Towards Mobile Cloud Security Performance: A Cross-Border Approach

Theodoros Mavroeidakos[1] , Dimitrios Kallergis[2] , Dimitrios D. Vergados[2] and Christos Douligeris[2]

[1]National Technical University of Athens, Greece
Email: el10807@central.ntua.gr

[2]University of Piraeus, Greece
Email: (d.kallergis, vergados, cdoulig)@unipi.gr

ICT2016
23rd International Conference on Telecommunications

Outline

Introduction

What happens today?

- Security performance challenges deter organizations and companies from exploiting the full benefits of Cloud Computing (CC).
- The security mechanisms and methods of CC differ from the ones in legacy environments and their efficiency has been heavily contested.
- Data flow across borders brings out significant law and regulatory challenges for cloud providers and consumers.
- More information is transferred by Mobile Devices remotely to CC environments.

How can these challenges be overcome in a CC environment?

Motivation

- This work aims at addressing the issue of cloud security performance and the significance of Service Level Agreements (SLAs) as well as the security challenges that are presented during a Cross-Border data flow.
  - The **security** and **privacy** of a CC environment are determined by the SLA that is applied during a cross-border transaction of data through the definition of the appropriate Service Level Objectives (SLOs).
  - The importance of the **security perspective** of an SLA is identified when Personally Identifiable Information (PII) are managed in a CC environment.

What is the impact of Cross-Border Regulations
on the security of PII in CC?
and
How safe are the Cross-Border Regulations?

Cross-Border Scenario

Theoretical Background:

- In this scenario a collaboration between a data controller such as a company or a governmental authority and a Cloud Service Provider abroad takes place.
- The SLA that supervises the collaboration is determined by the national legislation of the data controller.
- The SLA consists of four SLO categories that cover:
  - Functionality
  - Service Security
  - Data Management
  - Data Protection
- Priority will be given to SLOs so as to secure the end-service and the collected data.

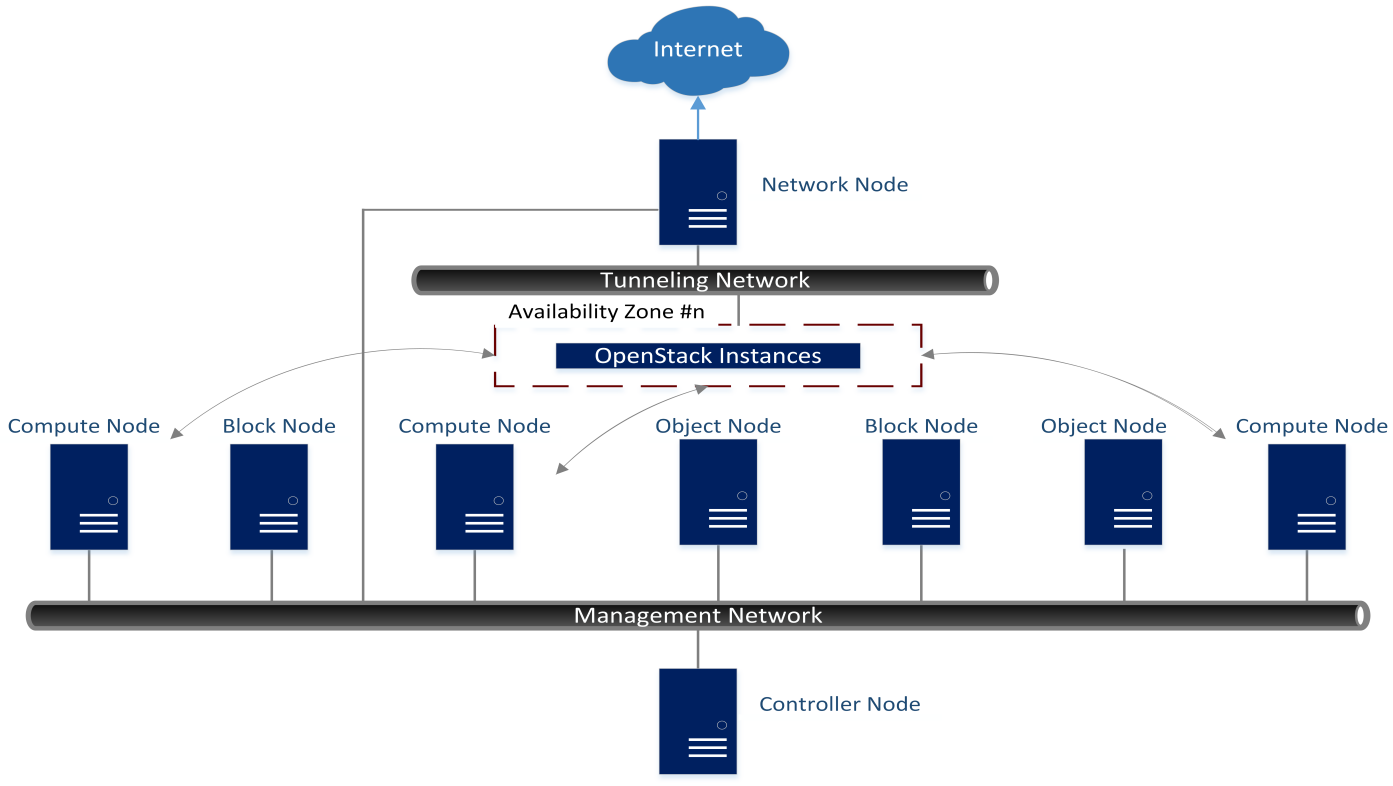
Cross-Border Scenario

Practical Approach:

Abstract presentation of the Cross-Border Scenario

Cross-Border Scenario

Custom OpenStack Environment:

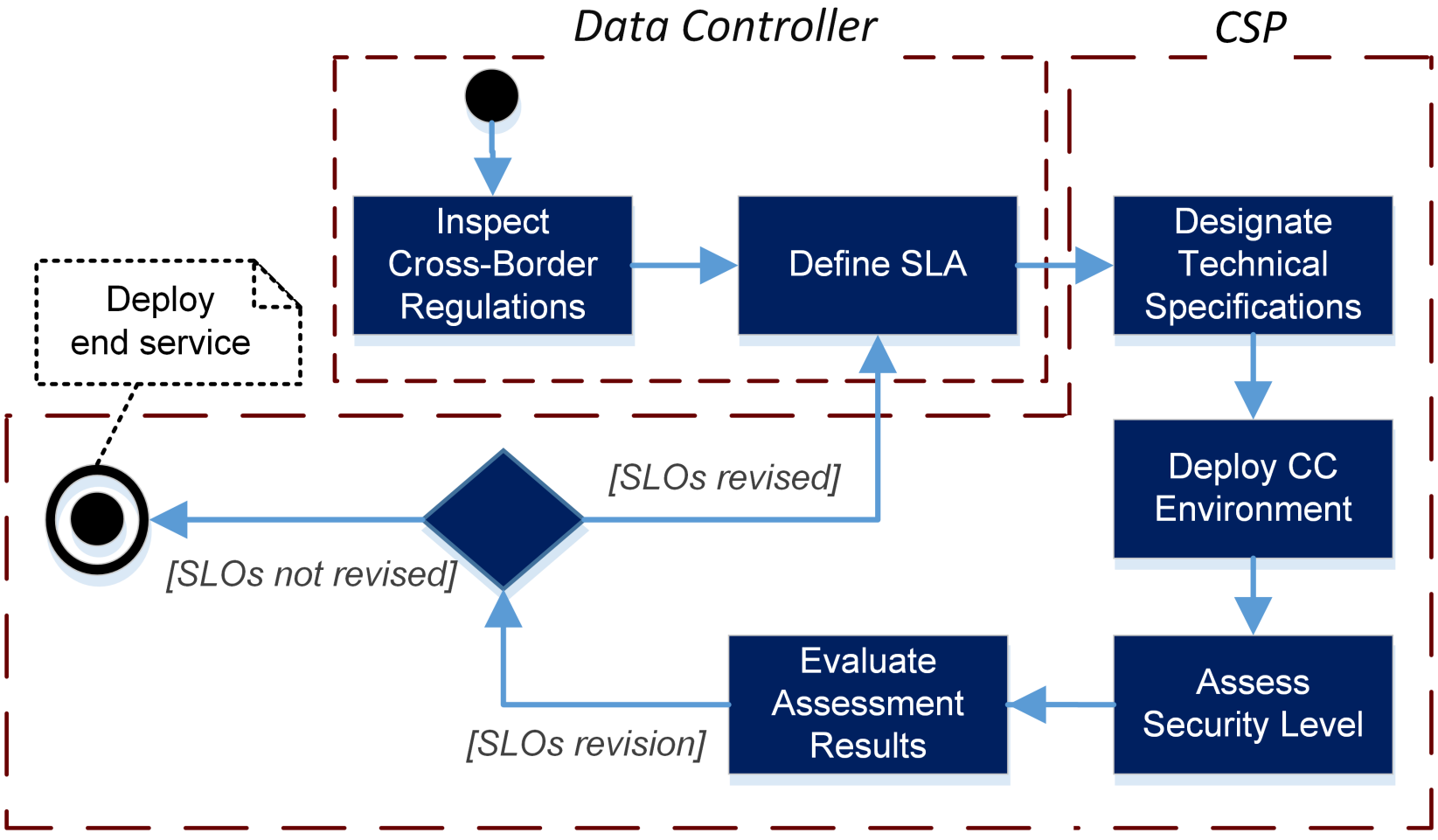


CSP's Environment

- The simulated CC infrastructure of the CSP developed using OpenStack and its operations were conducted according to the defined SLA.

Cross-Border Scenario

Scenario Analysis:



Activity Diagram of the Data Controller-CSP collaboration.

Security Assessment

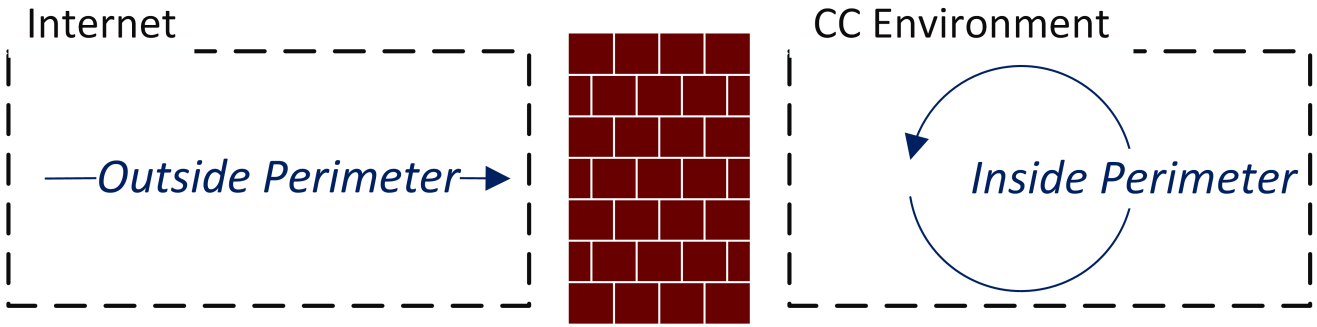
Methodology:

- The scope of the security assessment is to define the minimum information the attacker could gain so as to exploit the cloud boundary.
- The aggregation of the assessment results leads to the vulnerabilities definition that can be leveraged for exploitation.
- In the OpenStack environment, many computing entities with different characteristics interact and various technologies are combined (e.g., RPC-SDN), creating a diversity of vulnerabilities.
- A wide spectrum of tools and methods are orchestrated in order to identify the vulnerabilities and the attack vectors in the context of this security assessment.

Security Assessment

The Cloud Boundary is divided into:

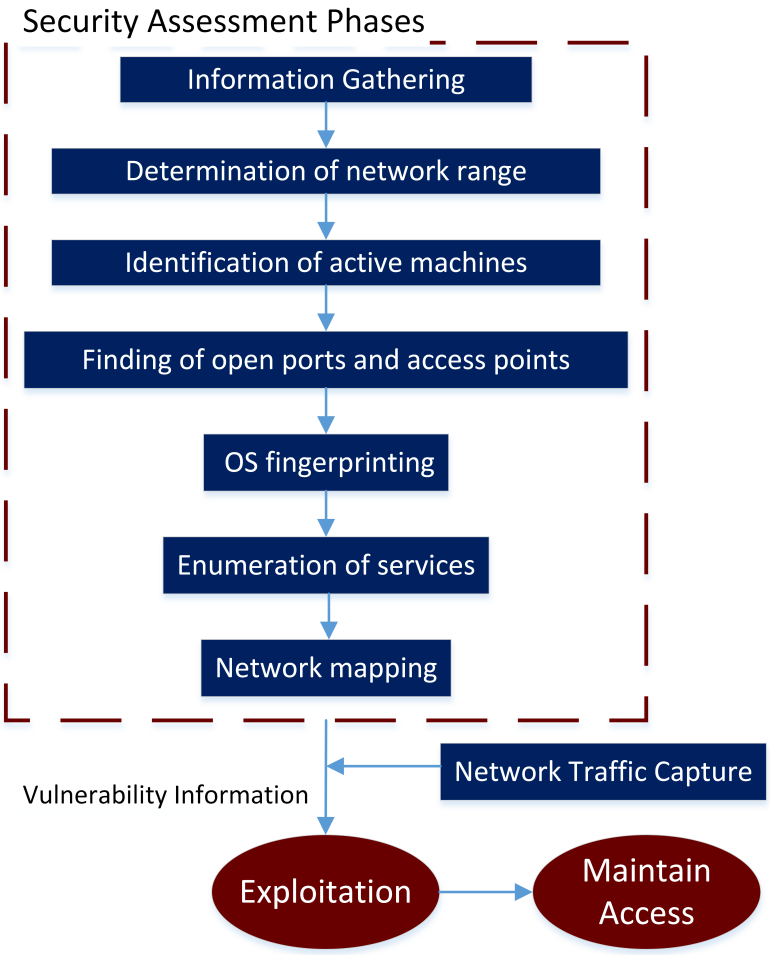
- The **Outside Perimeter** (and the Mobile Devices) extends among the computing entities that are visible to the end-users.
  - There exist limited PIIs and information about specified CC systems.
- The **Inside Perimeter** (and the Controller Node) extends among the intranets of the environment.
  - There exist PIIs and critical operational data.



Inside and Outside Perimeters

Security Assessment

- The security assessment phases are necessary to identify the environment's vulnerabilities.



Security Assessment Phases

Security Assessment

The Inside Perimeter and the Controller Node:

- The captured network traffic reveals that the attacker acquires access to critical data about the CC environment and the PII.
- The Controller Node has a critical vulnerability that allows ntp reflection and a DoS attack to a spoofed IP address inside the CC environment.
- The CC administration dashboard is vulnerable to a vector of attacks that allows password attacks.
  - The dashboard is only visible inside the CC environment and it is used for the configuration of the end-service delivery.
- The importance of the insider threat is identified due to the combination of the particularities of this type of environment and the impact of the attacks.

Security Assessment

The Outside Perimeter and the Mobile Devices:

- A DoS attack performed on the loadbalancer IP address of an Availability Zone may lead to resource exhaustion and damage the end-service availability.

Mobile Cloud Computing (MCC) Assessment:

- By reverse engineering the mobile application, a rogue client was created, obtaining access to a legitimate user's data.
- An HTTP POST flood attack performed by the mobile devices aimed at the loadbalancer's IP address.
  - This attack caused the addition of a delay overhead and triggered the CC defense mechanisms.

Results Evaluation

The SLA used is **mainly** responsible for the existence of the identified vulnerabilities.

- The internal and external DoS attacks affected the SLOs namely the reliability, incident management and responsibility.
- The network traffic capture affected the SLOs namely the integrity, confidentiality and monitoring.
  - Therefore the PIIs and CC operational information are exposed.
- The majority of OpenStack services can not be exploited due to the operations performed by the SLO; vulnerability management.

Results Evaluation

MCC assessment results evaluation:

- The security challenges of MCC are not completely and suitably addressed through the SLA when the Mobile Devices behave as thin clients.
- The only countermeasures against attacks by the MDs are the CC defense mechanisms without specific customization.
- The SLA lacks mobile application guidelines concerning the client validation in order to avoid events such as rogue clients.

Conclusions

Synopsis

The used methodology aimed to:

- **assess** a cloud-based service which also uses mobile devices
- **determines** the outcome of a case in which the underlying environment is constructed based on the SLA, and
- **proposes** the revision of SLOs so as to improve the security level.(e.g., the critical time to deploy redundant systems)

- Cross-Border regulations that determine the creation of an SLA do not take into consideration the underlying environment that processes and manages the data.
- The compliance of the SLOs by the CSP should be continuously evaluated by the data controller through appropriate metrics.

Conclusions

- The Cross-Border regulations that are used to define the SLA force the CSP to operate legally but without adequate security constraints.

Future Work!

- Work needs to be done on Governmental or Regional legislation to strengthen the Cross-Border guidelines for the transfer of PII in the context of CC.
- A Unified Contract (UC) should be developed to ease the adoption of MCC environments by the mobile phone market and to sufficiently address the related security challenges.

23rd International Conference on Telecommunications
16-18 May 2016, Thessaloniki, Greece

IEEE

IEEE COMMUNICATIONS SOCIETY

ALEXANDER TECHNOLOGICAL EDUCATIONAL INSTITUTE of THESSALONIKI
Departments of Informatics & Electronics Engineering

Thank you for the attention!
Questions?

UNIVERSITY OF PIRAEUS RESEARCH CENTER

ICT2016
23rd International Conference on Telecommunications