*Chapter 2.1*

# Vulnerabilities and controls in cloud

# Aim

To equip the students with basic concepts of vulnerabilities and controls in cloud

# Instructional Objectives

Objectives of this chapter are:

- Explain the types of cloud security vulnerabilities
- Explain the security mitigation controls in the cloud
- Describe the need for Cloud Trust Protocol

# Cloud security vulnerabilities

# Cloud Security Vulnerabilities

- First vulnerability is that, a hacker may attack the computing facility provided by cloud through illegal activities.
- Another major security risk of cloud models is data loss.
- Third risk is that, traditional network attack strategies may be applied to attack different cloud models.

# Misuse of cloud computational resources

- In order to conduct cyber-attacks on computer systems, huge amount of computing power is required. So hackers used multiple computers to develop huge computing power.
- Brute force attack and Denial of service attack are examples of the attacks which uses the power of cloud computing.
- A brute force attack is a technique used to break passwords using powerful computing capability.
- Denial of Service (DoS) attempt to interrupt a host or network resources so that an authorized user cannot access it.

# Data Breaches

- Security threats may occur from both inside and outside of an organization.
- The reason for inside vulnerabilities are poor enforcement of roles, unclear roles and responsibilities, system or OS vulnerabilities, inappropriate physical security procedures, poor patch management or other application vulnerabilities.

# Cloud Security Attacks

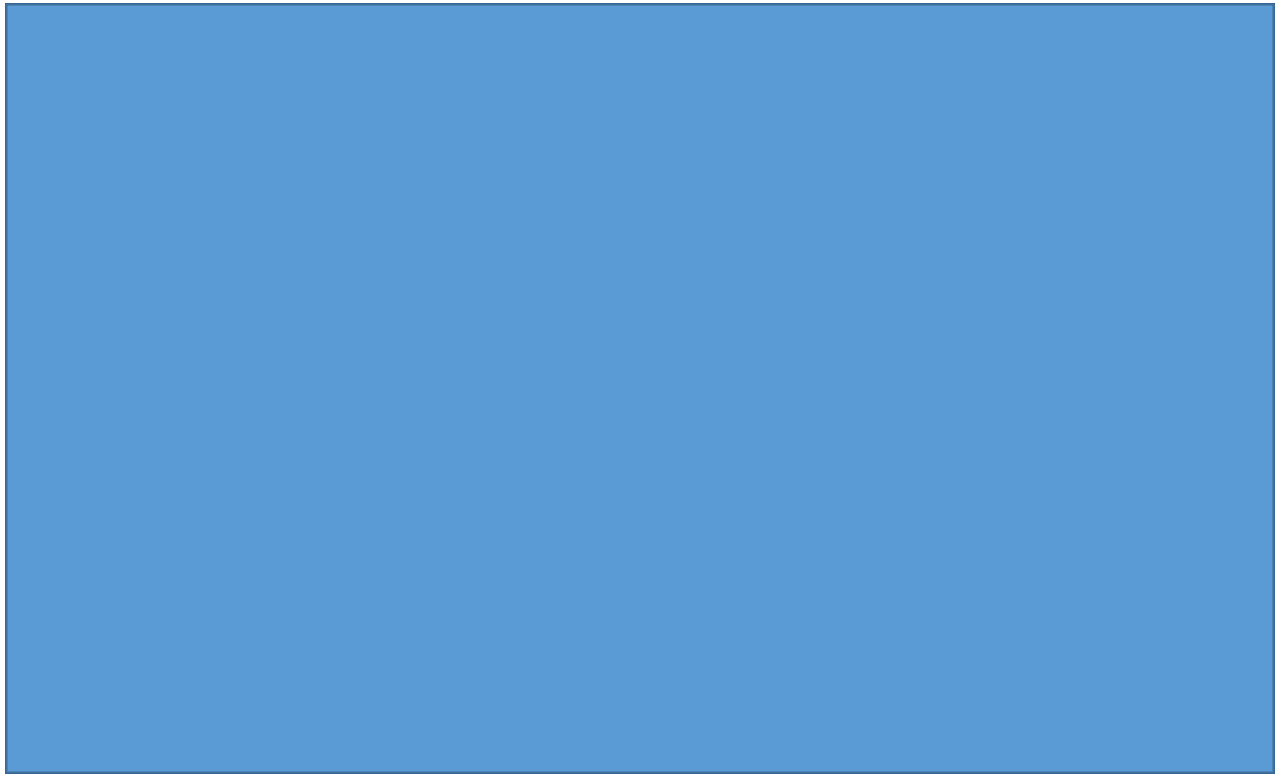
- Internet users get dynamic webpages from web based applications to access application servers using a web browser. These application servers are vulnerable to web based attacks.
- These attacks include information leakage and improper error handling, failure to restrict URL access, broken authentication and session management, improper data validation, malicious file execution and insecure communications.
- There are two categories of cloud security attacks. They are **malware injection attack** and **wrapping attack**.

# Cloud Service Provider Risks

Several areas of risk to virtualized systems are listed below.

- Complexity of configuration
- Privilege escalation
- Inactive virtual machines
- Segregation of duties
- Poor access controls

# Video Lecture



*Click the image to view the video lecture.*

# Video Lecture Explanation

# Quiz / Assessment

1) Which of the following cloud model helps users to customize a realistic environment which includes virtual machines running with different operating systems?

   a) IaaS
   b) PaaS
   c) TaaS
   d) SaaS

2) What are the categories of cloud security attacks?

3) List the different cloud service provider risks

# Cloud Security Mitigation Controls

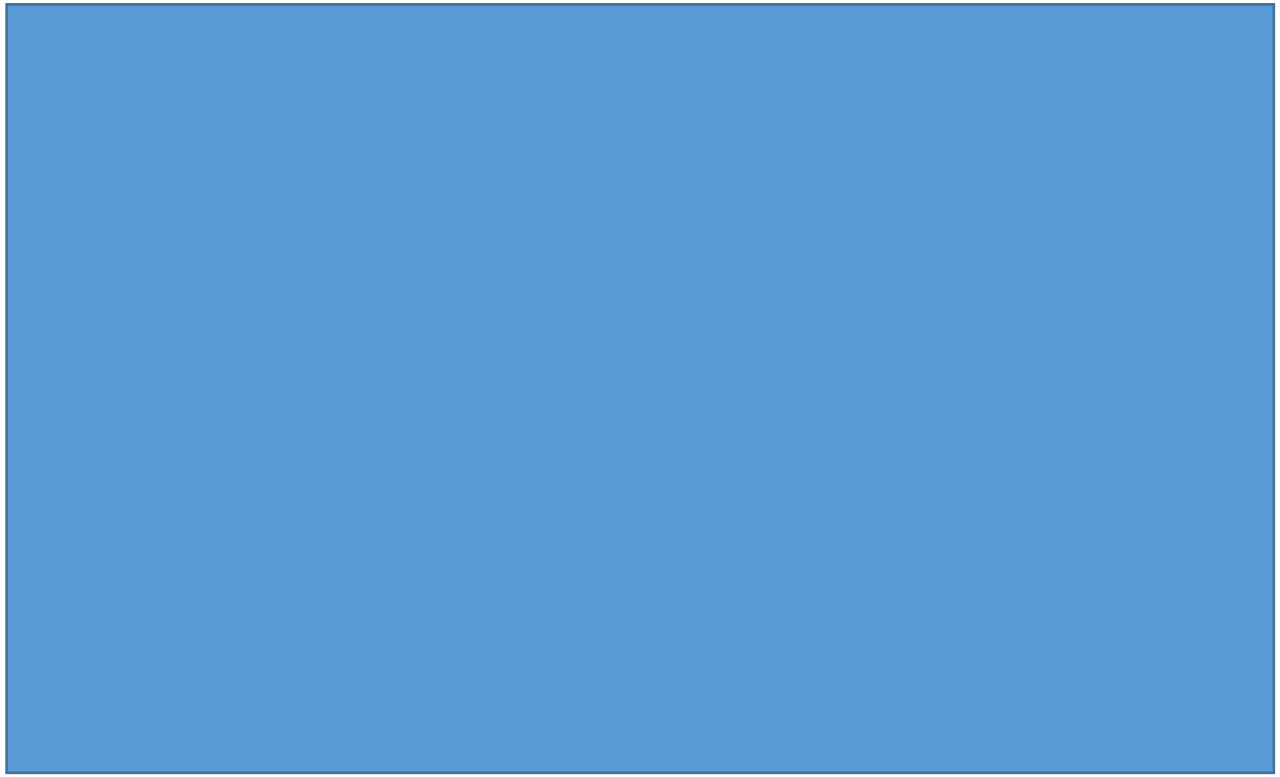
# Cloud Security Mitigation Controls

- Security policy enhancement
- Access management
- Data protection
- Security techniques implementation

## Best Security Practices

- Hardening the Virtual Machine
- Harden the Hypervisor
- Root secure the monitor
- Implement only one primary function per VM
- Firewall any additional VM ports
- Harden the host domain
- Use unique NICs for sensitive virtual machines
- Disconnect unused devices

# Video Lecture



*Click the image to view the video lecture.*

# Video Lecture Explanation

# Quiz / Assessment

1) Which of the following is a tool used to control access to cloud applications and data?

   a) HTML
   b) SAML
   c) XML
   d) SGML

2) List security practices that are unique to virtualized systems.

# Cloud Trust Protocol

# Cloud Trust Protocol

Cloud Trust Protocol (CTP) is a mechanism by which cloud users request and receive information about the factors of transparency as applied to cloud service providers.

By using cloud trust protocol, cloud users get a way to detect important parts of information which is called the *elements of transparency*

These information gave evidence about necessary security configuration and operational characteristics for the systems located in the cloud

Cloud Trust Protocol is a simple asynchronous protocol that follows a question and answer pattern. CTP is controlled by the cloud service users and this protocol is presented to all cloud service providers.

This deployment of the CTP from cloud consumers is itself a cloud capability known as *Transparency-as-a-service* (TaaS).

# Elements of Transparency in the CTP V2.0

Six types

15 Families

24 elements

# CTP Version 2.0 Element Types

- Initiation
- Evidence requests
- Policy introduction
- Provider assertions
- Provider notifications
- Client extensions

# CTP Version 2.0 - Families

1. Identity/ Session
2. Configuration
3. Vulnerability
4. Anchoring
5. Audit Log
6. Service management
7. Service Statistics
8. Provider capability and service claims
9. Alerts
10. Users and Permissions
11. Configurations
12. Anchoring
13. Quotas
14. Alerts
15. Client defined

# CTP Version 2.0 - Elements

1. Identify service owner and initiate evidence session
2. Terminate evidence (CTP) session
3. What is current configuration for {Hypervisor? Guest Oss? Virtual switches? Virtual firewalls? IDS?}
4. How does current configuration of {service unit type} differ from {service owner configuration specification/policy}
5. Results of latest vulnerability assessment on {hypervisor; guest OSs, virtual switches, virtual firewalls}
6. Date of latest vulnerability assessment on {hypervisor; guest OSs, virtual switches, virtual firewalls}
7. Perform vulnerability assessment now on {hypervisor; guest OSs, Virtual switches, virtual firewalls}

# CTP Version 2.0 – Elements

8) Provide geographic location and affirmation (by unit identity)
9) Provide platform separation affirmation and identities (by unit identity)
10) Provide process separation affirmation-positive or negative-(by process name- e.g., storage encryption, storage de-duplication, backup,…)
11) Provide log of policy violations {in last 'n' hours} (e.g., malware elimination, unauthorized access attempts, …)
12) Provide audit/event log {for last 'n' hours}
13) Provide list of currently authorized users/subjects and their permissions
14) Provide incident declaration and response summary {for last n hours}
15) Provide indicator/record of changes made and/or changes requested but not made (change control/ configuration control)
16) Provide application and/or service unit statistics that are collected and recorded as a standard output of the application or service unit

# CTP Version 2.0 – Elements

17) Deliver the list of claimed service capabilities available from this provider.
18) Deliver an alert for all confidentiality, integrity and availability events/ thresholds identified by the service owner concerning all cloud service units being used in support of the service owner
19) Provide declaration of user types, permissions and provisioning/ de-provisioning sources
20) Provide configuration standards to be applied
21) Provide anchoring needs for geographic, process, and platform anchoring
22) Provide quotas for use
23) Provide fundamental event/ threshold declarations to serve as alert stimuli
24) An additional set of question/answer elements defined and negotiated in agreement between cloud consumer and cloud providers

# Quiz / Assessment

1) The deployment of the CTP from cloud consumers is itself a cloud capability known as ________________________

   a) Software as a Service
   b) Infrastructure as a Service
   c) Platform as a Service
   d) Transparency as a Service

2) List various elements of transparency in CTP version 2.0.

# Activity

Activity can be either offline or online

**Offline Activity**
**(30 min)**

- Make a group of 4 and discuss various security vulnerabilities and their mitigating controls.

*Note: Refer Table of Content for the activities*

# Summary

- ✓ Services such as web-based e-mails or social networking sites are example for cloud computing services.
- ✓ Tools used to control access to cloud applications and data are authentication standards, Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML).
- ✓ One of the major security concern in cloud computing is the malware injection attack. It can be prevented by using File Allocation Table (FAT) system architecture.
- ✓ Cloud Trust Protocol (CTP) is a mechanism by which cloud users request and receive information about the factors of transparency that is applied to cloud service providers.
- ✓ By using cloud trust protocol, cloud users can detect important parts of information regarding security, compliance, privacy and integrity. These information is called the elements of transparency.

# e-References

1) http://www.cloudcomputing-news.net/news/2014/nov/21/top-cloud-computing-threats-and-vulnerabilities-enterprise-environment/
2) http://www.issa-dv.org/meetings/presentations/2011-12-09/2011-12-09_Presentation_01_Lingenfelter.pdf
3) http://eval.symantec.com/mktginfo/enterprise/white_papers/b-mitigating_security_risk_in_the_cloud_WP.en-us.pdf

# External Resources

1. *Kris James (2013), Cloud Computing. Library of Congress*
2. *Barrie Sosinsky (2011), Cloud Computing Bible A –Wiley publication*
3. *RajkumarBuyya, James Broberg, AndrzejGoscinski (2011) -Cloud Computing: Principles And Paradigms–Wiley publication*
4. *Tim Mather, SubraKumaraswamy, ShahedLatif (2009) - Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance –O'Reilly publication*
5. *Cengage Learning (2011), Virtualization Security- EC-Council press*