Cloud Computing Security

Rajendra Kachhwaha
rajendra1983@gmail.com

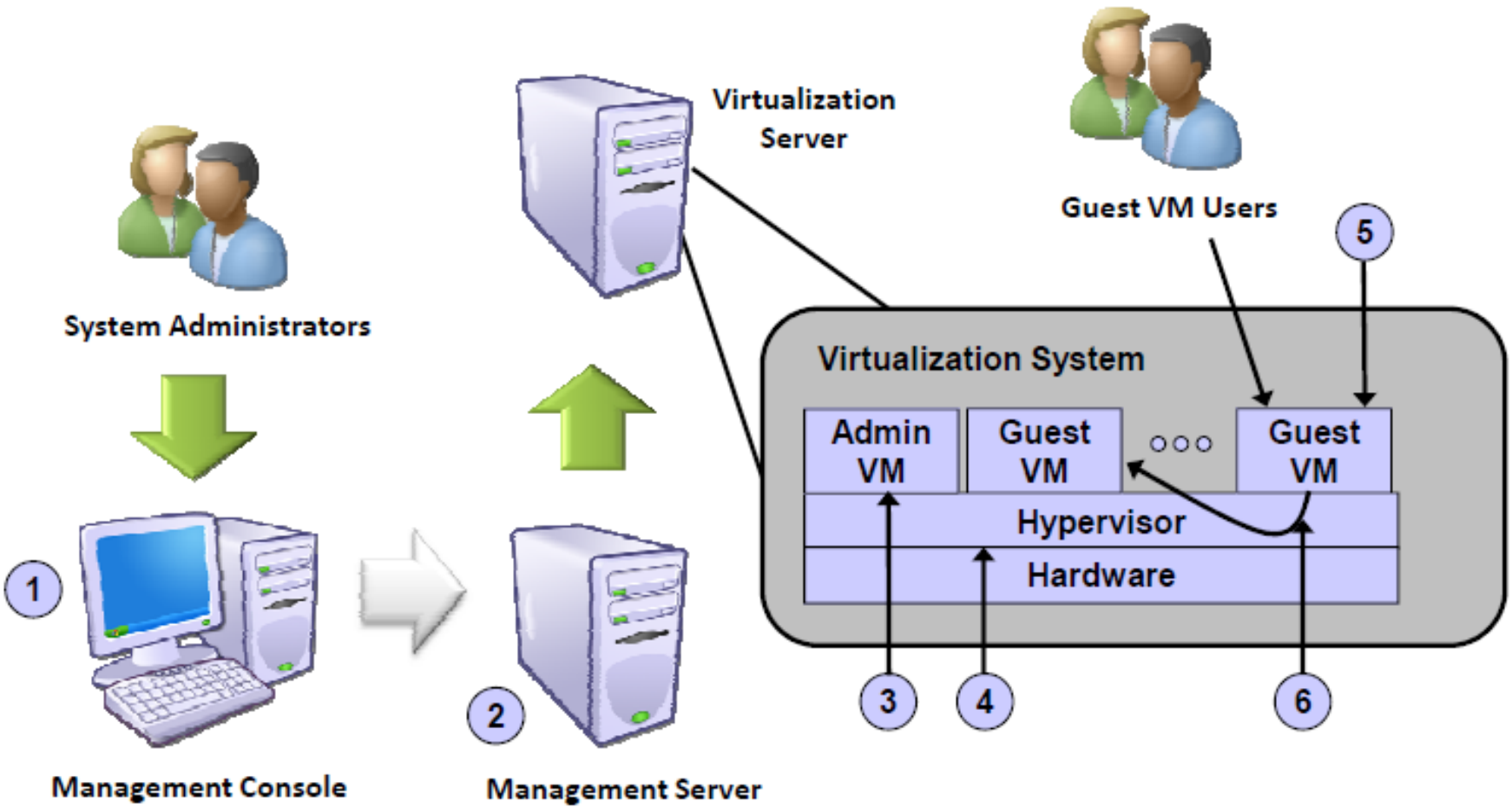
January 30, 2017

Outline

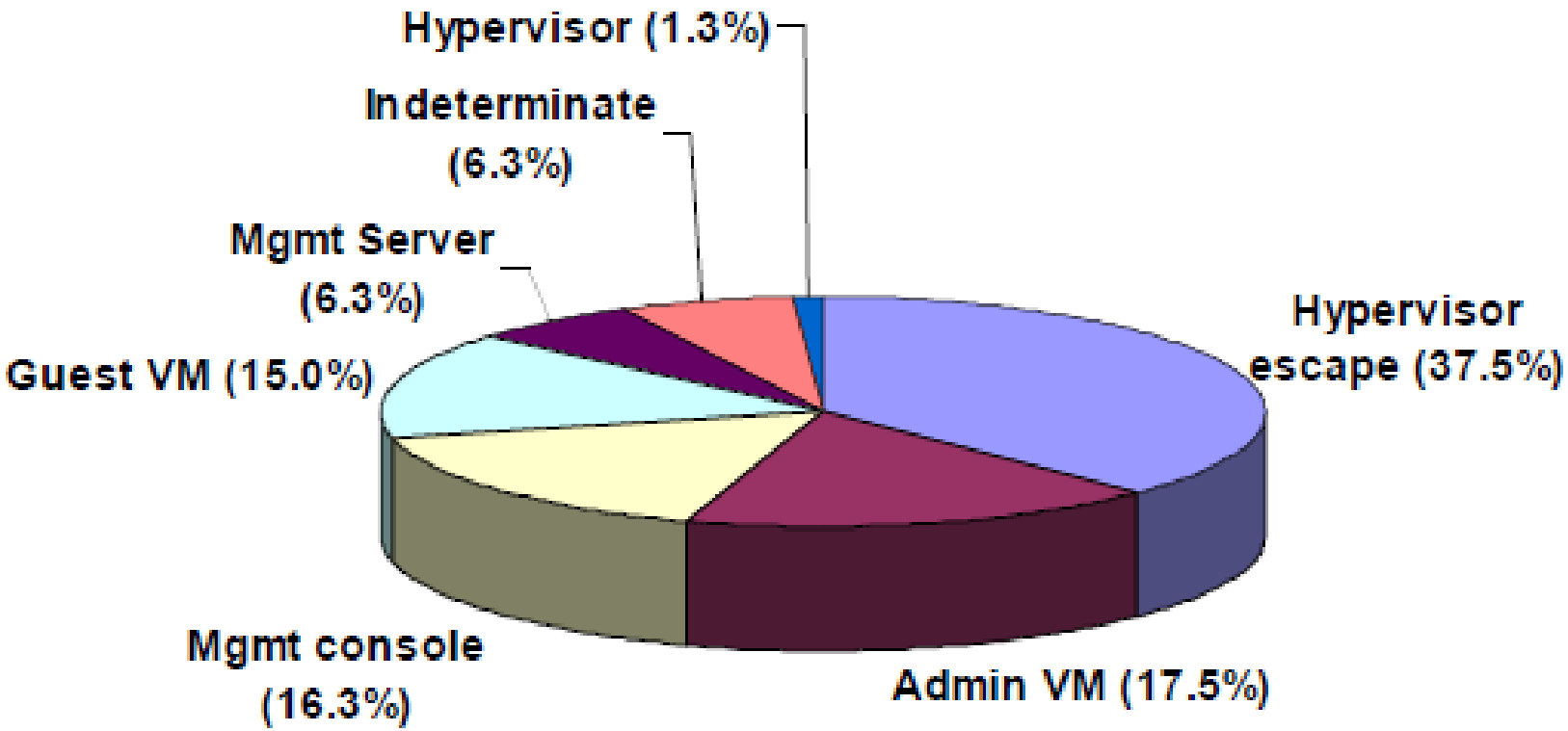
Virtualization System Vulnerability Classes

1. Management console vulnerabilities
2. Management server vulnerabilities
3. Administrative VM vulnerabilities
4. Hypervisor vulnerabilities
5. Guest VM vulnerabilities
6. Hypervisor escape vulnerabilities

Virtualization System Vulnerability Classes



Production Virtualization System Vulnerabilities By Class



Virtualization System Vulnerability Classes

1. Management console vulnerabilities:
   - Affect the management console host
   - Can provide platform or information allowing attack of management server
   - Can occur in custom consoles or web applications
2. Management server vulnerabilities:
   - Potential to compromise virtualization system configuration
   - Can provide platform from which to attack administrative VM
3. Administrative VM vulnerabilities:
   - Compromises system configuration
   - In some systems (like Xen), equivalent to a hypervisor vulnerability in that all guest VMs may be compromised
   - Can provide platform from which to attack hypervisor and guest VMs
4. Guest VM vulnerabilities:
   - Affect a single VM
   - Can provide platform from which to attack administrative VM, hypervisor, and other guest VMs
5. Hypervisor vulnerabilities:
   - Compromise all guest VMs

Virtualization System Vulnerability Classes

6. Hypervisor escape vulnerabilities:
   - A type of hypervisor vulnerability
   - Classified separately because of their importance
   - Allow a guest VM user to escape from own VM to attack other VMs or hypervisor
   - Violate assumption of isolation of guest VMs

Known Virtualization System Attacks

1. Management server attacks:
   - Exploit management console vulnerabilities that divulge password information.
   - Exploit management console vulnerabilities to gain access to management server.
   - Exploit vulnerabilities that allow local management server users to gain elevated privileges.
2. Administrative VM attacks exploit vulnerabilities to:
   - Cause a denial of service by halting the system.
   - Cause a denial of service by crashing the administrative VM.
   - Obtain passwords that are stored in cleartext.
   - Exploit buffer overflows in exposed services to execute arbitrary code.
   - Exploit vulnerable services to gain elevated privileges.
   - Bypass authentication
3. Guest VM attacks exploit vulnerabilities to:
   - Gain elevated privileges.
   - Crash the virtual machine.
   - Truncate arbitrary files on the system.
   - Execute arbitrary code with elevated privileges.

Known Virtualization System Attacks

4. Hypervisor attacks exploit vulnerabilities to:
   - Cause the hypervisor to crash.
   - Escape from one guest VM to another.

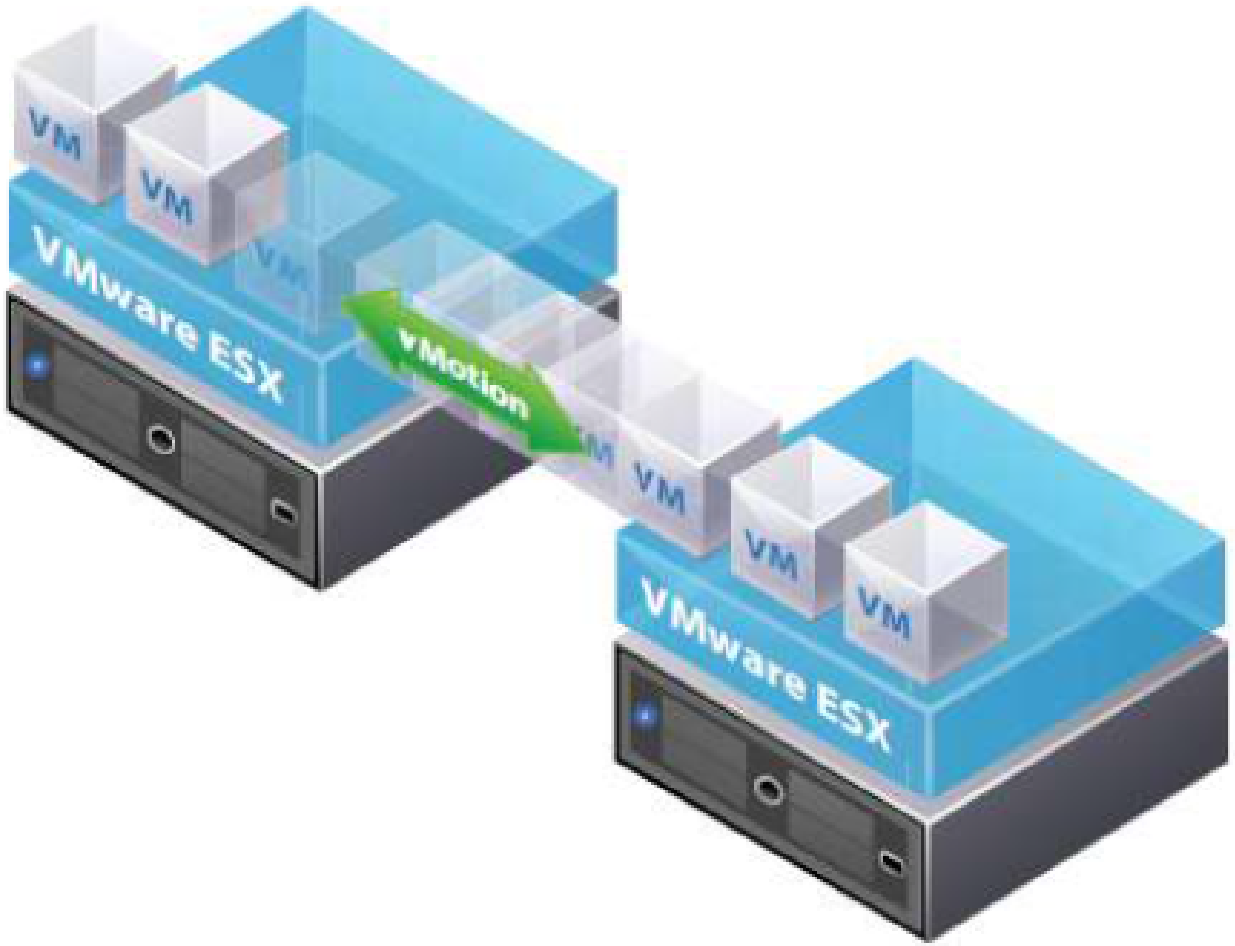
Virtualization System Vulnerability Examples

1. Management console:
   A cross-site scripting vulnerability in a VMware web console allows remote attackers to steal cookie-based authentication credentials.
2. Management server:
   VMware Virtual Center management server can allow a local attacker to use directory traversal sequences to gain elevated privileges.
3. Administrative VM:
   A buffer overflow in a VMWare management service running in the administrative VM could allow remote authenticated users to gain root privileges.
4. Hypervisor:
   By modifying the processor status register, a local attacker can cause the Xen kernel to crash.
5. Guest VM:
   A bug in the handling of page fault exceptions in VMware ESX Server could allow a guest VM user to gain kernel mode execution privileges in the guest VM.
6. Hypervisor escape:
   An error in the virtual machine display function on VMware ESX Server allows an attacker in a guest VM to execute arbitrary code in the hypervisor.

Virtualization System-Specific Attacks

1. VM jumping/guest hopping:
   - Attackers take advantage of hypervisor escape vulnerabilities to jump from one VM to another.
2. VM attacks:
   - Attacks during deployment and duplication
   - Deletion of virtual images
   - Attacks on control of virtual machines
   - Code/file injection into virtualization file structure
3. VM migration:
   - VM migration is transfer of guest OS from one physical server to another with little or no downtime.
   - Implemented by several virtualization products.
   - Provides high availability and dynamic load balancing.
   - Google the process/steps for VM migration for cloud.

Virtualization System-Specific Attacks



Virtualization System-Specific Attacks

1. VM migration attack:
   - If migration protocol is unencrypted, susceptible to man-in-the-middle attack
   - Allows arbitrary state in VM to be modified
   - In default configuration, XenMotion is susceptible (no encryption)
   - VMwares VMotion system supports encryption
   - Proof-of-concept attacks:
     Proof-of-Concept is typically developed by security researchers, academics, and industry professionals to demonstrate possible vulnerabilities in software and operating systems, and to show the security risks of a particular method of attack. Malicious hackers develop and exploit the code to attack vulnerable applications, networks and systems. (POC vulnerabilities example: Virtualization platform vulnerability allowing the execution of arbitrary code to escape virtual machines. (CVE-2015-3456))