Latin American Grid

Partnership for International Research and Education
A Global Living Laboratory for Cyberinfrastructure Application Enablement

LA Grid Summit 2011
November 3rd & 4th 2011
Florida Atlantic University

National Science Foundation

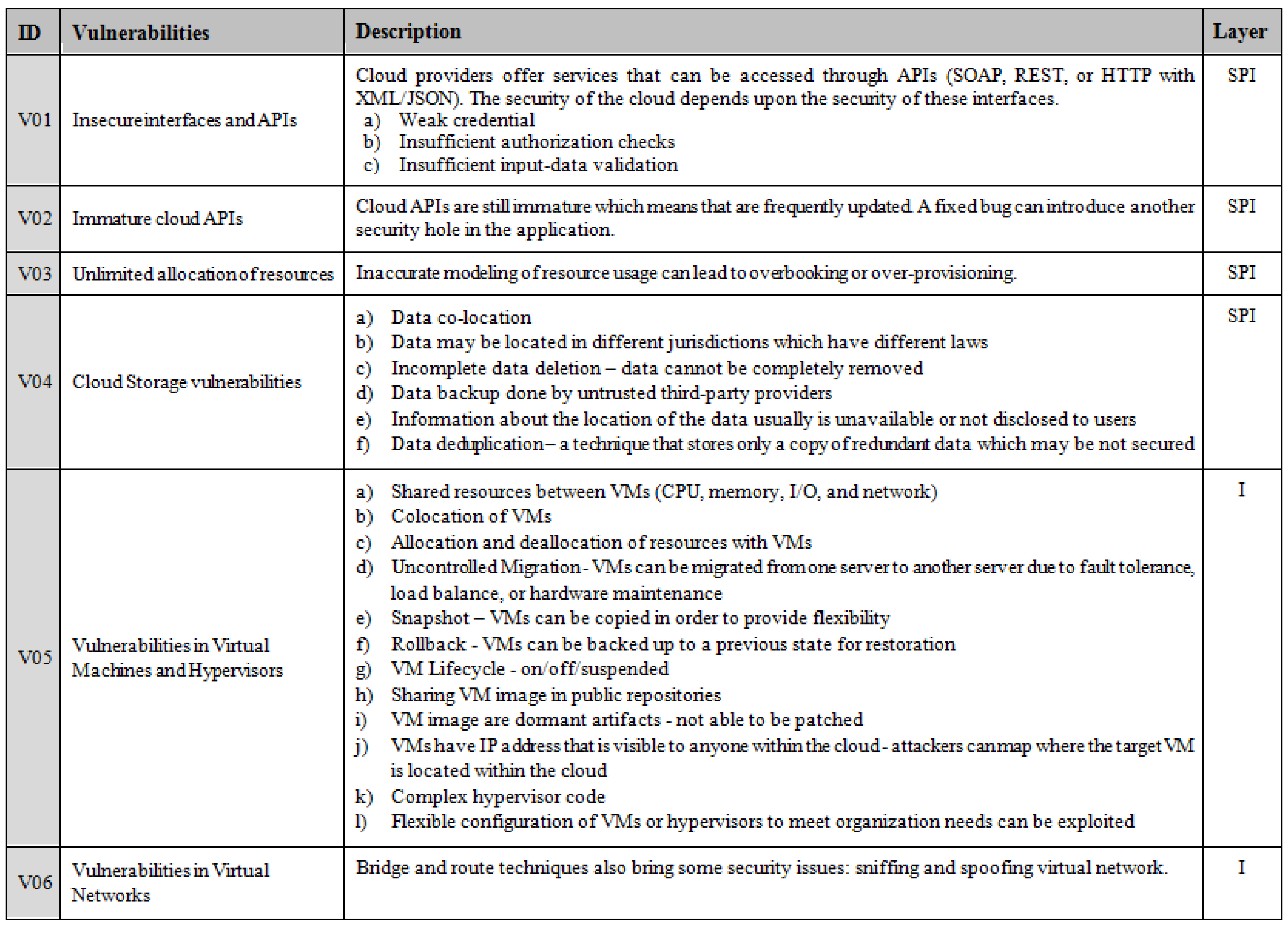
Security in Cloud Computing

Keiko Hashizume, PhD Student, Florida Atlantic University
FAU Advisor: Dr. Eduardo B. Fernandez, Florida Atlantic University
PIRE International Partner Advisor: Dr. Eduardo Fernandez-Medina, Universidad de Castilla-La Mancha

I. Research Overview and Outcome

Overview

- The importance of cloud computing is increasing and it is receiving a growing attention in the scientific community.
- Cloud computing combines a number of computing concepts and technologies such as SOA, Web 2.0, virtualization and other technologies with reliance on the Internet, providing common business applications online through web browsers to satisfy the computing needs of users, while the software and data are stored on the servers.
- Although there are many benefits to adopting cloud computing, there are also some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters.
- Security is the main obstacle for many organizations in their move to the cloud, related to risk areas such as external data storage, dependency on the “public” internet, lack of control, multi-tenancy and integration with internal security.
- In this work we present a categorization of security issues for Cloud computing focused in the so-called SPI model (SaaS, PaaS and IaaS), identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud computing and its environment.

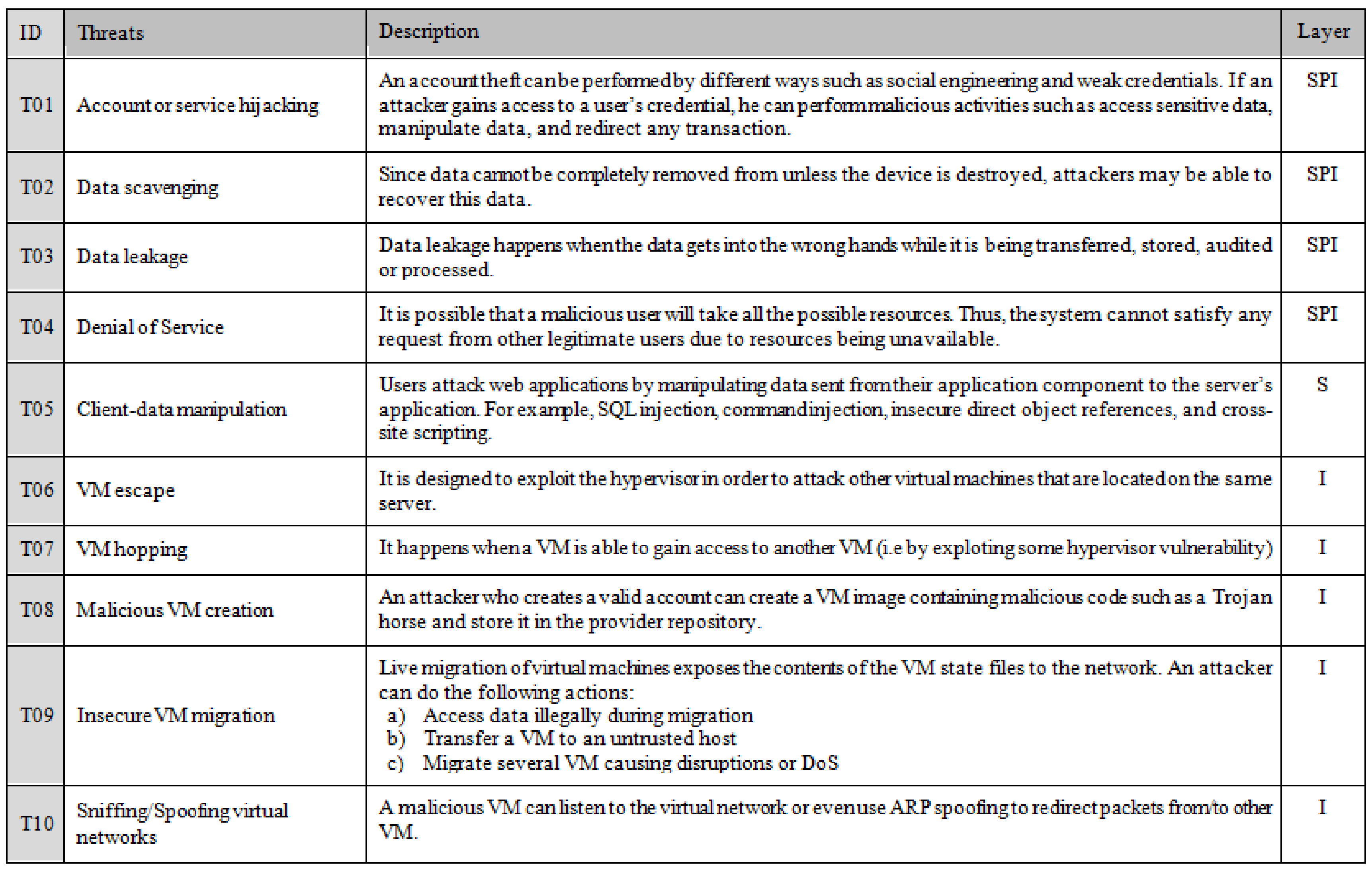


ID	Vulnerabilities	Description	Layer
V01	Insecure interfaces and APIs	Cloud providers offer services that can be accessed through APIs (SOAP, REST, or HTTP with XML/JSON). The security of the cloud depends upon the security of these interfaces. a) Weak credential b) Insufficient authorization checks c) Insufficient input-data validation	SPI
V02	Immature cloud APIs	Cloud APIs are still immature which means that are frequently updated. A fixed bug can introduce another security hole in the application.	SPI
V03	Unlimited allocation of resources	Inaccurate modeling of resource usage can lead to overbooking or over-provisioning.	SPI
V04	Cloud Storage vulnerabilities	a) Data co-location b) Data may be located in different jurisdictions which have different laws c) Incomplete data deletion – data cannot be completely removed d) Data backup done by untrusted third-party providers e) Information about the location of the data usually is unavailable or not disclosed to users f) Data deduplication – a technique that stores only a copy of redundant data which may be not secured	SPI
V05	Vulnerabilities in Virtual Machines and Hypervisors	a) Shared resources between VMs (CPU, memory, I/O, and network) b) Colocation of VMs c) Allocation and deallocation of resources with VMs d) Uncontrolled Migration - VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance e) Snapshot – VMs can be copied in order to provide flexibility f) Rollback - VMs can be backed up to a previous state for restoration g) VM Lifecycle - on/off/suspended h) Sharing VM image in public repositories i) VM image are dormant artifacts - not able to be patched j) VMs have IP address that is visible to anyone within the cloud - attackers can map where the target VM is located within the cloud k) Complex hypervisor code l) Flexible configuration of VMs or hypervisors to meet organization needs can be exploited	I
V06	Vulnerabilities in Virtual Networks	Bridge and route techniques also bring some security issues: sniffing and spoofing virtual network.	I

Table 1: Vulnerabilities in Cloud Computing

Analysis of Security issues in Cloud Computing

•We analyzed existing security vulnerabilities and threats of cloud computing.
•For each vulnerability and threat, we identified what cloud service model or models are affected by these security problems.
•Before analyzing security challenges in cloud computing, we need to understand the relationships and dependencies between these cloud service models.
•PaaS as well as SaaS are hosted on top of IaaS; thus, any breach in IaaS will impact the security of both PaaS and SaaS services, but also it will be true on the other way around. However, we have to take into account that PaaS offers a platform to build SaaS applications, which increases the security dependency between them.
•As a consequence of these deep dependencies, any attack that can compromise any cloud service model can be catastrophic for the cloud. Each cloud service model comprises its own inherent security flaws; however, they also share some challenges that affect all of them.
•Table 1 presents an analysis of vulnerabilities in cloud computing. This analysis offers a brief description, and it indicates what cloud service models (SPI) can be affected by these vulnerabilities.
•Table 2 presents an overview of threats in cloud computing. Like Table 1 it also describes the threats that are related to the technology used in cloud environments, and it indicates what cloud service models are exposed to these threats.



ID	Threats	Description	Layer
T01	Account or service hijacking	An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction.	SPI
T02	Data scavenging	Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data.	SPI
T03	Data leakage	Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed.	SPI
T04	Denial of Service	It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable.	SPI
T05	Client-data manipulation	Users attack web applications by manipulating data sent from their application component to the server's application. For example, SQL injection, command injection, insecure direct object references, and cross-site scripting.	S
T06	VM escape	It is designed to exploit the hypervisor in order to attack other virtual machines that are located on the same server.	I
T07	VM hopping	It happens when a VM is able to gain access to another VM (i.e by exploting some hypervisor vulnerability)	I
T08	Malicious VM creation	An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository.	I
T09	Insecure VM migration	Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can do the following actions: a) Access data illegally during migration b) Transfer a VM to an untrusted host c) Migrate several VM causing disruptions or DoS	I
T10	Sniffing/Spoofing virtual networks	A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VM.	I

Table 2: Threats in Cloud Computing

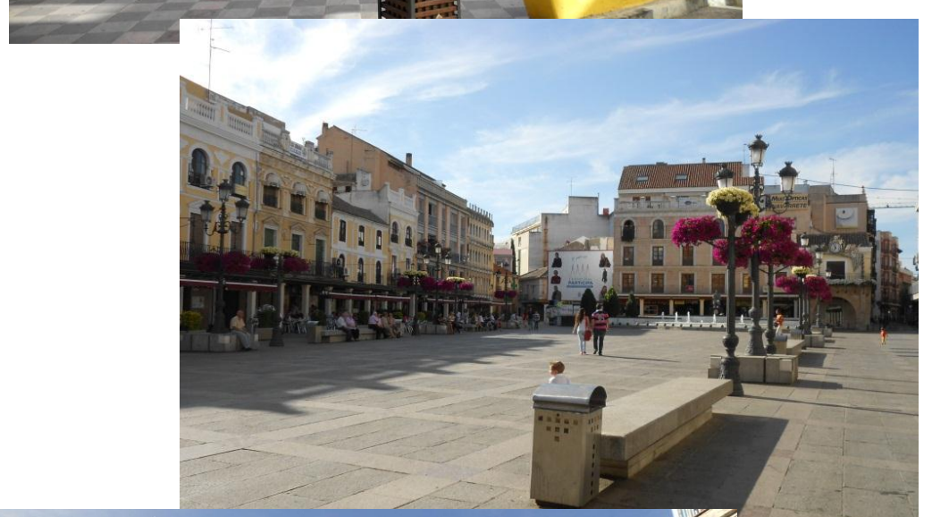
II. International Experience

UCLM

The University of Castilla-La Mancha is a public institution devoted to teaching and research. It is a regional univerity which is organized in provincial campuses: Albacete, Ciudad Real, Basin, and Toledo.

Ciudad Real

Ciudad Real (“Royal City”) is a small city in Castilla-La Mancha, Spain. Ciudad Real was founded by Alfonso X El Sabio (“The Wise”) in the 13th century. Ciudad Real was the scenario where Cervantes sited the adventures of the famous “Don Quixote de La Mancha”.



Career Impact

This experience offered me more opportunities in concern to experience different ways in which people work together as a group and solve problems.
This opportunity also gave the chance to get to know a place and a different culture.

III. Acknowledgement

The material presented in this poster is based upon the work supported by the National Science Foundation under Grant No. OISE-0730065. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.