Misuse Patterns for Cloud Computing

Keiko Hashizume
Florida Atlantic University
777 Glades Road
Boca Raton, FL, USA
ahashizu@fau.edu

Nobukazu Yoshioka
GRACE Center, NII
2-1-2 Hitotsubashi, Chiyoda-ku
Tokyo, Japan
nobukazu@nii.ac.jp

Eduardo B. Fernandez
Florida Atlantic University
777 Glades Road
Boca Raton, FL, USA
ed@cse.fau.edu

ABSTRACT
Cloud Computing is a new computing structure that allows providers to deliver services on demand by means of virtualization. We are studying some security attacks in cloud computing by describing them in the form of misuse patterns. A misuse pattern describes how an information misuse is performed from the point of view of the attacker. It defines the environment where the attack is performed, how the attack is performed, countermeasures to stop it, and how to find forensic information to trace the attack once it happens. We are building a catalog of misuse patterns and we present here two of them: Resource Usage Monitoring (complete) and Malicious Virtual Machine Creation (partially). We discuss also the value of having such a catalog.

Categories and Subject Descriptors
C.2.0 [**Security and protection**]: Computer-Communication Networks – General.

General Terms
Security.

Keywords
Cloud computing, misuse patterns, security, monitoring, virtual machine.

1. INTRODUCTION
The Internet has developed very fast during the last decade. The cost of storage is increasing as well as the cost of the power consumed by the hardware [1]. Thus, organizations need new solutions. Cloud computing is a new paradigm that improves the utilization of resources and decrease the power consumption of hardware by allowing users the sharing of these resources. Cloud computing allows users to have access to resources, software, and information using any device that has access to the Internet. The users consume these resources and pay only for the resources they use.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.
AsianPLoP '11, October 05 - 08 2011, Tokyo,Japan
Copyright 2011 ACM 978-1-4503-2109-9/11/10…$15.00.

Virtualization is a key feature for cloud computing, which attempts to offer a secure, reliable, scalable, shared, and manageable environment. Virtualization allows many virtual machines to run on a single physical machine. Virtual machines are created and monitored by a Virtual Machine Monitor, which is a software layer that mediates between the software and the hardware. Virtualization lets users create, copy, share, migrate, and roll back virtual machines, which may provide significant benefits to them. However, it also comes with new security problems. Cloud providers must undertake a substantial effort to secure their systems in order to minimize these threats. In this work, we characterize some of these threats.

In order to design secure systems we first need to understand possible threats to our system. In [2] we proposed an approach to identify threats based on the goals of the attacker with respect to the information assets of the system. However, we also need to understand what components of the system may be compromised or used by an attacker and how to react to the attack. For this purpose we have proposed misuse patterns [3]. A misuse pattern describes how an information misuse is performed from the point of view of the attacker. It defines the environment where the attack is performed, how is the attack performed, countermeasures to stop it, and how to find forensic information to trace the attack once it happens. Misuse patterns are useful for developers because once they determine that a possible attack can happen in the environment, a corresponding misuse pattern will indicate what security mechanisms are needed as countermeasures. Also, misuse patterns can be very useful for forensic examiners to determine how an attack is performed, and where they can find useful evidence information after the attack has happened. An important value of misuse patterns is that they describe the components of the system where the attack is performed using class diagrams and sequence diagrams, so there is a clear correspondence to the system units.

We present in this work two examples of misuse patterns that describe attacks found in cloud computing environments. One of the vulnerabilities that is inherent in cloud computing is the co-location of virtual machines, where an attacker's virtual machine tries to reside in the same server of the victim's virtual machine with purposes of misuse, such as information inference based on resource usage (leakage of information). Moreover, sharing Virtual Machine Images is one of the new threats that cloud computing is facing. Virtual Machine Images are prepackaged software templates that are used to instantiate virtual machines. Thus, these images are the foundation of the overall security of the cloud [4]. Cloud providers offer a repository service where providers and users can store their images. Users can either create their own image, or they can use any image stored in the repository. An attacker who creates a valid account can create an

image containing malicious code such as a Trojan horse. If another customer uses this image, the virtual machine that he creates will be infected with the hidden malware. This malware can then perform a variety of misuses. These patterns are part of an ongoing catalog that can be used by cloud systems designers to consider security aspects during the construction of such systems. Our contributions here are two misuse patterns and suggestions on how to use these patterns in building secure cloud systems.

Section 2 presents the reader a template used to describe misuse patterns. In Section 3, we present two misuse patterns for cloud computing: Resource Usage Monitoring Inference and Malicious Virtual Machine Creation. The first pattern is presented complete but for the second pattern we present only some sections due to space limitations. In Section 4, we present some discussion and motivate the value of these patterns, while in section 5 we offer some conclusions and possible future work.

2. TEMPLATE FOR MISUSE PATTERNS

This section describes each part of the template for misuse patterns.

2.1 Name

The name of the pattern should correspond to the generic name given to the specific type of attack in standard attack repositories such as CERT.

2.2 Intent or thumbnail description

A short description of the intended purpose of the pattern (what problem it solves for an attacker).

2.3 Context

The context describes the generic environment including the conditions under which the attack may occur. This may include minimal defenses present in the system as well as typical vulnerabilities of the system. The context can be specified using a deployment diagram of the relevant portions of the system as well as sequence or collaboration diagrams that show the normal use of the system. A class diagram may show the relevant system structure. We can list specific preconditions for an attack to happen.

2.4 Problem

From an attacker's perspective, the problem is how to find a way to attack the system. An additional problem occurs whenever a system is protected by some defense mechanisms. The forces indicate what factors may be required in order to accomplish the attack and in what way; for example, which vulnerabilities can be exploited. Also, which factors may obstruct or delay accomplishing the attack.

2.5 Solution

This section describes the solution of the hacker's problem, i.e., how the attack can reach its objectives and the expected results of the attack. UML class diagrams show the involved units of the system under attack. Sequence or collaboration diagrams show the exchange of messages needed to accomplish the attack. State or activity diagrams may add further detail.

Affected system components (Where to look for evidence) (targets)

This is a new section compared to standard security patterns. The solution should not be a comprehensive representation of all components and relationships involved in an attack. Rather, the solution should represent all components that are involved in the attack, are important to prevent the attacks, or are essential to the forensic examination. This can be represented by a class diagram that is a subset or superset of the class diagram of the context.

2.6 Known uses

Specific incidents where this attack occurred are preferred but for new vulnerabilities, where an attack has not yet occurred, specific contexts where the potential attack may occur are enough.

2.7 Consequences

Discusses the benefits and drawbacks of a misuse pattern from the attacker's viewpoint. Is the effort and cost of the attack commensurate with the results obtained? This is an evaluation that must be made by the attacker when deciding to perform the attack; the designers should evaluate the risk to their assets using some risk analysis approach. The enumeration includes good and bad aspects and should match the forces.

2.8 Countermeasures and Forensics

This section describes the security measures necessary in order to stop, mitigate, or trace this type of attack. This implies an enumeration of which security patterns are effective against this attack. From a forensic viewpoint, it describes what information can be obtained at each stage tracing back the attack and what can be deduced from this data in order to identify this specific attack. Finally, it may indicate what additional information should be collected at the involved units to improve forensic analysis.

2.9 Related Patterns

Discusses other misuse patterns with different objectives but performed in a similar way or with similar objectives but performed in a different way.

3. MISUSE PATTERNS FOR CLOUD COMPUTING

3.1 Resource Usage Monitoring Inference in Cloud Computing

Intent

Cloud systems allow many virtual machines to share the same physical infrastructure. An attacker's virtual machine may be placed in the same hardware as the victim's virtual machine to obtain some information such as estimate traffic rates or detect cache activity spikes. Also, the attacker may request many resources, so others customers that are sharing the same resources cannot have them available when needed (Denial of Service).

Context

In Infrastructure as a Service (IaaS) in clouds, physical infrastructure is shared by multiple virtual machines. IaaS is accessible through the Internet, and it provides a computer infrastructure that consists of physical storage and processing capabilities. A Virtual Machine Monitor (VMM) creates virtual machines and provides isolation between them.

Problem
To perform some types of misuse it is necessary to have a virtual machine co-located with the target's virtual machine in the same physical structure (availability zone). How to assign a machine to be located in the same hardware as the victim's virtual machine? Once the attacker's virtual machine is placed on the same hardware as the victim's virtual machine, how the attacker can deduce information by monitoring the victim's behavior?

The attack can be performed by taking advantage of the following vulnerabilities:

- Any person can open an account and create a VM.
- Knowing when a VM is running helps the attacker by informing him when the victim is running.
- The attacker should be able to receive unlimited resources as needed.
- Any resource that is shared by different virtual machines can become a channel that will provide some information that can be useful to infer something about any co-located virtual machine.

Solution
When the user requests a virtual machine, he specifies a region and may either choose an availability zone or is assigned one on his behalf. Also, the user specifies a VM instance type that indicates a combination of computational power, memory and persistent storage. The VMM creates a virtual machine that is assigned to a particular server located in the region specified by the user.

Like any other customers, an attacker can simply request to rent an infrastructure, and he can run and control virtual machines in the cloud. The attacker can successfully locate his virtual machine in the same hardware as the victim, and then learn some information by monitoring some channels. For example, In Amazon's EC2 and other clouds, it is more likely that an availability zone corresponds to a certain range of IP addresses [5]. Knowing the IP address of the victim, the attacker can determine the location of the VM and create his VM in the same zone. The attacker can observe the behavior of the victim, such as traffic rate or cache activity and deduce some information. Also, after being able to be located in the same hardware, the attacker can request for more resources to the provider making the provider run out of resources (a Denial of Service attack).

In order for the attacker to determine the victim's IP address, systems such as EC2 map public IP addresses to private IP addresses through their DNS services. As a result, the attacker can make DNS queries in EC2 in order to find the required internal IP addresses. In [5], they conducted a survey of public servers on EC2 and they identified four distinct IP address prefixes. Then, they performed a TCP either to port 80 or port 443. From the IP addresses that corresponded to these ports, they performed a DNS lookup using the EC2's DNS.

Structure
Figure 1 shows a class diagram for the virtual machine structure in cloud computing. A User creates one or more Accounts in order to use the Provider's infrastructure. The Provider is composed of a Hypervisor, Hardware (server, storage and network), and DNS (Domain Name System). The Virtual Machine Monitor (VMM) creates Virtual Machines (VM) and assigns their instances to the users who requested them. When the instance is launched, it is assigned to a physical server and given other hardware resources. The Virtual Machine passes system calls to the Virtual Machine Monitor which executes those calls in the Hardware.

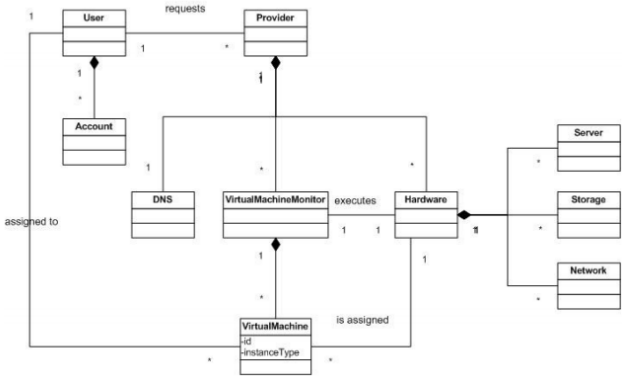

Figure 1. Class Diagram for Virtualization in Cloud Computing.

Dynamics
UC1: Create a Virtual Machine for a user (Figure 2)

Summary: The Provider creates a Virtual Machine for a user.
Actor: User
Precondition: The user must have an account with the Provider
Description:

a) The User requests to the Provider to create a virtual machine. He specifies the physical location and the type of the instance.
b) The Provider checks if the user has an account and redirects the request to the Hypervisor.
c) The Virtual Machine Monitor creates an instance of the Virtual Machine and assigns it to a server and to the user.

Postcondition: A Virtual Machine is created in the specified location and assigned to a server and to the user.

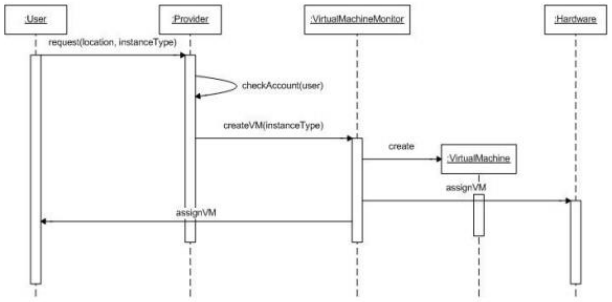

Figure 2: Sequence Diagram for the use case Create a Virtual Machine

UC2: Infer some of the victim's information by monitoring his resource usage (Figure 3)

Summary: An attacker's virtual machine is located in the same hardware as the victim's virtual machine.
Actor: Attacker

Precondition: The attacker must have an account and know some information about the victim such as her public IP in the cloud
Description:

a) The Attacker requests to the Provider's DNS to map the victim's public IP address to his private IP address.
b) The Provider returns the private IP address to the Attacker.
c) The Attacker finds out victim's information such as physical location and instance type.
d) The Attacker requests to rent an infrastructure from the Provider. He specifies the physical location and the instance type which are the same as the ones obtained in step (c).
e) Do the same as the Use Case 1
f) The Attacker can now observe the resource usage and make some inference.

Postcondition: The attacker's virtual machine is created and assigned to the same hardware where the
victim's virtual machine resides, and the attacker can infer some of the victim's information.

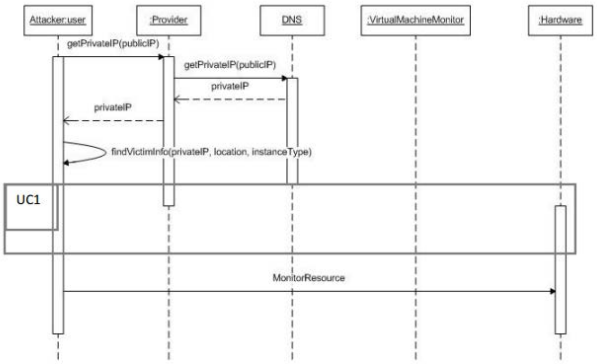

Figure 3: Sequence Diagram for the use case Infer some of the victim's information by monitoring his resource usage

Consequences

The success of this attack implies:

- Basically, anyone who has a valid credit can request a virtual machine from a provider. For example, in Amazon's EC2, a user creates an account using his email account and a valid credit card. Thus, an attacker can create and control virtual machines in the cloud.
- Attackers can take advantage of knowledge about the target location because the DNS provides such information. A DNS's provider can map public IP addresses to local IP addresses.
- Different physical locations are likely to correspond to different local IP addresses and the same may be true for instance types as well.
- Any physical resource that multiplexes between the attacker and the target can be a potentially useful channel: data cache, network access, CPU branch predictors and instruction cache, DRAM memory bus, CPU pipelines, scheduling of CPU cores and time slices, disk access, etc. This information could be used by a competitor to deduce an imminent product announcement, a company reorganization, or another significant institution event.
- Servers in cloud computing environments only run when needed, so an attacker can look at the status of the server and see if any virtual machine instances are running. This can make his work more efficient.
- Cloud computing offers pay as you go services where users can get more or less resources on demand. Thus, the attacker can request for more resources making other co-located users not to be able to get more computing from the cloud when needed (denial of service).

Possible sources of failure include:

- There is a possibility that an attacker's instance is not assigned to the same server as the victim's instance even when we know the location and the type of the victim's instance. That location can UC1 be composed of many servers and the same types of instances can be assigned to different servers.
- Some defenses described in the next section can stop this attack.
- In some clouds, users could request their virtual machines to be assigned on hardware that only can be occupied by virtual machines of their accounts.

Countermeasures

Resource Usage Monitoring Inference can be stopped by the following countermeasures:

- Verify the background of the user when opening an account; however, this is very hard to do and may reduce the economic incentives of the provider.
- Assign random local IP addresses to the instances, so the attacker will not associate a local IP address to a certain location or instance type.
- Control access to the DNS map.
- Control access to resource usage monitoring.
- Monitor the utilization of the infrastructure so all users get some portion of the computing in the cloud.

From the victim's perspective, cloud customers cannot monitor other customers' computations to protect themselves against timing side-channel, and the provider cannot monitor their customers' computations due to privacy concerns. However, [6] proposes a new approach to reduce the risk of timing channel in clouds.

From the point of view of the cloud provider, covert channel and side channel attacks cannot be detected since they rely on legitimate use of the system [7]. However, cloud providers can mitigate these types of attacks; two possible solutions are proposed in [7].

Forensics

Where can we find evidence of this attack?

- Providers can keep logs of the requests made by the users.
- Providers can keep logs of the co-located virtual machines that are assigned to the same server.

Related Patterns

- The Virtual Machine Monitor [8] provides isolation between different virtual machines that execute different operating systems.
- Resource Assignment patterns can be used for assigning servers to users.

3.2 Malicious Virtual Machine Creation

Intent

A Virtual Machine Image is a type of virtual appliance that is used to instantiate a Virtual Machine (VM). Virtual Machine Images

contain initial file system state and software for the machine. An attacker may create a virtual machine image that contains malicious code so it can infect other users when they create their virtual machines. The attacker may read also confidential data from images that are publicly stored in the provider's repository.

Context
Some IaaS (Infrastructure as a Service) providers offer a VM image repository where users can retrieve images in order to initialize their VM. These VM Images can be created and published by the provider or by a client.

Problem
To perform some types of misuse it is necessary to be able to create and publish VM images.
The attack can be performed by taking advantage of the following vulnerabilities:

- Any person who has a valid account can create and register a VM image.
- There should be a common place where the users can share VM images.
- VM images contain prepackaged software components for an application. Thus, an attacker can create a VM image with malicious code.
- VM images contain installed and fully configured applications. The configuration may require sensitive operations such as creating username and password [4].

Solution
When a user publishes a VM image as public, any other user of the cloud is able to use it to instantiate his VM. This VM image can contain malicious code such as Trojan horse. The Virtual Machine Monitor (VMM) will run this image in order to instantiate the user's VM. Now, the attacker can have control of the virtual machine and perform malicious activities such as infect other computers. Infected virtual machines may appear briefly, infect other virtual machines, and disappear before they can be detected [9]. Also, since users can store their VM images in the provider's repository, these images can be accessed by "anyone". Thus, an attacker can retrieve these images and get some confidential information if any.

Structure
The class diagram for this pattern is almost the same as Figure 1 plus classes for WMImage and VMRepository.

Dynamics
Two use cases here are UC1: Publish a Malicious Virtual Machine Image and UC2: Launch a VM using an infected VM Image but we omit them for lack of space. The rest of the pattern has also been omitted for the same reasons.

4. CONCLUSIONS AND FUTURE WORK

Cloud computing is a new concept that presents some benefits for its users; however, it also raises some security problems which may slow down its adoption. We have presented some cloud computing threats as a form of misuse patterns which describe in a systematic way how two cloud misuses are performed. Virtualization, a key component for cloud, has been one of the hottest topics lately. Virtualization enables clouds to improve the utilization of physical resources by sharing resources among different users. This sharing of resources among different virtual machines gives some opportunities to attackers to monitor confidential information. Also, sharing virtual machine images, virtual appliances that contain prepackaged software used to initialize the virtual machine, can lead to several types of misuse. Virtual machine images may contain malicious code that can be propagated once a user executes one of these malicious images.

We will continue developing misuse patterns for cloud environments in order to create a relatively complete catalog for it that can be used by designers of secure cloud environments. Traditional security mechanisms may not be sufficient to mitigate these threats. Thus, we need to develop new approaches and we intend to develop patterns for new defenses as well as extend existing misuse patterns to include the new patterns as defenses. Finally, we intend to incorporate these patterns into a secure systems design methodology.

5. ACKNOWLEDGMENTS

We thank our shepherd, K.V. Dinesha, for his useful comments that helped improve this paper. This work was supported in part by the NSF (grants OISE-0730065). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect those of the NSF. This work was also supported by the National Institute of Informatics of Japan.

6. REFERENCES

[1] S. Zhang, X. Chen, et al, "Cloud Computing Research and Development Trends", *2010 Second International Conference on Future Network. 2010*

[2] F. Braz, E.B.Fernandez, and M. VanHilst, "Eliciting security requirements through misuse activities" *Procs. of the 2nd Int. Workshop on Secure Systems Methodologies using Patterns (SPattern'07)*. In conjunction with the 4th International Conference onTrust, Privacy & Security in Digital Business (TrustBus'07), Turin, Italy, September 1-5, 2008. 328-333.

[3] E.B. Fernandez, N. Yoshioka, and H. Washizaki, "Modeling misuse patterns", *4th Int. Workshop on Dependability Aspects of Data Warehousing and Mining Applications (DAWAM 2009),* in conjunction with the 4th Int.Conf. on Availability, Reliability, and Security (ARES 2009). March 16-19, 2009, Fukuoka, Japan

[4] J. Wei, X. Zhang, et al, "Managing Security of Virtual Machine Images in a Cloud Environment", *2009 ACM Cloud Computing Security Workshop (CCSW) at CCS*. November 13, 2009. Chicago, Illinois, USA.

[5] T. Ristenpart, et al, "Hey, You, Get Off of my Cloud: Exploring Information Leakage in Third-Party Compute Clouds", *Procs. of ACM CCS'09,* 2009, Chicago, Illinois, November 9-13. 199-212

[6] A. Aviram, S. Hu, B. Ford, and R. Gummadi, "Determinating Timing Channel in Compute Clouds", *Proceedings of the 2010 ACM Workshop on Cloud Computing Security*.

[7] Z. Wang and R. Lee, "Covert and Side Channel due to processor architecture", *Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC'06)*, December 2006

[8] E.B.Fernandez and T. Sorgente, "A pattern language for secure operating system architectures", *Proceedings of the*

5th Latin American Conference on Pattern Languages of Programs, Campos do Jordao, Brazil, August 16-19, 2005, 68-88.

[9] T. Garfinkel and M. Rosenblum, "When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments", *Proceedings of the 10th conference on Hot Topics in Operating Systems*. June 12-15, 2005. Santa Fe, NM