Analyzing and Modeling Security Aspects of Cloud-based Systems

Melanie Siebenhaar*, Hsin-Yi Tsai†, Ulrich Lampe*, and Ralf Steinmetz*
*Multimedia Communications Lab (KOM), Technische Universität Darmstadt, Darmstadt, Germany
†Institute of Electrical Control Engineering, National Chiao Tung University, Taiwan
Email: *{firstname.lastname}@KOM.tu-darmstadt.de, †hytsai.ece96g@nctu.edu.tw

***Abstract*—Security is one of the most challenging aspects in cloud computing. To date, cloud solutions do not cover all the countermeasures against attacks that may occur in a cloud-based system. In order to gain an overview of the components and their interfaces in a cloud-based system and to design adequate countermeasures, a holistic framework is required which provides the means to model and analyze the cloud security concerns. This extended abstract outlines both, such a framework and its possible application.**

I. Introduction

Cloud computing represents a new paradigm and promises to deliver computing resources as a utility [1]. Cloud users gain a high level of flexibility, but are not aware of the location of their data in the virtualized cloud space and of all the measures required to secure the cloud-based system. Hence, security is considered as one of the major challenges in cloud computing (e.g., [2]). Besides well-known security issues, clouds also face new security challenges. Appropriate countermeasures are required to protect cloud components and their interfaces from attacks. An effective design of the countermeasures makes it necessary to model and analyze the security issues in a preceding step. For this purpose, the cloud components, their interfaces, the parties involved, and the possible threats have to be taken into account. In the following, we introduce a holistic framework, which provides support for practitioners and researchers performing a cloud-based security analysis.

II. Cloud Security Framework

Creating a holistic framework that addresses the security issues in cloud computing requires exploring the properties, components, and interfaces of cloud-based systems first. We included these aspects in the *cloud layer* of the security framework (cf., Fig. 1). In doing so, the means for analyzing cloud security issues are provided. In addition, elements to model and analyze the security issues are required. These elements constitute the *security layer* of the framework. Both layers are presented in detail in the following.

A. The Cloud Layer

Relevant aspects of cloud computing can be obtained from its definition. We adhere to the definition provided by the National Institute of Standards and Technology (NIST), since it is one of the most cited: ”Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [3]. Hence, cloud computing represents a new way of providing and consuming resources. The NIST definition further comprises five essential characteristics, three service models, and four deployment models.

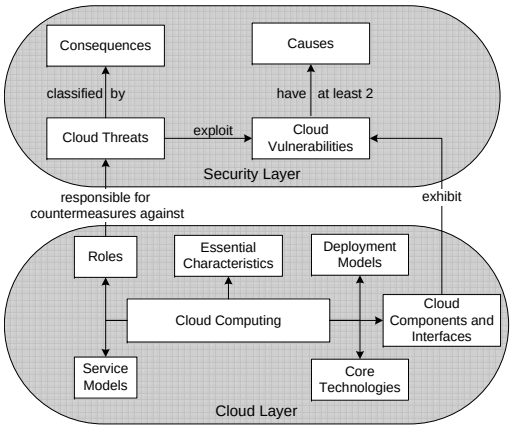

Fig. 1. Excerpt of the Cloud Security Framework

1) Essential Characteristics: include on-demand self service, broad network access, resource pooling, rapid elasticity, and measured service.

2) Service Models: refer to different layers of a common IT stack and comprise Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

3) Deployment Models: are distinguished with respect to the ownership and operating mode of a cloud and encompass public, private, community, and hybrid clouds.

Especially in hybrid cloud scenarios, where several parties are involved and clouds are even interconnected, a security analysis will be very difficult. Since security concerns arise in different spheres of control, a clear role model is required to determine the responsibilities for establishing adequate countermeasures. Based on the work by Armbrust et al. [1], we defined the following role model.

4) Cloud Roles:

- Service user: the user consuming SaaS services
- Service provider: the SaaS provider
- Broker: intermediary, e.g., providing value-added services
- Cloud provider: the PaaS or IaaS provider

From our analysis of the different roles, we found that the responsibilities for setting up appropriate countermeasures increase from the top to the bottom of a common IT stack. A service user is typically confronted with basic security concerns (e.g., secure passwords). A service provider and a broker share very similar responsibilites regarding service provision (e.g., conflicting service level agreements with different stakeholders), but without control of the underlying computing resources. Therefore, many security issues are located in the IaaS layer (cf., Section II-C) or can be traced back to the core technologies of cloud computing [4].

5) Core Technologies:

- Web Services and applications: clouds provide virtualized resources as a service and typically make use of Web service technologies
- Virtualization: allows for an abstract, logical view on physical resources and their aggregation within pools
- Cryptography: data or communication is vulnerable to attacks and cryptographic solutions are often applied

Also the targets (i.e., components, interfaces) of attacks have to be taken into account. We adapted the classification by Grobauer et al. [2] and obtained the following groups.

6) Cloud Components and Interfaces:

- Web services and applications: comprise the SaaS level
- Computing resources: virtual machines and platforms
- Storage: data storage
- Communication: network infrastructure and interfaces
- Services/APIs: support services and application interfaces
- Management Access: interfaces for cloud management
- IAAA Mechanisms: identification, authentication, authorization, and auditing mechanisms
- Compliance: legal requirements and business obligations

B. The Security Layer

Since cloud computing represents a new way of resource provision and consumption, it bears new security challenges. We define a vulnerability to be *cloud-specific*, if at least two of the following criteria are met (cf., [2]).

7) Causes:

- Core technology: the vulnerability is specific to one of the core technologies
- Essential characteristic: the vulnerability is caused by one of the essential characteristics
- Global distribution: the vulnerability arises from the global distribution of the resources
- Cloud setting: common security methods/mechanisms are not applicable/hard to implement

In general, cloud components and interfaces exhibit vulnerabilities which are exploited by cloud threats. A threat is realized by a concrete cloud attack. According to Shirey [5], the consequences of cloud threats can be classified as follows.

8) Consequences:

- Disclosure: unauthorized access to information
- Deception: acceptance of false data
- Disruption: interruption/prevention of correct operation
- Usurpation: unauthorized control of some part of a system

TABLE I
VIRTUAL-MACHINE ESCAPE (NUMBERS REFER TO ENUM. IN THIS PAPER)

Aspect	Characteristics
Threat	Virtual-Machine Escape
Vulnerability	Hypervisor Vulnerability
2) Service Models	IaaS
3) Deployment Models	All Models
4) Roles	Cloud Provider
6) Components	Computing Resources
7) Causes	1) Essential Characteristic: Resource Pooling, 5) Core Technology: Virtualization
8) Consequences	Usurpation

C. A Selected Threat: Virtual-Machine Escape

To illustrate the application of the cloud security framework, we sketch the analysis (cf., Table I) of the so-called *Virtual-Machine Escape Threat* (cf., [2]). In a corresponding realized attack, a virtual-machine user gains access to the so-called hypervisor. A hypervisor represents a meta operating system that is responsible for managing the hardware access of the virtual machine instances on a single physical machine. This attack is associated with the computing resources on the IaaS level and may happen in all deployment models. The respective cloud provider is responsbile for establishing appropriate countermeasures. Main causes that this vulnerability may exist are the virtualization technology and the aggregation of resources within pools. Hence, a proper isolation of resources must be ensured by the cloud provider. The primary consequence of such an attack is usurpation, since the unauthorized attacker obtains control over the hypervisor and thus, may gain access to other virtual-machines located on the same physical machine. Since this threat also depends on the deployment model (e.g., private/public cloud) applied, the cloud provider must assess the probability and severity of the attack. It can be assumed that this threat will be more severe in public clouds due to the high amount of multiple tenants.

III. CONCLUSION

In this paper, we presented a holistic framework for cloud computing security and its application. With the framework, we aim at supporting a security analysis of cloud-based systems from the perspective of different cloud roles as well as the design and application of appropriate countermeasures.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," Electrical Engineering and Computer Sciences, University of California at Berkeley, Tech. Rep. UCB/EECS-2009-28, 2009.

[2] B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding Cloud-Computing Vulnerabilities (preprint)," *IEEE Security and Privacy*, 2010.

[3] P. Mell and T. Grance. (2009) The NIST Definition of Cloud Computing. National Institute of Standards and Technology (NIST), Information Technology Laboratory. [Online]. Available: http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

[4] C. Baun, M. Kunze, J. Nimis, and S. Tai, *Cloud Computing. Web-basierte dynamische IT-Services*. Springer-Verlag Berlin Heidelberg, 2010.

[5] R. W. Shirey. (Internet Draft (1994)) Security Architecture for Internet Protocols: A Guide for Protocol Designs and Standards. [Online]. Available: https://datatracker.ietf.org/drafts/draft-irtf-psrg-secarch-sect1/