UNIT V : SECURITY

1. What are the challenges to establish the trust among grid sites ?
The first challenge is integration with existing systems and technologies.
The second challenge is interoperability with different "hosting environments."
The third challenge is to construct trust relationships among interacting hosting environments.

2. What are the various trust models ?
A Generalized Trust Model
Reputation-Based Trust Model
A Fuzzy-Trust Model

3. What are the various authorities categories?
attribute authorities, policy authorities, and identity authorities.

4. What are the various authentication methods in Grid?
The major authentication methods in the grid include passwords, PKI, and Kerberos. The password is the simplest method to identify users, but the most vulnerable one to use.The PKI is the most popular method supported by GSI. To implement PKI, we use a trusted third party, called the certificate authority (CA).

5. What are the Three Authorization Models
The subject-push model
The resource-pulling model
The authorization agent model

6. What does the GSI authentication certificate include.
(1) a subject name, which identifies the person or object that the certificate represents;
(2) the public key belonging to the subject;
(3) the identity of a CA that has signed the certificate to certify that the public key and the identity both belong to the subject;
(4) the digital signature of the named CA. X.509 provides each entity with a unique identifier.

7. What are the necessary security features of Cloud?
Dynamic web services with full support from secure web technologies
Established trust between users and providers through SLAs and reputation systems
Effective user identity management and data-access management
Single sign-on and single sign-off to reduce security enforcement overhead
Auditing and copyright compliance through proactive enforcement
Shifting of control of data operations from the client environment to cloud providers .
Protection of sensitive and regulated information in a shared environment.

8. Name a few cloud component that needs security?
Protection of servers from malicious software attacks such as worms, viruses, and malware.

Protection of hypervisors or VM monitors from software-based attacks and Vulnerabilities.

Protection of VMs and monitors from service disruption and DoS attacks

Protection of data and information from theft, corruption, and natural disasters

Providing authenticated and authorized access to critical data and services.

9. Differentiate Active and Passive attacks

passive attacks steal sensitive data or passwords.

Active attacks manipulate kernel data structures which will cause major damage to cloud servers.

10. What is cloud security ?

Cloud security is attributed to user confidentiality, data integrity, access control, firewalls, IDSes, defense capability against viruses or worm attacks, reputation systems,copyright protection, data lock-in, APIs, data-center security policies, trust negotiation,and security auditing services.

11. What are the risks of storing data in the Cloud?

- Reliability
- Security
- User error
- Access problems

12. What are the Security Issues in the Cloud

In theory, minimizing any of the issues would help:

a. Loss of Control
b. Lack of trust
c. Multi-tenancy

13. What are Physical and Cyber Security Protection at Cloud/Data Centers ?

Secure data centers and computer buildings
Use redundant utilities at multiple sites
Trust delegation and negotiation
Worm containment and DDoS defense
Reputation system for data centers
Fine-grained file access control
Copyright protection and piracy prevention
Privacy protection

14. what are the security Challenges in VMs

Buffer overflows, DoS attacks, spyware, malware, rootkits, Trojan horses, and worms. In a cloud environment, newer attacks may result from hypervisor malware, guest hopping and hijacking, or VM rootkits, the man-in-the-middle attack for VM migrations.

15. what are the Aspects of Data Security ?

Security for

- Data in transit
- Data at rest
- Processing of data including multitenancy
- Data Lineage
- Data Provenance
- Data remnance

16. State Security at the Network Level.

Ensuring data confidentiality and integrity of the organizations data in transit to and from the public cloud provider

Ensuring proper access control (Authentication, Authorization, Auditing) to resources in the public cloud

Ensuring availability of the Internet facing resources of the public cloud used by the organization

Replacing the established network zones and tiers with domains

17. State Security at the Host Level.

Host security at PaaS and SaaS Level

a. Both the PaaS and SaaS hide the host operating system from end users
b. Host security responsibilities in SaaS and PaaS are transferred to CSP

Host security at IaaS Level

c. Virtualization software security
   i. Hypervisor security
   ii. Threats: Blue Pill attack on the hypervisor
d. Customer guest OS or virtual server security
   i. Attacks to the guest OS: e.g., stealing keys used to access and manage the hosts

18. State Security at the Application Level.

Application security at the SaaS level

a. SaaS Providers are responsible for providing application security

Application security at the PaaS level

b. Security of the PaaS Platform
c. Security of the customer applications deployed on a PaaS platform

Application security at the IaaS Level

d. Customer applications treated a black box
e. IaaS is not responsible for application level security

19. How are the Reputation Systems are classified ?

The reputation systems are classified as centralized or distributed depending on how they are implemented. In a centralized system, a single central authority is responsible for managing the reputation system, while the distributed model involves multiple control centers working collectively. Reputation-based trust management and techniques for securing P2P and social networks could be merged to defend data centers and cloud platforms against attacks from the open network.

Part – B

1. Explain the Trust Models of Grid Security. (16)
2. Explain in detail about Grid Security infrastructure. (16)
3. Explain in detail about cloud security infrastructure. (16)
4. Describe IAM architecture and Practices. (16)
5. Describe IAM standards and Protocols in detail. (16)