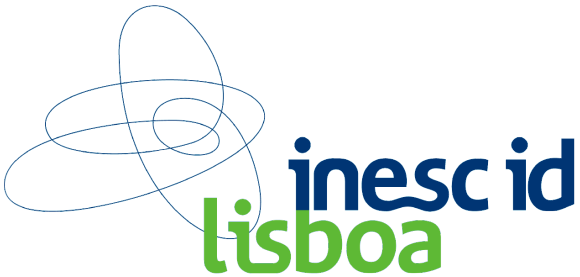
Recovery from Security Intrusions in Cloud Computing

Shuttle: Intrusion Recovery in PaaS

Dissertation to obtain the Master Degree in
Telecommunications and Informatics Engineering

TÉCNICO
LISBOA



Dário Nascimento

68210 - MERC
Instituto Superior Técnico
Universidade de Lisboa

Supervisor:

Prof. Miguel Pupo Correia

TÉCNICO LISBOA

Agenda

1 Motivation

2 Related Work

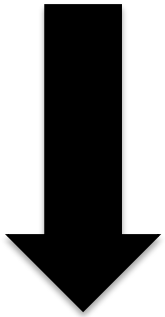
3 Proposed Solution
Goals
Architecture

4 Conclusion
Evaluation
Schedule
Conclusion

TÉCNICO LISBOA

Motivation

Number of **critical applications** in Cloud is **increasing**



Number of **Intrusions** in Cloud is **increasing**

Motivation

Reasons:

- Sofware Flaws (e.g. Shellshock)
- Configuration and usage mistakes (malicious or accidental)
- Corrupted legitimate requests (e.g. SQL-Injection)

Compromise:

- Integrity
- Availability
- Confidentiality

TÉCNICO LISBOA

Problem statement

Intrusions happen in cloud applications!

Goal

Recover the application's integrity when intrusions happen

Related Work

- **Operating Systems:** Taser, Retro
- **Databases:** ITDB, Phoenix
- **Web-Services:** Goel et. al, Warp, Aire, Undo for Operators

Issues:

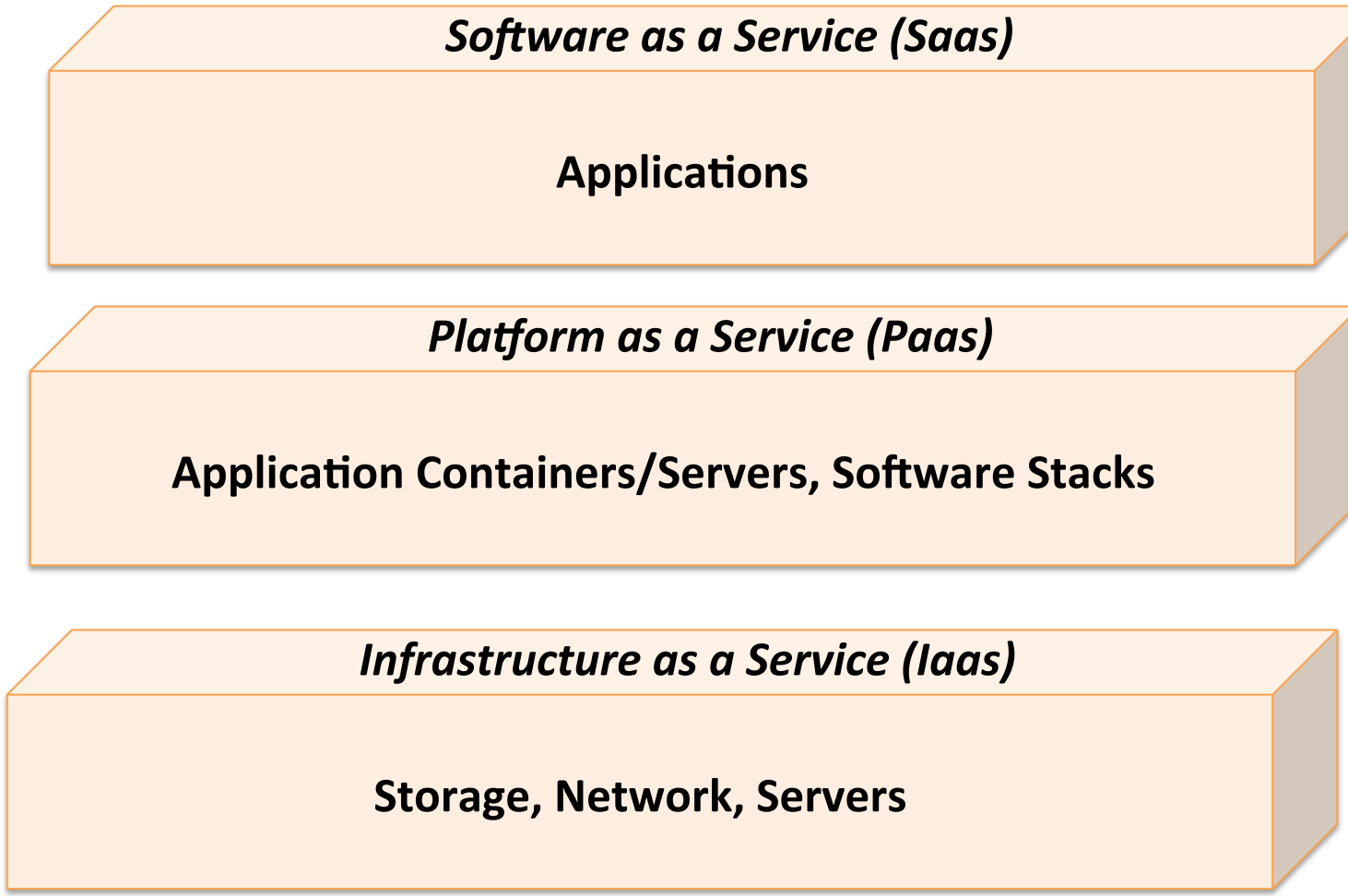
- All require setup and configuration
- Limited to 1 application servers and 1 database instance
- Cause application downtime during the recovery process

Challenges

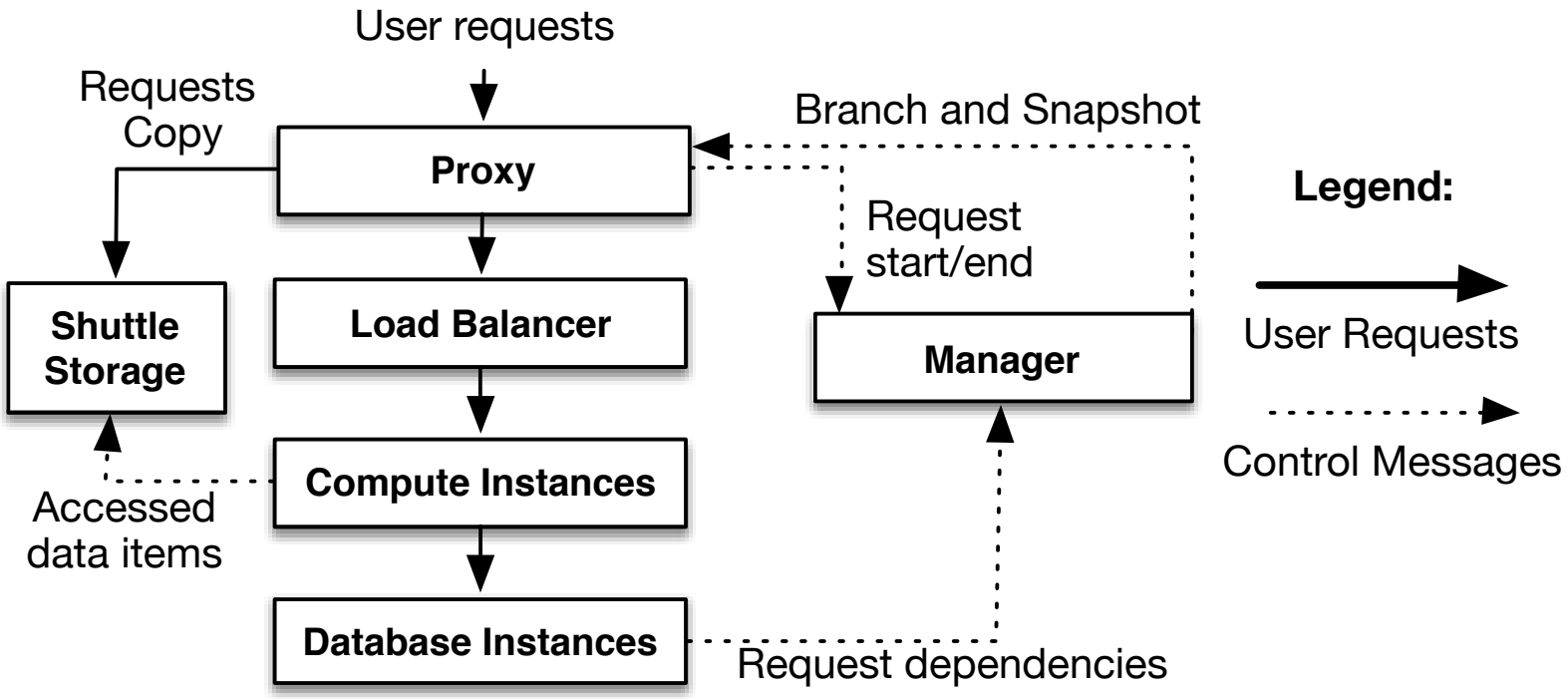
Develop an Intrusion Recovery system for Cloud Computing

- Remove the intrusion effects
- Support applications deployed in various instances
- Available without setup
- Avoid application downtime
- Cost efficient
- Recover timely

Architecture



Normal Execution



Replay Process

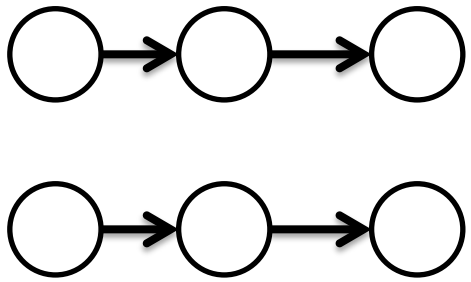
1. Identify the intrusion actions
2. Create new application and database instances
3. Load a snapshot previous to intrusion instant
   (create a new branch)
4. Order requests by their start instant during first execution
5. Replay requests
   1. Database operations shall replay in same order as original
6. Block the incoming requests
7. Replay the requests retrieved during the replay process
8. Change branch

Architecture

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

Full-Replay: Replay every operation after snapshot
Selective-Replay: Replay only affected (tainted) operations

Serial: Consider all dependency graph as a cluster
Clustered: Independent clusters can be replayed concurrently



Evaluation

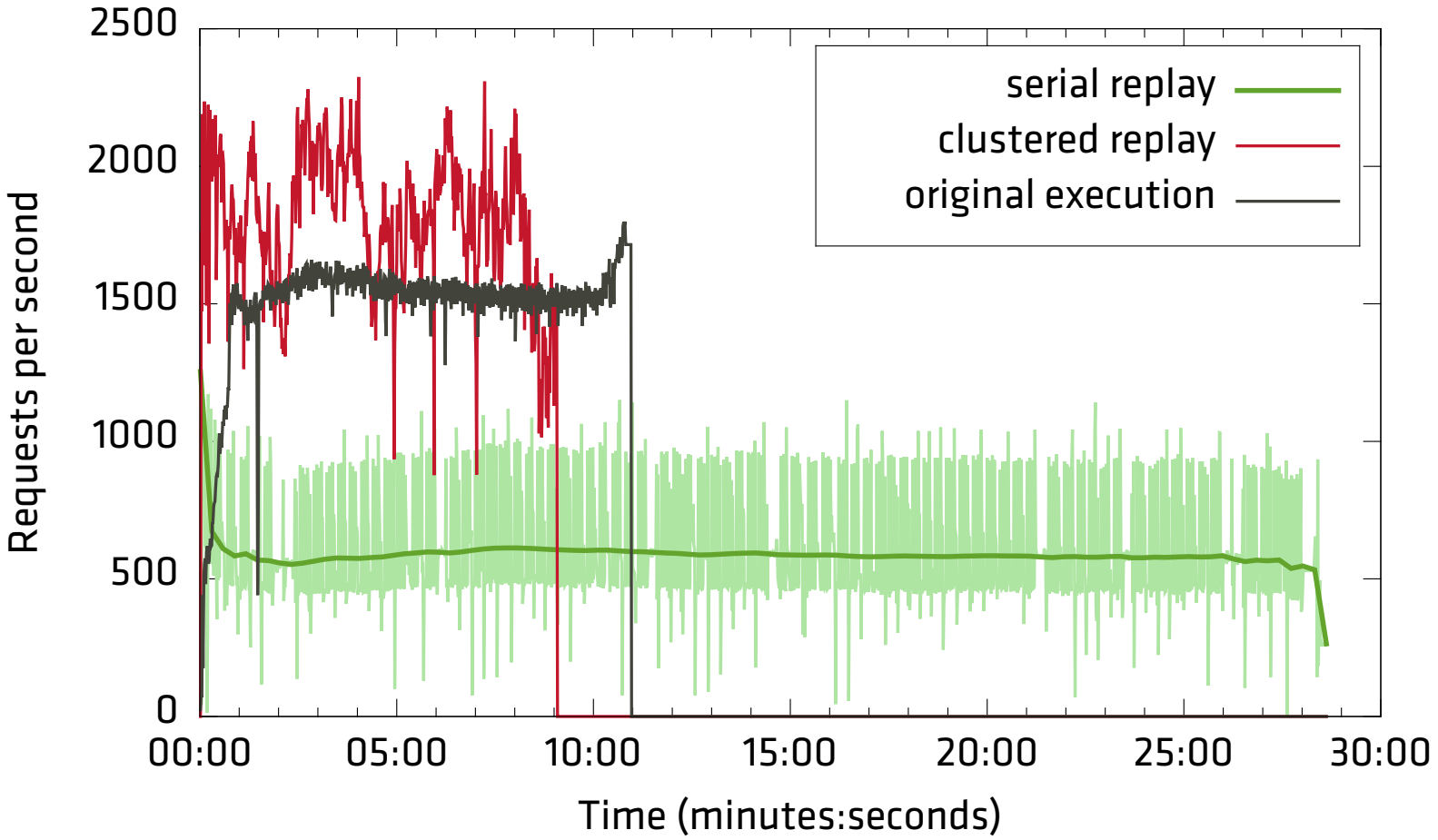
Accuracy: *Intrusion Scenarios:*

1. Malicious requests
2. Software vulnerabilities
3. External Channels

	# Intrusion	# tainted	# Selective Replay	# Full Replay
1a	106	0	< 605	> 38 620
1b	58	14	< 379	> 38 620
1c	48	52	< 253	> 38 620
2a	4 338	0	-	> 38 620
2b	18 286	1 278	-	> 38 620
3	> 2 000	-	-	> 38 620

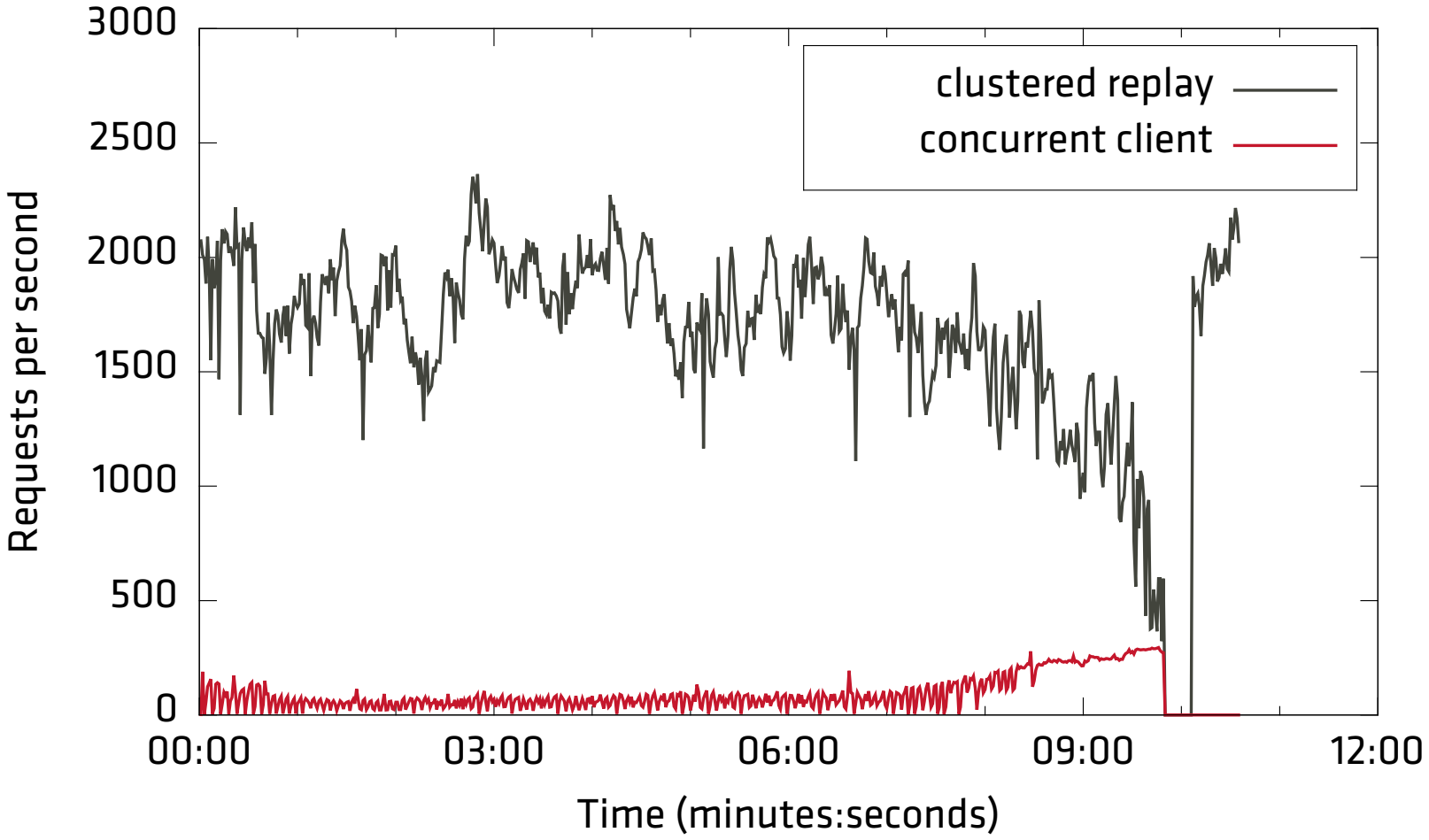
Evaluation Performance

Application deployed in Amazon Web Services



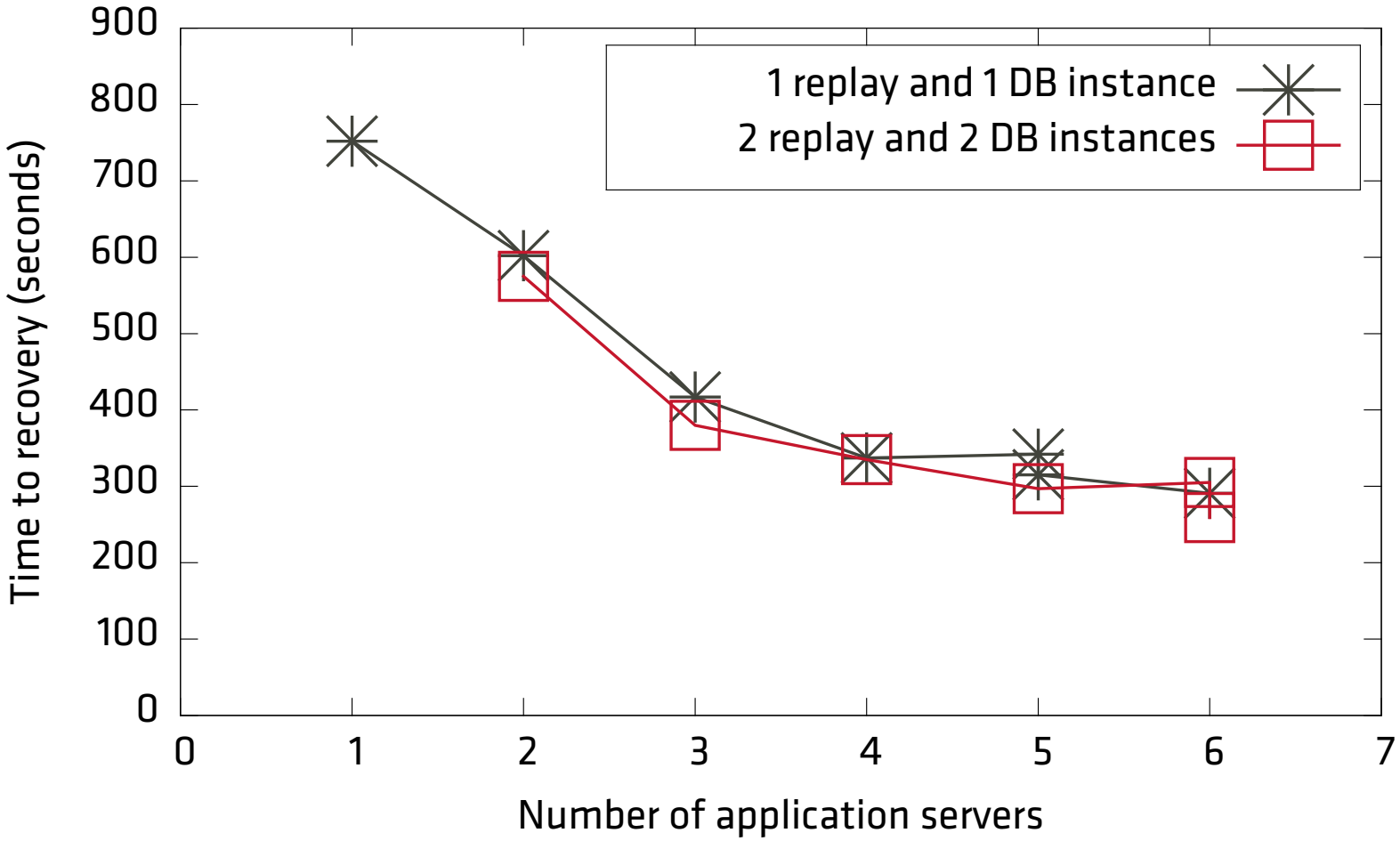
Evaluation Performance

Restrain Duration



Evaluation Performance

Scalability



Conclusions

- New intrusion recovery service integrated in PaaS
- Supports applications running in various instances backed by distributed databases;
- Order the replayed user requests considering their accesses to databases;

Conclusions

- Accomplishing intrusion recovery without service downtime using a branching mechanism;
- Leveraging the resource elasticity and pay-per-use model to reduce the recovery time and costs;
- Globally transaction-consistent snapshot of for NoSQL databases;
- Remove intrusions by redeploy the applications;

TÉCNICO LISBOA

Future Work

- Eleger as mais importantes (com o professor)

TÉCNICO LISBOA

Publications

- Published in my computer

References

[Taser] A. Goel, K. Po, K. Farhadi, Z. Li, and E. de Lara, "The taser intrusion recovery system," in SOSP. ACM, 2005.

[Retro] T. Kim, X. Wang, N. Zeldovich, and M. F. Kaashoek, "Intrusion recovery using selective re- execution." USENIX, 2010.

[ITDB] P.Liu, J.Jing, P.Luenam and Y.Wang, "The design and implementation of a self healing database system," Journal of Intelligent Information Systems, vol. 23, no. 3, Nov. 2004.

[Goel] I. Akkus and A. Goel, "Data recovery for web applications," in DSN. IEEE, Jun. 2010, pp. 81–90

[Warp] R. Chandra, T. Kim, and M. Shah, "Intrusion recovery for database-backed web applications," in SOSP. ACM, 2011.

[Aire] R.Chandra, T.Kim and N.Zeldovich, "Asynchronous intrusion recovery for interconnected web services," in SOSP. ACM, 2013.

[UndoForOperators] A. B. Brown and D. A. Patterson, "Undo for operators : Building an undoable e-mail store," in USENIX ATC, 2003.

TÉCNICO LISBOA

Thank you for your attention

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA

TÉCNICO LISBOA