Classifying Security Threats in Cloud Networking

Bruno M. Barros[1], Leonardo H. Iwaya[1,2], Marcos A. Simplicio Jr.[1], Tereza C. M. B. Carvalho[1], András Méhes[3] and Mats Näslund[3]

[1]*Escola Politécnica, Universidade de São Paulo, São Paulo, Brazil*

[2]*Karlstad University, Karlstad, Sweden*

[3]*Ericsson Research, Stockholm, Sweden*

bbarros@larc.usp.br, leonardo.iwaya@kau.se, {mjunior, carvalho}@larc.usp.br, {andras.mehes, mats.naslund}@ericsson.com

Keywords: Cloud Networking, Cloud Security, Security Threats, Security Taxonomy.

Abstract: A central component of managing risks in cloud computing is to understand the nature of security threats. The relevance of security concerns are evidenced by the efforts from both the academic community and technological organizations such as NIST, ENISA and CSA, to investigate security threats and vulnerabilities related to cloud systems. Provisioning secure virtual networks (SVNs) in a multi-tenant environment is a fundamental aspect to ensure trust in public cloud systems and to encourage their adoption. However, comparing existing SVN-oriented solutions is a difficult task due to the lack of studies summarizing the main concerns of network virtualization and providing a comprehensive list of threats those solutions should cover. To address this issue, this paper presents a threat classification for cloud networking, describing threat categories and attack scenarios that should be taken into account when designing, comparing, or categorizing solutions. The classification is based on the CSA threat report, building upon studies and surveys from the specialized literature to extend the CSA list of threats and to allow a more detailed analysis of cloud network virtualization issues.

1 INTRODUCTION

The current concept of cloud computing evolved from technologies such as distributed computing and resource virtualization, enabling the utilization of shared computing infrastructures for delivering software, platforms and infrastructures to different customers over the Internet. Nevertheless, cloud computing has other particular requirements such as (Mell and Grance, 2011): on-demand provision of the computing resources; broad network access to configure and request computing capabilities; resources are pooled to be used by multiple customers in a multi-tenant model; the resources should be elastically provisioned and released; and delivered services should be transparently measured for managing and billing purposes. This new model of delivering computing power takes advantage of economies of scale, allowing cloud providers to deliver services for a reasonable cost to several institutions and companies. It also brings advantages to customers, who can pay only for what they consume instead of obliging them to purchase, install and maintain their own equipment.

Unfortunately, however, the advantages brought by the cloud are also accompanied by threats and security vulnerabilities that discourage its full adoption by many companies.An example is the need of isolating resources, data and communication within the cloud. Public cloud systems utilize a multi-tenant architecture, in which customers should only ”see” the cloud resources assigned to them, as if they were the sole user of the infrastructure.

Virtualization technologies play a crucial role in enforcing this isolation, given that they are the main building block in provisioning the customers' infrastructure, including virtual machines (VMs) and virtual networks (VNs). Additionally, a virtualization solution(s) should ensure not only that the VMs operate with isolated resources, but also allow network traffic monitoring and the creation of *secure network domains*. For this reason, enabling SVN in the cloud computing is currently a subject of intense research (Sun and Hu, 2012). Many of the existing proposals rely on open network virtualization solutions such as Open vSwitch for defining virtualized network architectures with security features (Hao et al., 2010; Cohen et al., 2013), inserting security modules inside VMs and virtual switches (Basak et al., 2010;

Barjatiya and Saripalli, 2012), or creating hypervisor-based network controllers (Mattos and Duarte, 2013).

Nonetheless, it is often hard to clearly identify all the threats and vulnerabilities that are addressed by the different network virtualization solutions. Indeed, there is a myriad of issues that can be targeted, such as ensuring traffic isolation, preventing sniffing and address spoofing, as well as detecting and mitigating Distributed-/Denial-of-Service DoS/DDoS and man-in-the-middle attacks (Hao et al., 2010; Basak et al., 2010; Barjatiya and Saripalli, 2012; Cohen et al., 2013; Mattos and Duarte, 2013). However, it is not always the case that solutions proposed in the literature explicitly analyze their (in)ability to cope with each of the existing threats, even if they are truly able to prevent them. This makes comparing and evaluating these solutions a difficult task.

Aiming to address this lack of uniformity in the treatment of network virtualization security proposals, this paper presents a threat classification for SVNs, describing threat classes and attack scenarios that should be taken into account when designing, comparing, categorizing or evaluating solutions. This classification is based on technical reports from cloud standardization organizations such as European Network and Information Security Agency (ENISA, 2013), the Cloud Security Alliance (CSA, 2013), and National Institute of Standards and Technology (NIST, 2011), as well as on scientific papers that reviewed problems in this area (Chowdhury and Boutaba, 2010; Pearce et al., 2013). Given the broad scope of the security challenges described in these reports, they do not (intend to) provide a framework to evaluate security issues directly related to network virtualization in cloud computing. Therefore, the classification proposed herein aims to fill part of this gap by focusing specifically on the technical issues related to virtual networking in the cloud environment.

The rest of this paper is organized as follows. Section 2 reviews the security threat classification for cloud computing proposed by CSA (CSA, 2013). Section 3 presents our proposed threat classification, which builds upon the CSA work. Section 4 then discusses, by means of examples, different cloud virtual networking attacks from each threat category, showing the coverage of the proposed classification. Section 5 presents the conclusion and future work.

2 CLOUD SECURITY THREATS

With the widespread adoption and popularization of cloud-based systems, considerable effort has been made to identify and classify security threats in this environment. Some relevant examples include the security guidelines for cloud computing provided by the ENISA (Catteddu, 2010; ENISA, 2013), the CSA (CSA, 2013), and NIST (NIST, 2011).

Among these documents, the CSA "Notorious Nine" report (CSA, 2013), which identifies important threats that may occur accidentally or intentionally in cloud systems, is of especial interest: it provides a clear view of the most relevant security threats when deploying and consuming cloud services, ranked according to the industry perspective. Therefore, the report highlights the main security aspects that need to be taken into account by cloud providers for ensuring trust in their services. It is important to notice, however, that (CSA, 2013) is intended as a general guideline of relevant security aspects, not focused on networking issues. Nonetheless, given its importance, it can be seen as an interesting starting point for identifying relevant cloud networking threats, which is exactly the approach adopted in this document. Next, we present a classification method for indentify security threats in cloud networking, built upon the CSA classification for cloud security threats.

3 THREAT CLASSIFICATION

CSA "Notorious Nine" (CSA, 2013) and similar-purpose reports (CSA, 2011; ENISA, 2013; NIST, 2011; Gonzalez et al., 2012) are important sources of information about cloud security threats. However, their main goal is to give a high level description of potential problems, not on providing a fine-grained analysis of how each of the many threats identified apply to specific scenarios (e.g., virtual networking). On the other hand, there are works in the literature that investigate SVNs in more depth, such as (Chowdhury and Boutaba, 2010; Schoo et al., 2011; Natarajan and Wolf, 2012). Unfortunately, since their goal is to survey solutions and to identify challenges in the area, they fail to provide a reusable classification of the virtual networking threats described. Given the relevance of threat modeling to identify security requirements (Myagmar et al., 2005), those works are not ideal for the task of comparing and evaluating different security proposals in virtual networking or guiding the design of comprehensive solutions for the most relevant threats. Aiming to bridge this gap, next, we build upon the CSA "Notorious Nine" threat report for deriving finer-grained threat classification focused specifically on SVNs.

3.1 Extending Current Classifications

For the purpose of building the proposed classification, the CSA "Notorious Nine" threats were decomposed into more specific menaces. The resulting finer-grained list, containing specific attacks and countermeasures, was then analyzed aiming to identify threats that could be associated to virtual networking security issues. The aggregation of the identified threats according to their characteristics then lead to the general categories presented as follows.

Before we present the proposed classification, however, it is important to emphasize that attaining the right level of abstraction is a considerable challenge when trying to create a comprehensive view of virtual networking vulnerabilities in the cloud. Aiming to be both concise and comprehensive, our approach in the proposed classification involves two main requirements: (1) threats should have a detailed enough description to effectively help guide the development of innovative solutions; and (2) the number of threat groups should be small enough to allow the classification to be applied to the analysis and comparison of common solutions. These requirements have an obvious trade-off: a large number of threat classes may lead to an overly detailed classification, but a reduced number of threat groups may lead to a high level description that may be vague and less useful to comparative studies. As a result, our classification proposes a reduced number of categories without ignoring important aspects of virtual networking.

In addition to those basic requirements, we considered the different attack scenarios within the cloud environment, i.e., who the attacker is and who is being attacked. In each scenario, we then try to identify the different threat classes to reflect the concerns already evidenced in the literature.

3.2 Threat Scenarios

The first is the Cloud Provider Network, which includes all the cloud provider private network resources connecting all the data center infrastructure that allows the cloud service provision. The second is the Public Network, which comprises the public Internet that allows users to access the cloud services. Both networks are illustrated in Figure 1. We have limit our scope to threats in the Cloud Provider Network, to identify security issues related only to the cloud computing paradigm and to its technological mechanisms. We can identify three attack scenarios involving different entities of the cloud:

1. **Tenant-to-Tenant.** Threats related to attacks promoted by a legitimate tenant targeting another legitimate tenant. Such attacks are usually performed by exploring vulnerabilities of the cloud provider network infrastructure
2. **Tenant-to-Provider.** Threats related to cloud vulnerabilities that allow a legitimate tenant to disrupt the operation of the cloud infrastructure, preventing the cloud provider from delivering the service in accordance with the service level agreements established with other legitimate tenants.
3. **Provider-to-Tenant.** Threats related to vulnerabilities in the cloud provider infrastructure, which allows malicious insider attacks from employees and other agents with direct access to the cloud infrastructure.

Figure 2 illustrates these three attack scenarios in the network context previously mentioned. Despite the interest of provider-to-tenant threats, for the purpose of this research we consider a reliable cloud provider, focusing our efforts on the tenant-to-tenant and tenant-to-provider threats.

3.3 Cloud VN Threat Categories

Following the method and the requirements discussed in Section 3.1, we identified five general classes of virtual networking security threats, described as follows. For each class, we also present the CSA-related threats and the virtual networking attacks obtained from the decomposing process described in Section 3.1. We note, however, that the inclusion of new threat classes to this classification should be considered a matter of continuous work, following new discoveries in the field of cloud security.

1. **Physical Isolation.** Covers all the vulnerabilities related to the physical resources of the underlying network infrastructure being shared by multiple tenants. Attacks in this class are normally related to capturing and to analyzing data collected from shared resources, but can also involve the exhaustion of resources from shared hardware.
2. **Logical Isolation.** Covers all the vulnerabilities directly related to situations in which logical resources (e.g., vCPUs, vLANs and vSwitches) are not adequately isolated, allowing tenants to access each other's networking capabilities. Attacks of this class can exploit vulnerabilities in the cloud

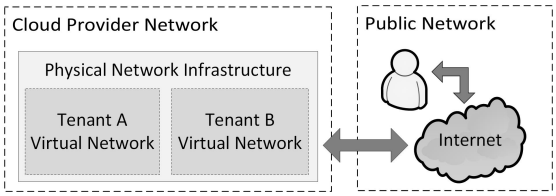

Figure 1: Complementary networks in cloud environments.

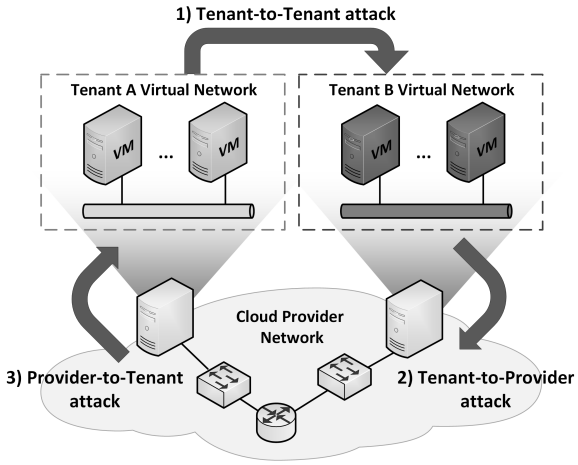

Figure 2: Security attack scenarios in cloud VNs.

virtualized network functions and network management modules.

3. **Authentication.** Covers all the vulnerabilities related to inadequate authentication, which allow attackers to mask their real identities. This can be accomplished by exploiting authentication protocols, acquiring credentials and/or key materials by capturing data traffic, or via password recovery attacks (e.g., brute force or dictionary attacks).
4. **Authorization.** Covers all the vulnerabilities related to authorization problems, allowing granting or scaling rights, permissions or credentials to or from an unauthorized user. The attacker can exploit a vulnerability in the cloud platform authorization modules, or even in the victim computer, to create or change its credentials in order to obtain privileged rights. Similarly to attacks that exploit authentication threats, authorization threats can lead to the leakage of confidential data and access to management modules.
5. **Insecure APIs.** Covers all the threats related to failures, malfunctions and vulnerabilities in APIs that compose the cloud system. Attacks of this class try to exploit insecure interfaces for accessing or tampering with services running in other tenants or cloud administrative tools. This may lead to data loss/leakage, as well as to cause unavailability of services.

3.4 Correlation with CSA Threats

Table 1 summarizes the correlations between CSA threats and the network threat categories herein proposed. Analyzing this table, one can notice that CSA threats related to *shared technology vulnerabilities*, *data breaches*, and *DoS* are the most frequently related to network vulnerabilities. Therefore, they should be the main focus of SVN-oriented solutions, considering both tenant-to-tenant and tenant-to provider attack scenarios, as discussed in more details in the next section.

Table 1: Correlation of proposed categories and threats with CSA notorious top nine threats.

Category	Threat Examples	CSA Top 9
Physical Isolation	Side-channel attack	DB,
	Guest-hoping attack	DoS,
	Resource exhaustion	STV
	Physical man-in-the-middle	
Logical Isolation	Man-in-the-middle	DB,
	Sniffing	DoS,
	Port scanning	STV
	Replay attacks	
Authentication	Spoofing	DB,
	Compromised-key attack	ASH,
	Password-based attacks	STV
Authorization	Software exploitation	DB, MI,
	Phishing	ACS, STV
Insecure APIs	API exploitation	IIA
	Code and Package injection	

Abbreviations: data breaches (DB), Denial-of-Service (DoS), shared technology vulnerabilities (STV), account or service traffic hijacking (ASH), malicious insiders (MI), abuse of cloud services (ACS), insecure interfaces and APIs (IIA).

4 CLASSIFICATION ANALYSIS

This section correlates the threat scenarios discussed in Section 3.2 with the classification proposed in Section 3.3, presenting threat examples for each proposed category in both Tenant-to-Tenant and Tenant-to-Provider scenarios.

4.1 Physical Isolation

Such attacks can be perpetrated if the attacker's VM is sharing the same host machine or physical network node as the victim's VM. In this scenario, the attacker can engage in: a side-channel attack, subjecting confidential traffic to cryptanalysis; use DoS/DDoS attacks to exhaust or to bring physical network resources down; or to gather information about the services running in the target machine. Sniffing is one of the most common attacks: attackers attempt to access information from other tenants or cloud provider network by reading packets going through the physical NICs.

Threat Examples on Tenant-to-Tenant Scenario. *1) Side channel*: An encryption algorithm used by

tenants is subject to cryptanalysis based on timing attacks. *2*) *Guest hopping*: The attacker inserts a VM in the same host of the victim to exploit shared network components in subsequent attacks. *3*) *DoS/DDoS*: Exhaustion of network resources shared by tenants inside the same host.

Threat Examples on Tenant-to-Provider Scenario. *1*) *Sniffing*: By monitoring physical network interfaces an attacker may intercept provider management data. *2*) *Side channel*: An encryption algorithm used by a provider is subject to cryptanalysis based on timing attacks. *3*) *DoS*: Amplification attacks performed from inside the cloud, possibly combined with address spoofing can flood provider network infrastructure.

4.2 Logical Isolation

The cloud provider should ensure isolation of resources among its customers, which includes virtualized network components that compose the cloud logical network and the tenants virtual networks. Tenant-to-tenant attacks involves breaking this logical isolation, allowing a malicious tenant to get access victim's resources. This sort of attack can lead to data leakage, malicious use of other tenants' resources, and/or disruption of network services.

A malicious tenant may also exploit virtual network resources, controllers and other services provided by the cloud provider. Some examples involve the use of port scanning and network reconnaissance mechanisms, so that the attacker can get access to privileged information, such as the network topology, list of virtual networks, or configuration messages. Also, a malicious tenant may use the cloud infrastructure to deploy botnets for launching DoS attacks against the cloud infrastructure, its tenants or any external targets.

Threat Examples on Tenant-to-Tenant Scenario. *1*) *Port scanning*: The attackers scans open ports and running services in other tenant VMs. *2*) *Network reconnaissance*: Protocols for network configuration and identification can be exploited to discover other virtual networks and/or network topologies pertaining to other tenants (e.g., using ARP requests) *3*) *Sniffing*: Sniffing and/or man-in-the-middle attacks due to the lack of isolation between virtual networks. *4*) *Malware (worm)*: Malicious software that can replicate itself through and between tenant virtual networks. *5*) *Botnets*: Use the cloud infrastructure to deploy botnets, in which groups of VMs running malicious computer programs target other tenants and shared network resources.

Threat Examples on Tenant-to-Provider Scenario. *1*) *Network reconnaissance*: Use network reconnaissance mechanisms to discover other network topologies, VNs, and services. *2*) *Malware (worm)*: Malicious software that can replicate itself through the provider network infrastructure from a compromised tenant virtual network. *3*) *Botnets*: Use the cloud infrastructure to deploy botnets, targeting shared network resources and network controller nodes. *4*) *Replay attack*: replication of control messages that can impair network services and cloud operations (e.g., instantiating duplicated VMs)

4.3 Authentication

Attacks that exploit authentication vulnerabilities can be performed either in Tenant-to-Tenant and Tenant-to-Provider scenarios. In both cases the attacker may exploit the authentication protocols by means of compromised-key (e.g., leakage of key material information) and/or password-based attacks (e.g., dictionary and brute force attacks). Also, the authentication and identity management modules can be exploited to force authentication threats. In the case of Tenant-to-Tenant scenario, the attacker wants to gain access to the victim's virtual networks. In Tenant-to-Provider scenario, the attacker may gain access to the whole network services and/or controlling modules, affecting the whole cloud.

Threat Examples on Tenant-to-Tenant Scenario. *1*) *Credential replay*: By capturing and replaying a user's credential. *2*) *Spoofing*: The malicious tenant masquerades as another tenant by falsifying data and thereby gaining illegitimate access to resources.

Threat Examples on Tenant-to-Provider Scenario. *1*) *Credential replay*: The replay of a user's credential might allow impersonation of a cloud administrator. *2*) *Spoofing*: The malicious tenant performs a DNS spoofing attack, inserting bogus data into a DNS name server cache database and causing the name server to return an incorrect IP address.

4.4 Authorization

In this case, the attackers try to escalate their privileges in the system. Since network privileges in the cloud usually make sense only with respect to the cloud provider, authorization attacks are reasonable only when we consider Tenant-to-Provider scenario. For instance, a malicious user may fake its credentials to acquire administrative roles, authorization to other customers services, or to gain access to services out of contract.

Threat Examples on Tenant-to-Provider Scenario. *1*) *Network Reconnaissance*: A legitimate tenant can

escalate its privileges to run network reconnaissance scripts in the cloud network infrastructure, discovering the cloud provider network topology and using this information for promoting more precise attacks against the network resources. *2*) *Cloud Exploit Kits (Malware-as-a-Service)*: Malicious software hosted inside cloud provider infrastructure and available to other tenants to attack the provider services through its network resources. *3*) *Network Programmability*: The attackers try to escalate their privileges to get access to program APIs of the network devices (e.g., OpenFlow API).

4.5 Insecure APIs

Attacks to APIs can affect a broad range of cloud modules, e.g., those responsible for resource allocation, authentication and identity management, storage, or accounting. The network modules deployed in VMs, as well as controller, computing and network nodes, are usually distributed along the cloud infrastructure. Therefore, the APIs used for network virtualization and configuration may be target of attacks and vulnerability exploitation. For instance, attacks based on code injection techniques may exploit computer errors caused by processing invalid data, undermining cloud services and databases. This category of attack may target either Providers or Tenants.

Threat Examples on Tenant-to-Tenant Scenario: *1*) *Code injection*: The attacker performs SQL injection using a network controller API (e.g., Neutron) to erase a tenant data from the cloud network configuration database.

Threat Examples on Tenant-to-Provider Scenario: *1*) *Code injection*: The attacker performs SQL injection using a network controller API (e.g., Neutron) to modify (parts of) the network configuration database.

5 CONCLUSIONS AND FUTURE WORK

The wide variety of threats related to cloud computing network virtualization makes it difficult to compare or to categorize existing solutions focused on securing virtual networks. This paper proposes a threat classification for cloud virtual networks built upon the *"notorious nine cloud computing top threats"* of CSA. Moreover, the presented classification allows a more detailed view of the network threats discussed in cloud computing literature. This finer-grained approach makes it easier to identify the technologies that might be used to solve different security issues in cloud networking, facilitating the analysis and design of security solutions.

As future work we plan to employ this threat classification in a literature review of cloud networking security solutions. The result expected is a comprehensive literature survey that allows not only comparing existing solutions, but also the identifying the gaps and challenges in cloud networking security.

ACKNOWLEDGEMENTS

Innovation Center, Ericsson Telecomunicações S.A. (Brazil) and CNPq (grant 305350/2013-7).

REFERENCES

Barjatiya, S. and Saripalli, P. (2012). BlueShield: A Layer 2 Appliance for Enhanced Isolation and Security Hardening among Multi-tenant Cloud Workloads. *IEEE Int. Conf. on Utility and Cloud Comp.*, pages 195–198.

Basak, D., Toshniwal, R., Maskalik, S., and Sequeira, A. (2010). Virtualizing networking and security in the cloud. *SIGOPS Oper. Syst. Rev.*, 44(4):86–94.

Catteddu, D. (2010). Cloud computing: Benefits, risks and recommendations for information security. In Serrão, C., Aguilera Díaz, V., and Cerullo, F., editors, *Web Application Security*, volume 72 of *CCIS*, page 17.

Chowdhury, N. and Boutaba, R. (2010). A survey of network virtualization. *Comput. Netw.*, 54(5):862–876.

Cohen, R., Barabash, K., Rochwerger, B., Schour, L., Crisan, D., Birke, R., Minkenberg, C., Gusat, M., Recio, R., and Jain, V. (2013). An intent-based approach for network virtualization. In *IFIP/IEEE INM'13*.

CSA (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. Technical report, CSA.

CSA (2013). The Notorious Nine Cloud Computing Top Threats in 2013. Technical report, CSA.

ENISA (2013). Threat landscape 2013-overview of current and emerging cyber-threats. Technical report, ENISA.

Gonzalez, N., Miers, C., Redígolo, F., Jr. Simplicio, M., Carvalho, T., Näslund, M., and Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. *JCC*, 1(1):1–18.

Hao, F., Lakshman, T. V., Mukherjee, S., and Song, H. (2010). Secure Cloud Computing with a Virtualized Network Infrastructure. In *Proc. of the USENIX*.

Mattos, L. F. D. and Duarte, O. C. M. B. (2013). A Mechanism for Secure Virtual Network Isolation Using to Hybrid Approach Xen and OpenFlow. In *SBSeg'2013*.

Mell, P. and Grance, T. (2011). The NIST definition of cloud computing (draft). Technical report, NIST.

Myagmar, S., Lee, A., and Yurcik, W. (2005). Threat modeling as a basis for security requirements. In *SREIS*.

Natarajan, S. and Wolf, T. (2012). Security issues in network virtualization for the future internet. In *ICNC*.

NIST (2011). Guide to Security for Full Virtualization Technologies. Technical report, NIST.

Pearce, M., Zeadally, S., and Hunt, R. (2013). Virtualization: Issues, security threats, and solutions. *ACM Computing Surveys (CSUR)*, 45(2):17.

Schoo, P., Fusenig, V., Souza, V., Melo, M., Murray, P., Debar, H., Medhioub, H., and Zeghlache, D. (2011). Challenges for cloud networking security. In *MNM*.

Sun, Q. and Hu, Z. (2012). Security for networks virtual access of cloud computing. In *MINES'2012*.