CMU-PT/RNQ/0015/2009

Trustworthy and Resilient Operations in a Network Environment

TRONE

Deliverable D1

Use-Case Scenarios Analysis

Information and Communication Technologies Institute
Carnegie Mellon | PORTUGAL
AN INTERNATIONAL PARTNERSHIP

Executed by: **SRC**

Direction/Department: **DTI**

Date: **07-07-2011**

Version Number	Owner	Change Control	Date
1.0	DTI SRC	Document creation with first draft of Use Case Scenarios	07-01-2011
1.1	DTI-SRC	Second iteration for the use case scenarios	18-02-2011
1.2	DTI-ARS	Diagrams for the Use Case Scenario	18-03-2011
2.0	DTI-ARS	Final Structure of the Document	06-04-2011
2.1	FCUL	Revised structure and updated sections	28-04-2011
2.2	FCTUC	Revised text	30-05-2011
2.3	DTI-ARS	Final revision	07-07-2011

Index

Executive Summary

This project aims to develop a series of techniques and algorithms that can be applied to a particular scenario inside the Portugal Telecom network and services. These techniques and algorithms should improve resiliency and guarantee the needed trustworthiness in the particular scenario identified by PT.

This document introduces the Use Case Scenario evaluated by Portugal Telecom for the TRONE project, chosen to be the one that the academic affiliates are going to work with. The presented scenario results from a study in which different scenarios were evaluated. Therefore, this document represents the refined version of several working versions that were "living" statements regarding PT security issues that could be addressed during this project evolution.

From an initial list of 4 Use Case Scenarios, with a brief risk analysis for each, the project research team chose the one that is presented in this document. The chosen scenario implies an analysis regarding the risk associated to it, which is also included in this document.

It is intended that this document is seen as a starting point, a basis for work to be developed ahead in the project. Therefore, it should not be seen as a closed statement, but rather as an open and evolving reference, to be improved with inputs coming from the research teams. According to the workplan, prototypes will be developed and it is expected that they will be matched against the use case scenario described in this document. Therefore, by the end of the project there will be a new document building on the present one, but which will include descriptions of the prototype(s) that were developed to address the challenges initially described. Additionally, test beds and benchmark results should also be included in that final document.

This deliverable is structured as follows. After a brief introduction, we provide a short description of the initial use cases that were considered, and from which we made the exercise of selecting a PT use case for TRONE. Then, we present the selected scenario with the threats roughly identified, as well as the main controls that traditionally could be deployed to minimize the risk associated to the threats. The following chapter provides a brief risk analysis for the identified threats, with a special focus on the business impact that each vulnerability or threat would create if exploited and the probability of the exploitation that we consider. Finally, we present some conclusions and future steps for the project.

1 Introduction

As stated before, this document had a first version (with other two subversions) that introduced 4 use case scenarios. From these 4 scenarios we decided to group the first two and came up with this final scenario that had also received a “problem” (or a challenge) from the third one. Portugal Telecom chose to present all 4 initial scenarios focusing on the cloud computing environments. This choice stood on two major reasons:

1. Cloud computing environments will be in the next few years the hottest topic in Portugal Telecom services portfolio (altogether with the IPTV infrastructure, which nonetheless will have a major development with future projects regarding the utilization of the cloud computing infrastructures owned by PT;
2. Cloud computing is currently a reality inside PT and it would be easy to have live data from that infrastructure and could also be feasible to own a couple of virtual machines in order to run tests and pilots of the proposed techniques and algorithms.

This final case scenario represents several issues that may appear in the present moment, but could also be exploited in the very near future. This scenario raises a large number of theoretical and practical issues, and also requires that the reference architecture is designed to mitigate some (still) *unknown* issues and to deal with a challenge that future services retrieved by PT from this infrastructure will have the auto-provisioning of the infrastructure to guarantee the correct resources to each customer.

The academic affiliates should be able to successfully introduce knowledge in the final scenario, to increase its final value. A PoC (proof-of-concept) should be created or even a pilot of, if not all, pieces of the developments in order to fully demonstrate the validity of this project both for the academic affiliates and the industrial partner.

2 Initial Use Case Scenarios

In this section we briefly present the use case scenarios initially considered in the study. We considered four different scenarios that could serve as the basis for the remaining work in this project. We include only the main descriptions that are necessary to set the scope and reach of each scenario. Since PT first presented these scenarios we also noticed that some of them were intertwined. Furthermore, nearly all of the scenarios would also have some points of interest for the research teams involved. This motivated us to go for a scenario comprising more than one of the initial proposals. In this section, we overview these initial proposals.

2.1 Scenario 1 – Cloud Computing Operations Environment

This scenario concerned the infrastructure for PT cloud, as the request for cloud resources was growing quickly, not only from the outside, but also from the inside of PT. The idea was to deploy a complete new infrastructure for cloud computing services based on VMware (virtualization), Cisco (network and security) and EMC (storage) technologies. The main concern in this scenario lies in possible attacks to the hypervisor, rendering the entire physical machine, as well as other guest machines vulnerable to malicious users.

2.2 Scenario 2 – Cloud Computing Attacks and Intrusions

In the second scenario, the challenge was to prevent a different form of attack, where malicious users may take advantage of existing resources in the cloud to attack other parts of the network (or of the cloud itself).

2.3 Scenario 3 – Network Orchestration Hazards

This scenario takes as its starting point the existence of network orchestration programs that allow a dynamic provision of Cloud services for costumers (internal and external to PT), based on Business Processes Languages. However, the focus on this scenario would not be the construction of the orchestration itself, but rather the security of this facility, because malicious users could take advantage of this powerful feature to compromise some parts of the operation, namely order entry, billing or the network of the orchestration system itself.

2.4 Scenario 4 – Cloud Computing Resilient Infrastructure

This use case approaches the security issues in these environments in a preventive manner. Despite the existence of controls that monitor systems to identify threats and others that react to those threats, a lot can be gained from a sound, well-planned and structured resilient infrastructure.

The purpose is then to define how such an infrastructure should be built, which its essential components are and how they should interact with each other.

We could use wormholes or other approaches, like fault detectors to prevent different forms of attacks that could harm the normal operation of the infrastructure.

3 Consolidated Use Case Scenario Description

We decided to consolidate two of the scenarios and include a small part of the third one, to create a better use case scenario for the TRONE Project.

3.1 Final Use Case Proposal – Consolidated Cloud Computing Environment

Portugal Telecom's current cloud computing infrastructure is implemented on top of two different virtualization technologies: VMware ESX and Parallels Virtuozzo. The two actual infrastructures are becoming a scarce resource due to the amount of requests (both internal and external) currently being processed.

With this in mind PT is deploying a complete new infrastructure for cloud computing services based on VMware (virtualization), Cisco (network and security) and EMC (storage) technologies, which have the following reference architecture (Figure 1).

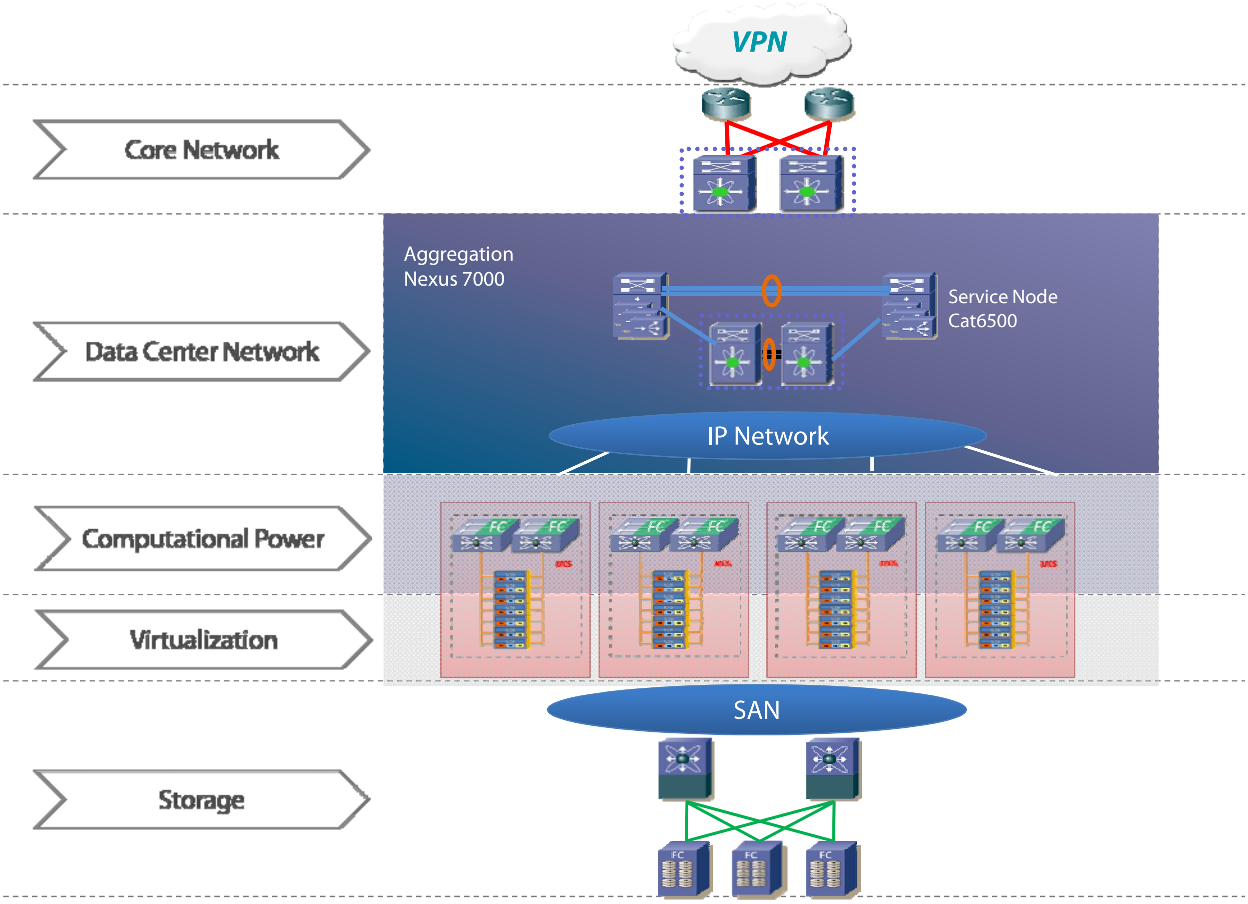

Figure 1 – PT Cloud Computing Reference Architecture

One of the biggest challenges in all these three infrastructures, security wise, is the ability to detect and eliminate threats against the operation of the infrastructure, the control plane. There are two main risks that we can anticipate: 1) the ability for an attacker to compromise the hypervisor and take control over the guest operating systems running in the same host, i.e., the virtualization layer in the reference architecture; 2) a malicious user uses our Cloud Computing infrastructure to execute a series of network attacks against the infrastructure or the outside world, i.e., by using the computational power layer. Other risks that can also be anticipated are:

- Service degradation (Layers: Core Network, Data Center Network, Computational Power and Storage)
- Monitoring faults (Layers: Data Center Network, Virtualization)
- Control disruption or failure (Layer: Virtualization)
- Other virtual machines being compromised (Layer: Virtualization)
- 3rd party (external) machines attacked
- Exploitation of segregation control failures of the shared resource (Layers: Data Center Network, Virtualization and Storage)

3.1.1 Scenario Threats

A malicious user which controls a guest machine in a virtualized environment is clearly the biggest threat agent. It can take control of that guest machine following an attack or pretending (and paying accordingly) to be a legitimate user of our virtualized services.

In Figure 2 we can see the different type of segregation at the virtualization layer in the reference architecture. This virtualization allows implementing up to 3-Tier application architectures within the provided infrastructure. In particular, it is possible to see the 3 typical tiers represented by the 3 depicted VLANs: Vlan-FE-Web-Cu1, corresponding to a Front-end Web for customer 1, Vlan-FE-App-Cu1, corresponding to a Front-end Application for customer 1 where the application logic and web services are provided and, finally, Vlan-BE-Cu1, corresponding to a Back-end network for customer 1, where database access is usually located. The customer can choose to have these 3 VLANs, but it could be just one or two.

In the figure it is also possible to observe four virtual switches (dVS1, dVS2, dVS3, vSwitch0) that allow segregating the different types of networks. Therefore, for instance both FE-App and BE networks run in the same virtual switch, while the FE-Web network is handled by a different virtual switch. Additionally, backup and virtual infrastructure management networks are connected into two other virtual switches.

This segregation presents several questions that can be treated as threats to the overall environment. For instance, the existence of just one firewall, which is a single point of failure, can be seen as one of those threats. Additionally, while segregation is positive for isolating networks with different criticality natures and levels of exposure to attacks, mitigating through contention the impact of a successful attack, it also introduces more complexity and additional points of attack. Other kinds of threats have thus to be considered, and one must not assume that the environment is safe just because segregation is implemented.

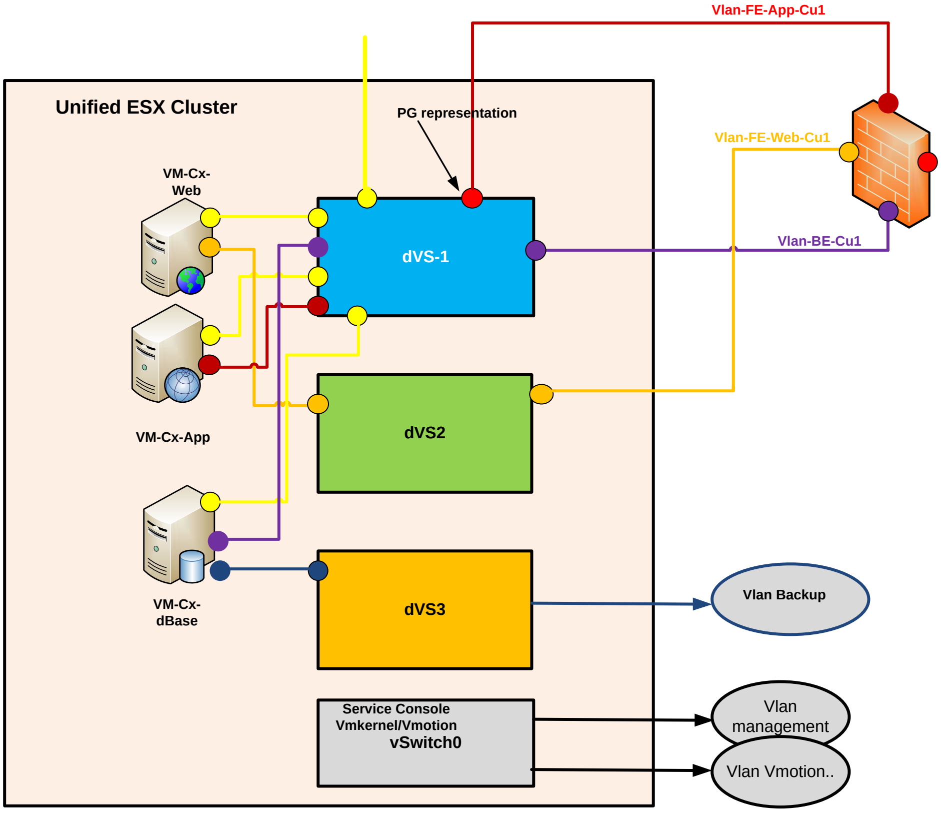

Figure 2 – Segregation at the Virtualization Layer

In general, several threats can be identified and grouped in some major type of threats:

- Threats against the hypervisor
- Threats against the virtualization platform
  - Reading memory space outside the range of her guest virtual machine
  - Privilege escalation in the virtualization environment
- Threats against the guest virtual machines
  - Taking control over other guest machines, without having control of the hypervisor
  - Service disruption or degradation in other guest virtual machines
- Threats against external machines or systems
  - Service disruption or degradation in systems outside the virtualization environment
  - Privileges escalation in systems that belong, or not, to the virtualized environment, and from this point on execute other type of malicious activity in the network
- Threats against the network and storage platforms
  - Attacks against the maximum number of IOPS allowed in the storage
  - Routing cache poisoning

- Threats against the deployed controls
    - Segregation controls are bypassed
    - Abusive use of the bandwidth allowed
    - Access to privileged data

3.1.2 Scenario Controls

The above threats can be detected, minimized or completely eliminated if we are able to implement a series of controls. Some of the controls can be chosen from the list below but some others need a complete analysis, study and research due to their nature, coverage and the potential impact in the business, both Portugal Telecom's business and our customers businesses.

- Characterization of the network usage profile for each guest virtual machine, with strong correlation procedures that can enable the discovery of covert channels, stealth attacks or control procedures that can command other systems to execute attacks;
- Closed monitoring of traditional attacks, i.e., resource exhaustion like CPU, Memory, Disk Space, etc.;
- Hypervisor monitoring and/or verification techniques in order to guarantee that it is executing correctly and without any strange behavior;
- Pro-active rejuvenation controls that can allow us to guarantee that a guest virtual machine is always behaving correctly.
- Use of IDS/IPS techniques in order to detect network attacks, i.e., signatures and heuristics based detection engines that can detect attacks or attempts to evade detection techniques;
- Implementation of active controls that can stop attacks or minimize them, e.g., application firewalls.

3.2 Orchestration Controls

In order to enrich this scenario we decided to include a small part of the orchestration scenario, as we're taking into consideration that these orchestration systems are relatively new. For PT Cloud Computing infrastructure it is very clear what the orchestration modules will execute:

- Deliver consistent task and workflow results, in order to implement a true end-to-end process automation
- Integrate easily with 3rd-party IT management applications, as some of the PT legacy systems, order entry applications, etc.
- Upgrade or change IT management applications without redesigning workflows, as the orchestration process will act as a "broker" for the entire system
- Improve quality of service, by improving the user experience and automate to the maximum the number of tasks the system need to execute in order to deliver the service

3.2.1 Orchestration Control Tasks

For this project, and concerning this very complex environment, we would like to receive two specific outputs:

- A reference architecture for the orchestration system to be resilient, both to faults and malicious users by defining an effective, accurate and realistic fault model and which are the proposals for this very important part of the Cloud Computing Global Infrastructure at PT.
- By choosing a specific, and simple orchestrator process used in PT's infrastructure we should be able to test this process (by using open source tools if needed), which should be used to validate the Reference Architecture previously defined. Several processes can be listed from a simple orchestration:
  - Controlling the order entry for the storage platform
  - Guarantee the effectiveness of the order entry and their correct implementation for the processing characteristics regarding hardware resources
  - Control of the images repository

4 Risk Analysis for the Case Scenario

4.1 Vulnerabilities in the scenario

In order to execute a risk analysis that cannot be in this moment very exhaustive we need to look at the list of major threats identified in 3.1.1. This list shows us the pre-identified major threats that a scenario as the one we depicted can have in the present or (in theory) in a near future. Also, and based on previous situations, we can predict that some threats can appear under new zero-day vulnerabilities:

Therefore we can group the vulnerabilities under three major groups:

- Known vulnerabilities (or that already existed at some point in time)
    - Threats against the virtualization platform
        - Reading memory space outside of the one allocated to her guest virtual machine
    - Threats against external machines or systems
        - Service disruption or degradation in systems outside the virtualization environment
        - Privileges escalation in systems that belong, or not, to the virtualized environment, and from this point on execute other type of malicious activity in the network
    - Threats against the network and storage platforms
        - Attacks against the maximum number of IOPS allowed in the storage
        - Routing cache poisoning
    - Threats against the deployed controls
        - Abusive use of the bandwidth allowed
        - Access to privileged data

- Theoretical vulnerabilities (under research or already existing to similar systems)
    - Threats against the hypervisor
    - Threats against the virtualization platform
        - Privilege escalation in the virtualization environment
    - Threats against the guest virtual machines
        - Taking control over other guest machines, without having control of the hypervisor
    - Threats against the deployed controls
        - Segregation controls are bypassed

- Zero-day vulnerabilities
    - Threats against the guest virtual machines
        - Service disruption or degradation in other guest virtual machines

4.2 Vulnerability exploitation probabilities of the scenario

The probabilities of exploitation of the vulnerabilities can have a direct correspondence to the list identified in the previous section, as known vulnerabilities (or already existing in some point in time) will have a greater probability of exploitation than the others (theoretical or zero-day). However in this section we want to present the probability as a product of the difficulty to explore the vulnerability and the "reward" (for the malicious user) of exploitation.

In these terms our analysis shows that:

- Threats against the hypervisor – Less to medium probability of exploitations
- Threats against the virtualization platform – Medium probability
- Threats against the guest virtual machines – Medium probability
- Threats against the network and storage platforms – Medium to high probability
- Threats against external machines or systems – High probability
- Threats against the deployed controls – High probability

4.3 Business impact

After the analysis of the possible vulnerabilities and correspondent exploitation we need now to define the importance of each piece of the infrastructure under this scenario. We identify this task as the business impact that having a problem in the infrastructure could cause to PT services, PT customers and PT brand reputations. Doing a "light" analysis our classification could lead everything to a major impact on the PT business for the cloud computing environment.

However, we want to clearly identify which parts of the infrastructure have the biggest impact in PT business and our analysis led us to the following classification:

- Major business impact (that could damage PT brand reputation and the continuation of selling services, as well as legal actions against PT)
    - Having the hypervisor compromised
- High business impact (that can affect PT brand reputation and may cause PT to lose existing customers and new sells)
    - Having the controls deployed compromised
    - Having the virtualization platform compromised
    - Compromised guest virtual machines
- Medium business impact (potential loss of existing customers or/and new sells of the service)
    - Having the network and storage platforms compromised or with severe problems
    - Use of PT cloud infrastructure to compromise external machines, systems or applications

5 Conclusion and Next Steps

We believe we found a very interesting setting for the work of this project. The consolidated scenario we presented owns a number of very interesting features: it uses technologies that gained a lot of importance in the last few years: virtualization and clouds. When used together, these promise to deliver better services and to save costs for clients. Therefore, not surprisingly, PT is putting a lot of stake in these technologies. Furthermore, we have been able to match this commercial interest of PT with the research interest of the academic partners, by defining real threats to architecture we defined here.

Our next step is to define a monitoring and control architecture for the service that allows us to observe and manage the system in a way that allows us to: i) detect and deter intruders; and ii) control the system, while simultaneously preventing intruders from doing the same.