Cloud Information security fundamentals

- *It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.*
- *Information security is the confidentiality, integrity, and availability of information.*
- aspect of information security
  - *organizational security*
  - *asset classification*
  - *personnel security*
  - *physical security*

Confidentiality is the prevention of unauthorized disclosure of information

Integrity aims at ensuring that information is protected from unauthorized or unintentional alteration, modification, or deletion.

Availability aims to ensure that information is readily accessible to authorized user

Figure: Quick View of CIA definitions

Cloud security services

- 10 categories of security services that can be offered over the cloud

1. **Identity and Access Management**
2. **Data Loss Prevention**
3. **Web Security**
4. **E-mail Security**
5. **Security Assessments**
6. **Intrusion Management**
7. **Security Information and Event Management**
8. **Encryption**
9. **Business Continuity and Disaster Recovery**
10. **Network Security**

Cloud Security Design Principles

1. Least Privilege
2. Separation of Duties
3. Defense in Depth
4. Fail Safe
5. Economy of Mechanism
6. Complete Mediation
7. Open Design
8. Least Common Mechanism
9. Psychological Acceptability
10. Weakest Link
11. Leveraging Existing Components

Cloud Security Design Principles

1. Least Privilege

- The principle of *least privilege* maintains that an individual, process, or other type of entity should be given the minimum privileges and resources for the minimum period of time required to complete a task

2. Separation of Duties

- *Separation of duties* requires that completion of a specified sensitive activity or access to sensitive objects is dependent on the satisfaction of a plurality of conditions. For example, an authorization would require *signatures of more than* one individual.

Cloud Security Design Principles (Cont...)

3. Defense in Depth

- *Defense in depth* is the application of multiple layers of protection wherein a subsequent layer will provide protection if a previous layer is breached.

4. Fail Safe

- *Fail safe* means that if a cloud system fails it should fail to a state in which the security of the system and its data are not compromised

5. Economy of Mechanism

- It promotes simple and comprehensible design and implementation of protection mechanisms, so that unintended access paths do not exist or can be readily identified and eliminated.

Cloud Security Design Principles (Cont...)

6. Complete Mediation

- every request to access must undergo a valid and effective authorization procedure.
  1. Identification of the entity making the access request.
  2. Verification that the request has not changed since its initiation.
  3. Application of the appropriate authorization procedures.
  4. Reexamination of previously authorized requests by the same entity.

7. Open Design

- exposing the algorithm to review and study by experts at large while keeping the encryption key secret leads to a stronger algorithm.

Cloud Security Design Principles (Cont...)

8. Least Common Mechanism

- a minimum number of protection mechanisms should be common to multiple users, as shared access paths can be sources of unauthorized information exchange.
- Shared access paths that provide unintentional data transfers are known as *covert channels*.
- Thus, the *least common mechanism* promotes the least possible sharing of common security mechanisms.

Cloud Security Design Principles (Cont...)

9. **Psychological Acceptability**
   - *Psychological acceptability* refers to the ease of use and intuitiveness of the user interface that controls and interacts with the cloud access control mechanisms.
10. **Weakest Link**
11. **Leveraging Existing Components**
   - to partition the system into defended subunits. Then, if a security mechanism is penetrated for one sub-unit, it will not affect the other sub-units.

Secure Cloud Software Requirements

- The requirements for secure cloud software are concerned with nonfunctional issues such as
  - minimizing or eliminating vulnerabilities and
  - ensuring that the software will perform as required, even under attack.
- This goal is distinct from security functionality in software, which addresses areas that derive from the information security policy, such as
  - identification,
  - authentication, and
  - authorization.

Secure Cloud Software Requirements (Cont...)

Department of Defense Data and Analysis Center for Software (DACS) state that all software shares the following three security requirements:

1. It must be ***dependable*** *under anticipated* operating conditions, and remain *dependable under hostile* operating conditions.
2. It must be ***trustworthy*** in its own behavior, and in its *inability* to be compromised by an *attacker* through exploitation of vulnerabilities or insertion of malicious code.
3. It must be ***resilient*** enough to ***recover quickly*** to full operational capability with a minimum of damage to itself, the resources and data it handles, and the external components with which it interacts.

6th sem

Cloud Computing Security Challenges

- Cloud computing security challenges fall into three categories:
  - **Data Protection:** Securing your data both at rest and in transit
  - **User Authentication:** Limiting access to data and monitoring who accesses the data
  - **Disaster and Data Breach:** Contingency Planning

Cloud Computing Security Challenges (cont...)

- **DATA PROTECTION**
  - Ensuring the data remains secure both at rest (data residing on storage media) as well as when in transit.
- **USER AUTHENTICATION**
  - Data resting in the cloud needs to be accessible only by authorized users.
  - In order to ensure the integrity of user authentication, companies need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data.

Cloud Computing Security Challenges (cont...)

- **CONTINGENCY PLANNING**
- if a natural disaster or cloud provider fails or goes bankrupt.
  - Can the data be easily retrieved and migrated to a new service provider or to a non-cloud strategy?
  - What happens to the data and the ability to access that data if the provider gets acquired by another company?

Virtualization security Management

- Consumers and CSPs should include traditional security as well as additional security for virtualization.
- **Security benefits due to virtualization**
  - Centralized storage used in virtualized environments prevents a loss of important data if a device is lost, stolen or compromised.
  - When VMs and applications are properly isolated, only one application on one OS is affected by an attack.

Security benefits due to virtualization (Cont...)

- a virtual environment provides flexibility in that it allows the sharing of systems without necessarily having to share critical information across the systems.
- If a VM is infected, it can be rolled back to a prior "secure" state that existed before the attack.
- Hardware reductions that occur due to virtualization improve physical security
- Desktop virtualization can be deployed to better control the user environment. An administrator can create and control a "golden image" that can be sent down to users' computers.

Security benefits due to virtualization (Cont...)

1. Server virtualization can lead to better incident handling since servers can **revert back** to a previous state in order to examine what occurred before and during an attack.
2. The system and network administration's access control as well as **separation of duties** can be improved as certain individuals may be assigned to only control VMs within the network while others only deal with VMs in the **DMZ**.
3. **Hypervisor** software is **small** and not really complex and this provides for a smaller attack surface on the hypervisor itself.
4. Virtual Switches (vswitches) provide additional layer of security.

Common Virtualization Attacks

Denial of Service (DoS)

- can lead to a shutdown of the hypervisor. This can lead to the ability to add a backdoor to allow access to the VMs underneath the hypervisor.

VM Jumping

- If a security hole in the hypervisor occurs and is found, a user logged into one VM can hop over to another VM and gain access to it to look at information or acquire it.

Host Traffic Interception

- Vulnerabilities in the hypervisor can allow for tracking of system calls, paging files, and monitoring of memory and disk activity.

Cloud Computing Security Architecture