million requests

CONCLUSION
Conclusion

• Intrusions may happen in mobile devices
  – SPD, a novel device for authentication and data protection
  – Data physically isolated, protected with biometrics
• Intrusions may happen in the cloud
  – Shuttle, a recovery service for PaaS offerings
  – Leverages the resource elasticity and pay-per-use model to reduce the recovery time and costs

THANK YOU
HTTPS://WWW.PCAS-PROJECT.EU
HTTPS://GITHUB.COM/DNASCIMENTO/SHUTTLE