Project PCAS at a glance

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

1	INESC ID - INSTITUTO DE ENGENHARIA DE SISTEMAS E COMPUTADORES, INVESTIGACAO E DESENVOLVIMENTO EM LISBOA	INESC ID - INSTITUTO	Portugal
2	מ"עב שדח קפוא ס"וא	OS	Israel
3	UNIVERSIDAD POLITECNICA DE MADRID	UPM	Spain
4	NORSK REGNESENTRAL STIFTELSE	NORSK REGNESENTRAL S	Norway
5	COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	CEA	France
6	MAXDATA-INFORMATICA LDA	Maxdata	Portugal
7	AFCON CONTROL & AUTOMATION LTD	AFCON CONTROL & AUTO	Israel

Personalised Centralized Authentication pcas

2

Schedule

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

3

1. SECURED PERSONAL DEVICE

4

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

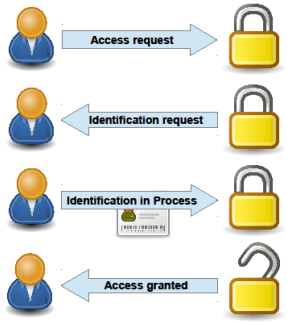
SPD sketches

Role of the smartphone

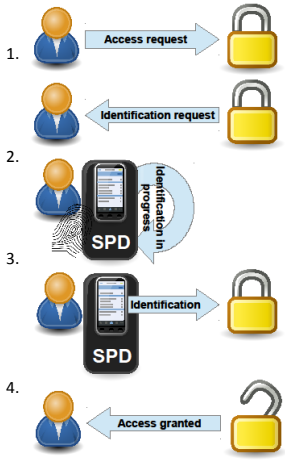
- SPD has to communicate with trusted (cloud) services
- Smartphone provides the SPD:
  - communications (e.g. Internet connection)
  - a user interface

Access control with SPD/biometrics

usual scheme



with SPD/biometrics



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

Personalised Centralized Authentication pcas

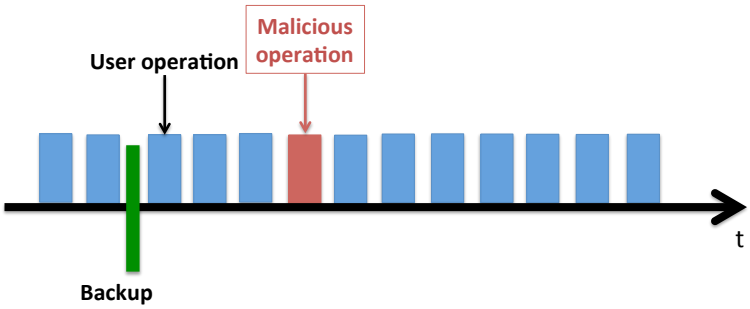
11

Shuttle's objective

- Recover PaaS applications' state integrity when there are intrusions

12

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

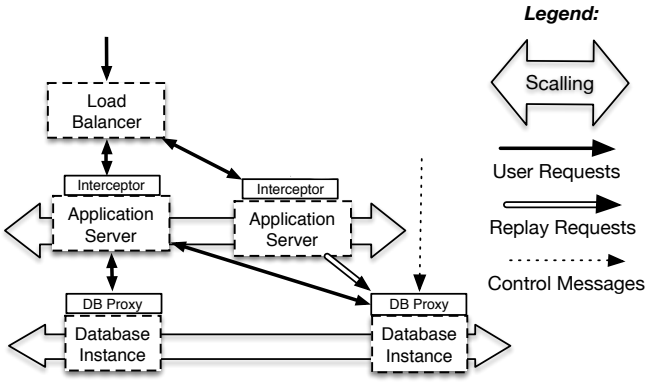
- Features:
  - Supported by the cloud: available without setup
  - Removes the intrusion effects in the applications' state
  - Supports applications deployed in various instances
  - Avoids application downtime
  - Cost effective
  - Recovers fast

Personalised Centralized Authentication pcas

15

Shuttle architecture

User requests



16

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

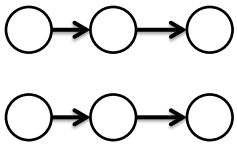
Personalised Centralized Authentication pcas

17

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



	Full-Replay	Selective-Replay
1 Cluster (Serial)	✔	✔
Clustered	✔	✗

Personalised Centralized Authentication pcas

18

Evaluation Environment

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

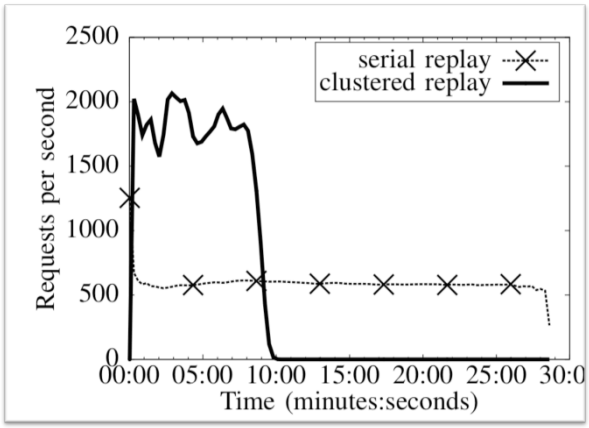
Performance overhead evaluation

- in normal execution

	Workload A	Workload B
Shuttle	6325 ops/sec [5.78 ms]	15346 ops/sec [3.62 ms]
No Shuttle	7148 ops/sec [5.07 ms]	17821 ops/sec [3.01 ms]
overhead	13% [14%]	16% [20%]

Recovery time

- for 1 million requests



Personalised Centralized Authentication pcas

21

CONCLUSION

Personalised Centralized Authentication pcas

22

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