Threat as a Service?
Virtualization's Impact on Cloud Security

Hsin-Yi Tsai, *National Chiao Tung University*
Melanie Siebenhaar and André Miede, *Technische Universität Darmstadt*
Yu-Lun Huang, *National Chiao Tung University*
Ralf Steinmetz, *Technische Universität Darmstadt*

Virtualization is essential to cloud computing, yet its security vulnerabilities in the cloud environment haven't been sufficiently studied. This analysis of cloud security focuses on how virtualization attacks affect different cloud service models.

As cloud computing realizes the vision of computing as a utility, providers are developing a shared pool of configurable computing resources, which customers can dynamically provision and release according to their changing needs.[1] Thus, both groups benefit: providers can reuse computing resources, and users reduce costs through on-demand resource provisioning.

Cloud computing provides different layers of computing utilities, from storage and networking to tools and applications, through three main service models: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The models rely on existing technologies for support—in particular, virtualization provides on-demand resource provisioning and multitenancy. However, current virtualization security mechanisms might not work in cloud computing.[2] For example, traditional virtualization security solutions assume that a guest OS inside a virtual machine (VM) is known in advance. In cloud computing, the guest OS running in a VM is controlled by a user, and a priori knowledge of the guest OS is unavailable.

Although many researchers have investigated cloud security (see the "Related Work in Cloud Security" sidebar), little is known about virtualization-related security issues, even though virtualization is a core cloud computing technology.[3] Here, we challenge the notion that cloud computing isn't necessarily subject to virtualization security issues. We analyze how virtualization vulnerabilities affect the different service models, which can differ greatly from how they affect conventional IT environments.

 Published by the IEEE Computer Society

Related Work in Cloud Security

Many researchers have investigated cloud computing security. Kresimir Popović and Zeljko Hocenski provide a generic overview of the security issues, requirements, and challenges that cloud service providers face.[1] S. Ramgovind and colleagues provide an overall security perspective on cloud computing, illustrating security requirements coupled with cloud service and deployment models.[2] Hassan Takabi and his colleagues discuss user authentication, access control, policies, service, and trust in the cloud environment.[3]

In 2011, S. Subashini and V. Kavitha surveyed SQL injection flaws, cross-site scripting, insecure storage, and invalidated redirects or forwards.[4] Minqi Zhou and colleagues investigated cloud security and privacy issues in terms of the special relationship between users and providers in a cloud.[5] The relationship contains three parties: the cloud service user, cloud service provider/cloud user, and cloud provider. However, most of the existing research discusses cloud security from a generic viewpoint outside a cloud. None of these works discuss the threat levels in different service models (SaaS, PaaS, IaaS) from the perspective of virtualization technologies. Yet because virtualization is essential to cloud computing, we must consider its security threats and develop appropriate countermeasures.

In 2009, Thomas Ristenpart and his colleagues showed that a cloud platform multiplexing many customers' VMs across a shared physical infrastructure can introduce new vulnerabilities, such as cross-VM side-channel attacks (extracting information from a target VM on the same host machine).[6] Their work emphasizes the importance of virtualization technologies in the context of cloud computing security. However, the authors only stated threats resulting from virtualization technologies. In 2011, Bernd Grobauer and his colleagues defined some indicators of cloud-specific vulnerabilities, including those resulting from Web applications, cloud software environments, and cloud infrastructures.[7] They didn't, however, discuss in detail the implications of virtualization technology on different service models. The work of M.A. Morsy and his colleagues is the closest to our work,[8] because it considers cloud security issues in different service models, but it discusses virtualization-related issues only for the IaaS model.

References

1. K. Popovic and Z. Hocenski, "Cloud Computing Security Issues and Challenges," *Proc. 33rd Int'l Convention on Information and Comm. Technology, Electronics and Microelectronics* (MIPRO 10), IEEE Press, 2010, pp. 344–349.
2. S. Ramgovind, M.M. Eloff, and E. Smith, "The Management of Security in Cloud Computing," *Proc. Information Security for South Asia* (ISSA 10), IEEE Press, 2010, pp. 1–7.
3. H. Takabi, J.B.D. Joshi, and G.-J. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," *Proc. 2010 IEEE 34th Ann. Computer Software and Applications Conf. Workshops*, IEEE Press, 2010, pp. 393–398.
4. S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *J. Network and Computer Applications*, vol. 34, no. 1, 2010, pp. 1– 11.
5. M. Zhou et al., "Security and Privacy in Cloud Computing: A Survey," *Proc. 6th Int'l Conf. Semantics, Knowledge and Grids*, IEEE Press, 2010, pp. 105–112.
6. T. Ristenpart et al., "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," *Proc. 16th ACM Conf. Computer and Communications Security* (CCS09), ACM Press, 2009, pp. 199–212.
7. B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding Cloud-Computing Vulnerabilities," *IEEE Security and Privacy*, vol. 9, no. 2, 2011, pp. 50–57.
8. M.A. Morsy, J. Grundy, and I. Müller, "An Analysis of the Cloud Computing Security Problem," *Proc. 17th Asia Pacific Software Eng. Conf. 2010 Cloud Workshop* (APSEC 10), IEEE Press, 2010.

Cloud Computing Security Challenges

Confidentiality, integrity, and availability are widely used benchmarks for evaluating IT security. We apply these conventional benchmarks to cloud computing and add one more—security management, which is also critical for cloud security.

Confidentiality

A user can access SaaS offerings via a Web browser over the Internet. The user's network traffic and data should remain confidential in transit—that is, protected from unauthorized access. Adopting HTTPS mitigates confidentiality risks. Additionally, because a user can upload data to a cloud when using the SaaS offering, the cloud should also prevent unauthorized users from reading the stored data. A PaaS provider offers a development environment to establish Web services or applications and thus has similar confidentiality concerns.

In IaaS, multiple users can rent computing resources from a single physical infrastructure. Thus, confidentiality in this case requires isolating resource usage among the multiple users—that is, one user shouldn't be able to view another user's memory status or resource use. Furthermore, because PaaS is based on IaaS virtualization, protecting the status of resource use is also a security challenge in PaaS.

Integrity

Integrity is damaged if an illicit user executes, modifies, suspends, copies, replays, or delays data, messages, or assets. Attackers are often interested in different targets, such as network traffic or virtual disks, so the integrity mentioned here varies based on the attack and service model.

Similar to the discussion about confidentiality in SaaS, we need to protect data in transit, stored data, and network traffic. In PaaS and IaaS, the integrity of the platform settings and configuration files is especially important, because if someone maliciously modifies such settings or files, it would affect not only the PaaS and IaaS offerings but also the services deployed through those offerings, such as SaaS applications. The business scenarios for cloud computing, to some extent, magnify the security challenges.

Availability

Availability is endangered if the service or server is spoofed, penetrated, or suspended and can't operate as expected. Since broad network access is essential to cloud computing,[1] the Internet-facing resources, such as the Domain Name System (DNS), are one of the main targets of attacks on availability.

DNS attacks aren't new in the IT security realm. However, the attacks are still problematic in cloud computing owing to its characteristic broad network access. A user can't access the service offering over the Internet without reliable DNS. In addition to the Internet-facing resources, the service offering itself should be secure in terms of availability.

Security management

To accommodate on-demand self-service and rapid elasticity, security management in cloud computing must be able to immediately address and reflect the changing requests. Additionally, the scope of cloud computing could increase the load and complexity of security management, leading to another security challenge.

Virtualization's Impact on Cloud Security

Threats to cloud security can originate in key mismanagement, vague service-level agreements, and weak service-oriented architectures. However, virtualization is fundamental to certain cloud characteristics, such as multitenancy and resource provisioning, so we focus on virtualization's related security issues as a starting point, leaving other critical issues for future work.

Virtualization lets users simultaneously run multiple isolated machines (VMs) on a single physical machine (the host machine). The hypervisor, or VM monitor, is the software that sits between the host machine and VM. The hypervisor allocates and manages the physical resources among the VMs. In cloud computing, a service provider can create a VM with customized configurations for a service user. The virtualization technology supports resource pooling and multitenancy, so its security is essential.

Virtualization security in general has been widely discussed in the literature,[4,5] but here we analyze certain virtualization vulnerabilities in terms of cloud security in particular.

VM Hopping

With VM hopping, an attacker on one VM gains access to another victim VM.[6,7] The attacker can monitor the victim VM's resource usage, modify its configurations, and delete stored data, endangering that VM's confidentiality, integrity, and availability.

A prerequisite for this attack is that the two VMs must be running on the same host, and the attacker must know the victim VM's IP address. Although PaaS and IaaS users have only limited authority, Thomas Ristenpart and his colleagues have shown that an attacker can obtain or determine the IP address using standard customer capabilities.[8] We thus infer that VM hopping is a reasonable threat in cloud computing. Furthermore, multitenancy makes the impact of a VM hopping attack potentially larger than in a conventional IT environment. Because several VMs can run simultaneously on the same host, all of them could become victim VMs. VM hopping

is thus a crucial vulnerability for PaaS and IaaS infrastructures.

It could also indirectly affect SaaS, because PaaS and IaaS offerings are often the foundation of SaaS. To develop and deliver SaaS offerings, SaaS providers rent or purchase computing capabilities from PaaS or IaaS providers. SaaS offerings deployed on victim VMs would also be vulnerable to VM hopping, affecting availability. It could also endanger SaaS confidentiality and integrity if the users' data is falsified when the attacker gains access to the target VM.

VM Mobility

The contents of VM virtual disks are stored as files such that VMs can be moved or copied from one host to another over the network or via portable storage devices without physically stealing a hard drive.[4] VM mobility provides quick deployment but could lead to security problems, such as the quick spread of vulnerable configurations, which an attacker could exploit to jeopardize the security of a new host.

Several types of attacks exploit vulnerabilities in VM mobility—including man-in-the-middle attacks.[9] Attack severity ranges from leaking sensitive information to completely compromising the guest OS. Also, because VM mobility offers increased flexibility, it similarly increases the complexity of security management.

In the IaaS model, a provider offers underlying hardware and resources as a service, and a user can create his or her own computing platform by importing a customized VM image into the infrastructure service. The large scale of IaaS makes VM mobility's impact on confidentiality and integrity in the cloud potentially larger than in a conventional IT environment. On the other hand, SLAs could reduce the complexities raised by VM mobility if they clearly stated the shared obligations of service providers and users for security management.

A PaaS provider offers a provider-designated computing platform and solution stacks to service users. The users exploit the libraries and APIs to develop their own applications on a fixed computing platform with importing their own VM images. Although PaaS depends on virtualization as a key implementation technology, it doesn't support VM mobility, so this service model doesn't have the same the security challenges as a conventional IT environment. Nevertheless, SaaS and PaaS confidentiality, integrity, and availability are still exposed to the threats raised from IaaS.

VM Diversity

Virtualization lets a user efficiently create many VMs, but securing and maintaining the VMs is difficult owing to the wide range of OSs that can be deployed in seconds.[4,7] VM diversity makes VM security management a challenge, but SLA constraints could help address this issue.

In IaaS, a service provider must ensure security and robustness of the services and hypervisor, while the user must properly configure his or her VM image and secure the service offerings. In other words, the user should share the responsibility of keeping the guest OS patched and updated. Because IaaS scatters the responsibilities of a central service provider, it's resistant to the security management issues raised by VM diversity. Similarly, PaaS is robust against VM diversity compared with the conventional IT environment, if the obligations of both the provider and user are explicitly described in SLAs.

VM Denial of Service

Virtualization lets multiple VMs share physical resources, such as CPU, memory disk, and network bandwidth. A denial-of-service (DoS) attack in virtualization occurs when one VM occupies all the available physical resources such that the hypervisor can't support more VMs, and availability is imperiled.

The best approach to preventing a DoS attack is to limit resource allocation using proper configurations. In cloud computing, DoS attacks could still occur, but having service providers set adequate configurations to restrict the resources allocated to the VMs reduces their probability. In addition, it's beneficial to configuration management to have the SLA clearly define service provider and user responsibilities.

Table 1 summarizes the threats and compares the impacts on the conventional IT environment with that of each cloud service model in terms of virtualization attacks. The virtualization attacks don't impact SaaS directly,

Table 1. Security impacts of virtualization in different IT environments.

Virtual machine (VM) vulnerability	Conventional environment	Cloud computing environment		
		SaaS	PaaS	IaaS
VM hopping	Confidentiality	—*	Confidentiality	Confidentiality
	Integrity		Integrity	Integrity
	Availability		Availability	Availability
VM mobility	Confidentiality	—	×**	Confidentiality
	Integrity			Integrity
	Availability			Availability
	Security management			
VM diversity	Security management	—	×	×
VM denial of service	Availability	—	×	×

*No direct impact, though indirect affects are possible
**Reduced occurrence of the vulnerability or alleviated impact

but this doesn't imply that virtualization attacks on PaaS and IaaS can't indirectly affect SaaS. However, in some instances (marked with an "×"), the conditions of the PaaS and IaaS models actually help reduce the vulnerabilities or alleviate their impact.

Our analysis showed that threats associated with VM mobility are reduced in PaaS. Moreover, the challenges of security management in IaaS could be lower than those in a conventional IT environment because of the SLAs. Thus, although virtualization still poses cloud computing security threats, some of the characteristics of cloud service models can inhibit certain virtualization vulnerabilities. We hope our findings help researchers and practitioners explore cloud-specific security issues and design appropriate countermeasures.

Acknowledgments

This work is supported in part by the Trust Center at UC Berkeley; Networked Communications Program, Taiwan; Taiwan Information Security Center; NSC-DAAD (National Science Council-Deutscher Akademischer Austausch Dienst) Sandwich Program (NSC grant 99-2911-I-009-053-2); and National Science Council (NSC grants 100-2219-E-009-005 and 99-2218-E-009-017).

References

1. P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, tech. report, Information Technology Laboratory, National Institute of Standards and Technology, 2009.
2. M. Christodoresch et al., "Cloud Security Is Not (Just) Virtualization Security: A Short Paper," *Proc. 2009 ACM Workshop on Cloud Computing Security* (CCSW 09), ACM Press, 2009, pp. 97–102.
3. B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding Cloud-Computing Vulnerabilities," *IEEE Security and Privacy*, vol. 9, no. 2, 2011, pp. 50–57.
4. T. Garfinkel and M. Rosenblum, "When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments," *Proc. 10th Workshop on Hot Topics in Operating Systems* (HotOS 05), USENIX Assoc., 2005.
5. D. Hyde, *A Survey on the Security of Virtual Machines*, project report, Apr. 2009; http://www1.cse.wustl.edu/~jain/cse571-09/ftp/vmsec/index.html.
6. K. Owens, "Securing Virtual Computer Infrastructure in the Cloud," white paper, Savvis Communications Corp., 2009.
7. A. Jasti et al., "Security in Multi-Tenancy Cloud," *Proc. IEEE Int'l Carnahan Conf. Security Technology* (ICCST 10), IEEE Press, 2010, pp. 35–41.
8. T. Ristenpart et al., "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," *Proc. 16th ACM Conf. Computer and Communications Security* (CCS 09), ACM Press, 2009, pp. 199–212.
9. J. Oberheide, E. Cooke, and F. Jahanian, "Empirical Exploitation of Live Virtual Machine Migration," *Proc. Black Hat DC 2008 Convention*, 2008; www.net-security.org/dl/articles/migration.pdf.

Hsin-Yi Tsai *is a PhD student at the Institute of Electrical Control Engineering of National Chiao Tung University. Her research interests include evaluation of protection techniques, risk assessment of networks, and design of security metrics. Tsai received her MS in electrical and control engineering from the National Chiao Tung University. She is a member of the Phi Tau Phi Society. Contact her at hytsai.ece96g@nctu.edu.tw.*

Melanie Siebenhaar *is a research staff member at the Multimedia Communications Lab (KOM) at Technische*

Universität Darmstadt. Her research focuses on quality of service—in particular, on cloud computing service-level agreements. Siebenhaar received a diploma degree with distinction jointly in computer science and business administration (Dipl.-Wirtsch.-Inform.) from Technische Universität Darmstadt. Contact her at melanie.siebenhaar@kom.tu-darmstadt.de.

André Miede *is an associate researcher with the E-Finance Lab and Multimedia Communications Lab partnership at Technische Universität Darmstadt. His research focuses on security for cloud computing and the Internet of Services, especially on attacks and countermeasures. Miede received his PhD in information technology from Technische Universität Darmstadt. He's a member of IEEE and the ACM. Contact him at andre.miede@kom.tu-darmstadt.de.*

Yu-Lun Huang *is an assistant professor in the Department of Electrical Engineering of National Chiao Tung University. Her research interests include wireless security, secure testbed design, embedded software, embedded operating systems, risk assessment, secure payment systems, VoIP, and QoS. Huang received her PhD in information engineering from the National Chiao Tung University. She's a member of the Phi Tau Phi Society. Contact her at ylhuang@cn.nctu.edu.tw.*

Ralf Steinmetz *is a professor of multimedia communications at Technische Universität Darmstadt. Together with more than 30 researchers, he has been working toward the vision of seamless multimedia communications. Steinmetz received his PhD in electrical engineering from Technische Universität Darmstadt. He's the International Council for Computer Communication (ICCC) governor and a fellow of IEEE and the ACM. He's also a member of the Scientific Council of Madrid Institute for Advanced Studies (IMEDA) and president of the Board of Trustees of IMDEA. Contact him at ralf.steinmetz@kom.tu-darmstadt.de.*