UNIT- 4

Date ___/___/___
Page _____

CLOUD SECURITY

① **Cloud Information security fundamentals** –

Developing secure software is based on applying the secure software design principles that form the fundamental basis for software assurance.

The software must exhibit the following three properties to be consider secure –

(1) Dependability
(2) Trustworthiness
(3) Survivability (Resilience)

Seven complementary principles that support information assurance are confidentiality, integrity, availability, authentication, authorization, auditing and accountability.

→ Confidentiality, integrity and availability are sometimes known as the CIA triad of information system security, and are important pillars of cloud software assurance.

→ Confidentiality – It refers to the prevention of intentional or or unintentional authorization disclosure of information. Confidentiality is cloud systems is ~~used~~ related to the areas of intellectual property rights, covert channels, traffic analysis, encryption and inference.

→ Integrity – The concept of cloud information integrity requires that the following three principles are met –

(1) Modifications are not made to data by unauthorized personnel or processes
(2) Unauthorized modifications are not made to data by authorized personnel or process.
(3) The data is internally and externally consistent.

→ Availability – It ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel.

×××× The reverse of confidentiality, integrity and availability is disclosure, alteration and destruction (DAD).

Date ____/____/____
Page _____

② Cloud security services -

Additional factors that directly affect cloud software assurance include

(1) Authentication - It is the testing or reconciliation of evidence of a user's identity.

(2) Authorization - It refers to rights and privileges granted to an individual or process that enables access to computer resources and information assets.

(3) Auditing - To maintain operational assurance, organizations use two basic methods -

(i) A system audit is a one-time or periodic event to evaluate security.

(ii) Monitoring refers to an ongoing activity that examines either the system or the users, such as intrusion detection.

(4) Accountability - It is the ability to determine the actions and behaviors of a single individual within a cloud system and to identify that particular individual. Audit trail or logs support accountability.

③ Design Principles -

The goal is to have a system that is secure enough for everyday use while exhibiting reasonable performance and reliability characteristics.

The following 11 security design principles are -

(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 - It requires that completion of a specified sensitive activity or access to sensitive objects is dependent on the satisfaction of a plurality of conditions.

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

(4) Fail safe - It means that if a cloud system fails it should fail to a state in which the security of the system and its data are compromised.

(5) Economy of mechanism – It promotes simple & comprehensible design and implementation of protection mechanisms, so that unintended access paths do not exist or can be readily identified and eliminated.

(6) Complete Mediation – Every request by a ~~subject~~ to access an object in a computer system must undergo a valid and effective authorization procedure. It includes identification, verification and reexamination.

(7) Open design – An open-access cloud system design that has been evaluated and tested by a myriad of experts provides a more secure authentication method than one that has not been widely accessed.

(8) least common mechanism – It promotes the least possible sharing of common security mechanism which avoids shared access paths for unauthorized information exchange.

(9) Psychological Acceptability – It 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 – It is important to identify the weakest mechanisms in the security chain and layers of defense, and improve them so that risks to the system are mitigated to an acceptable level.

(11) leveraging Existing Components – Two approaches –

(i) Reviewing ~~and~~ the state and settings of the extant security mechanisms and ensuring that they are operating at their optimum design points will greatly improve the security posture of an information system

(ii) Partition the system into defended sub-units.

(4) 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.

In many aspects, ~~to~~ the tool and techniques used to design and develop clean, efficient cloud applications will support the development of secure code as well. Special attention, however, should be shown in the following areas –

(1) Handling data - Some data is more sensitive and requires special handling.
(2) Code practices - Care must be taken not to expose too much information to a would-be attacker.
(3) Language Options - Consider the strengths and weakness of the language used.
(4) Input validation and contention injection - Data (content) entered by a user should never have direct access to a command or a query.
(5) Physical Security of the system - Physical access to the cloud servers should be restricted.

⑤ Policy Implementation -

Cloud software security requirements are a function of policies such as system security policies, software policies, and information system policies.

For proper secure cloud software implementation, these issues have to be accounted for during the software development life cycle and through an effective cloud software security policy. Implementation issues are -

(1) Access Controls
(2) Data Protection
(3) Confidentiality
(4) Integrity
(5) Identification and authentication
(6) Communication Security
(7) Accountability.

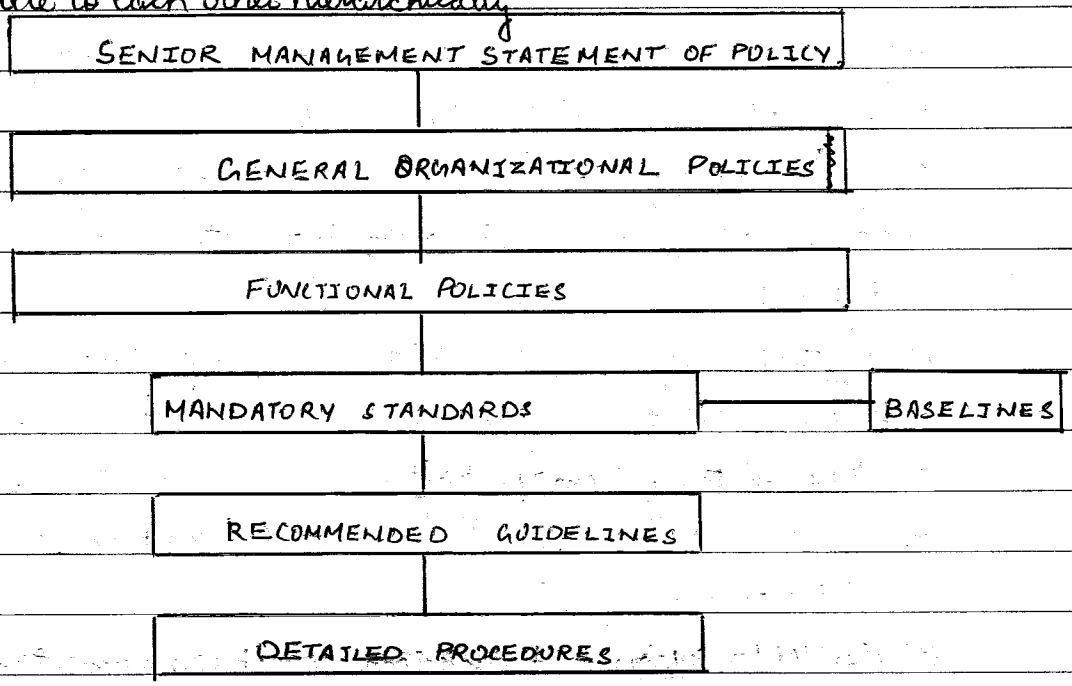
⑥ Cloud computing security challenges -

Some security challenges can and should be addressed through management initiatives. These management initiatives will require clearly delineating the ownership and responsibility roles of both the Cloud Service Provider (CSP) and the organization functioning in the role as customer. Some management initiatives are security policy implementation, computer intrusion detection and response and virtualization security management.

Date ____/____/____
Page _____

→ Security policy implementation -

Security policies are the foundation of a sound security implementation. Policies relate to each other hierarchially -



SECURITY POLICY HIERARCHY

→ Policy Types -

(1) Senior Management statement of Policy -

- General, high-level policy that acknowledges the importance of computing resources to the business model,
- states support for information security throughout the enterprise
- Commits to authorizing & managing the definition of the lower-level standards, procedures and guidelines.

(2) Regulatory Policies -

They are security policies that an organization must implement due to compliance, regulation, or other legal requirements

(3) Advisory Policies -

They are security policies that are not mandated but strongly suggested, perhaps with serious consequences defined for failure to follow them.

(4) Informative Policies -

Policies that exist simply to inform the reader.

Date ____/____/____
Page _____

Virtualization Security Management -

Virtual Threats -

Some threats to virtualized systems are general in nature, as they are inherent threats to all computerized systems. Some of the vulnerabilities exposed to any malicious-minded individuals are -

(1) Shared clipboard - It allows data to be transferred between VMs and the host, providing a means of moving data between malicious programs in VMs of different security realms.

(2) Keystroke logging - Some VM technologies enable the logging of keystrokes and screen updates to be passed across virtual terminals in the VM.

(3) VM monitoring from the host - Because all network packets coming from or going to a VM pass through the host, the host may be able to affect the VM.

(4) VM monitoring from another VM

(5) ~~The~~ VM backdoors - A backdoor, covert communications channel between the guest and host could allow intruders to perform potentially dangerous operations.

Hypervisor Risks - They are -

(1) Rogue Hypervisor - VM-based rootkits can hide from normal malware detection systems by initiating a "rogue" hypervisor and creating a covert channel to dump unauthorized code into the system.

(2) External Modification of the hypervisor - A poorly protected or designed hypervisor may allow direct modifications of the hypervisor by an external intruder.

(3) VM Escape - An improperly configured VM could allow code to completely bypass the virtual environment, and obtain full root or Kernel access access to the physical host.

VM Security Recommendation -

Best Practice Security techniques are -

(1) Hardening the host operating system

(2) Limiting Physical access to the host

(3) Using Encrypted Communications

(4) Disabling Background Tasks.

(5) Updating and Patching
(6) Enabling Perimeter Defense on the VM.
(7) Implementing file integrity checks
(8) Maintaining Backups

→ VM-Specific Security Techniques are -
(1) Hardening the VM
(2) Harden the hypervisor
(3) Root Secure the ~~Manual~~ Monitor
(4) Implement only one primary function per VM
(5) Firewall any additional VM Ports
(6) Harden the host domain
(7) Use Unique NICs for sensitive VMs
(8) Disconnect unused devices
(9) Securing VM Remote access

⑦ Cloud computing Security Architecture -

The Open Security Alliance (OSA) defines security architecture as - "The design artifacts that describe how the security controls (= security countermeasures) are positioned, and how they relate to the overall IT architecture. These controls serve the purpose to maintain the system's quality attributes, among them are confidentiality, integrity, availability, accountability & assurance."

→ Architectural Considerations -

(1) General issues -

(i) Compliance - Cloud vendor should provide transparency to the client by supplying information about storage used, processing characteristics, and other other relevant cloud information.

Another compliance issue is the accessibility of a clients data by the providers system engineers and certain other employees.

(ii) Security Management - Proper cloud security management and administration should identify management issues in critical areas such as access control, vulnerability analysis, change control, incident response, fault tolerance,

disaster recovery and business continuity planning.

(iii) Information classification - It supports disaster recovery and planning and business continuity planning. It also supports privacy requirements and enables regulatory compliance.

Information classification benefits are -

1) Security protections
2) Identify most sensitive or vital information
3) It supports CIA triads
4) Identify which protection applies to which information
5) It might be required for regulatory, compliance, or legal reasons

(iv) Employee termination - The impact of employee terminations on the integrity of information stored in a cloud environment. Typically, there are two types of terminations, friendly and unfriendly, and both require specific actions.

(v) Security awareness, Training and Education - Employees of both the cloud client and the cloud provider must be aware of the need to secure information and protect the information assets of an Enterprise.

All employees need education in the basic concepts of security and its benefits to an organization.

(2) Trusted Cloud Computing -

It can be viewed as a computer security architecture that is designed to protect cloud systems from malicious intrusions and attacks, and ensure that computing resources will act in a specific, predictable manner as intended. Factors that inspire trust include the following -

(i) Use of industry-accepted standards
(ii) Provision of interoperability and transparency
(iii) Robust authentication & authorization mechanisms in access control

(3) Secure Execution Environments and communication -

(i) Proper APIs must be used
(ii) Virtual Private Network (VPN) → Remote access VPNs, Network-to-

Tunneling is a method of transfering data from one network to another network by encapsulating the packets in an additional header.

Date ___/___/___
Page _____

Network VPNs and VPN tunnelling.

(iii) Public Key Infrastructure and Encryption Key Management -

The integration of digital signatures and certificates and the other services required for e-commerce is called the public key infrastructure (PKI). It includes the following elements -

1) Digital certificates
2) Certificate authority (CA)
3) Registration authorities
4) Policies and procedures
5) Certificate Revocation
6) Nonrepudiation support
7) Timestamping
8) lightweight Directory Access ~~Control (LDAC)~~ Protocol (LDAP)
9) Security enabled application.

Components of Key management are -

1) Key distribution can be done by using asymmetric key cryptosystems.
2) Key revocation
3) Key recovery
4) Key renewal
5) Key destruction
6) Multiple Keys.

(4) Microarchitecture -

The design elements of the microprocessor hardware and firmware that provide for the implementation of the higher-level architecture are referred to as microarchitecture. A microarchitecture design might incorporate the following -

(i) Pipelining
(ii) Superscalar Processor
(iii) Very-long instruction word (VIW) processor
(iv) Multiprogramming
(v) Multi tasking
(vi) Multi processing
(vii) Multi threading
(viii) Simultaneous multi threading (SMT)

Date ____/____/____
Page _____

xxaxx

Microarchitectures can be designed as hardware accelerators for functions such as encryption, authentication, and secure web transactions to support cloud computing.

→ Identity Management and Access Control -

There are fundamental functions required for secure cloud computing.

→ Identity Management can be done by using -

(1) Passwords - Static password or dynamic password.

(2) Tokens - Static password tokens, synchronous dynamic password tokens (clock based or counter based), asynchronous tokens (challenge-respo

(3) Memory cards

(4) Smart cards

(5) Biometrics - Fingerprints, Retina scans, Iris scans, Hand geometry, voice, Handwritten signature dynamics.

→ Access control are done by using -

(1) Administrative controls

(2) Logical or technical controls.

(3) Physical controls.

→ Models for controlling access are -

(1) Mandatory access control

(2) Discretionary access control

(3) Non discretionary access control

(4) Single Sign-On (SSO)

→ Autonomic Security -

Autonomic computing refers to a self-managing computing model in which computer systems reconfigure themselves in response to changing conditions and self-healing. It enhanced security and provides recovery from harmful events.

Characteristics of autonomic computing are self-awareness, self-configuring, self-optimizing, self-healing, self-protecting, context-aware, open & anticipatory