CLOUD SECURITY FUNDAMENTALS

MODULE 11

Related Terms

- Confidentiality – refers to keeping data private.
- Integrity – is degree of confidence that data is protected against accidental or intentional alteration without authorization.
- Availability – means being able to use the system as anticipated.
- Accountability – maps action in system to responsible parties.
- Assurance – refers to need of system to behave as expected.
- Resilience – allows to cope with security threats, rather than failing critically.

Privacy and security in cloud

- Cloud computing security is an evolving sub-domain of computer security, network security and broadly information security.
- It refers to broad set of policies, technologies and controls deployed to protect data, applications and the associated infrastructure of cloud computing.

Dimensions of Cloud Security

- Three general areas of Cloud Security are:
  - Security and Privacy
  - Compliance
  - Legal or Contractual Issues

Security and privacy

- In order to ensure security and privacy of data, cloud must attend to following challenges:
  - Data Protection – data from different users are kept segregated.
  - Physical Control – private cloud more secure than public cloud.
  - Identity Management – to control access to information and computing resources.
  - Physical and personnel security – physical machine should be secure. Restrict use to customer data and maintain log of every access.
  - Availability – assurance to customers that they will have regular and predictable access to their data and applications.

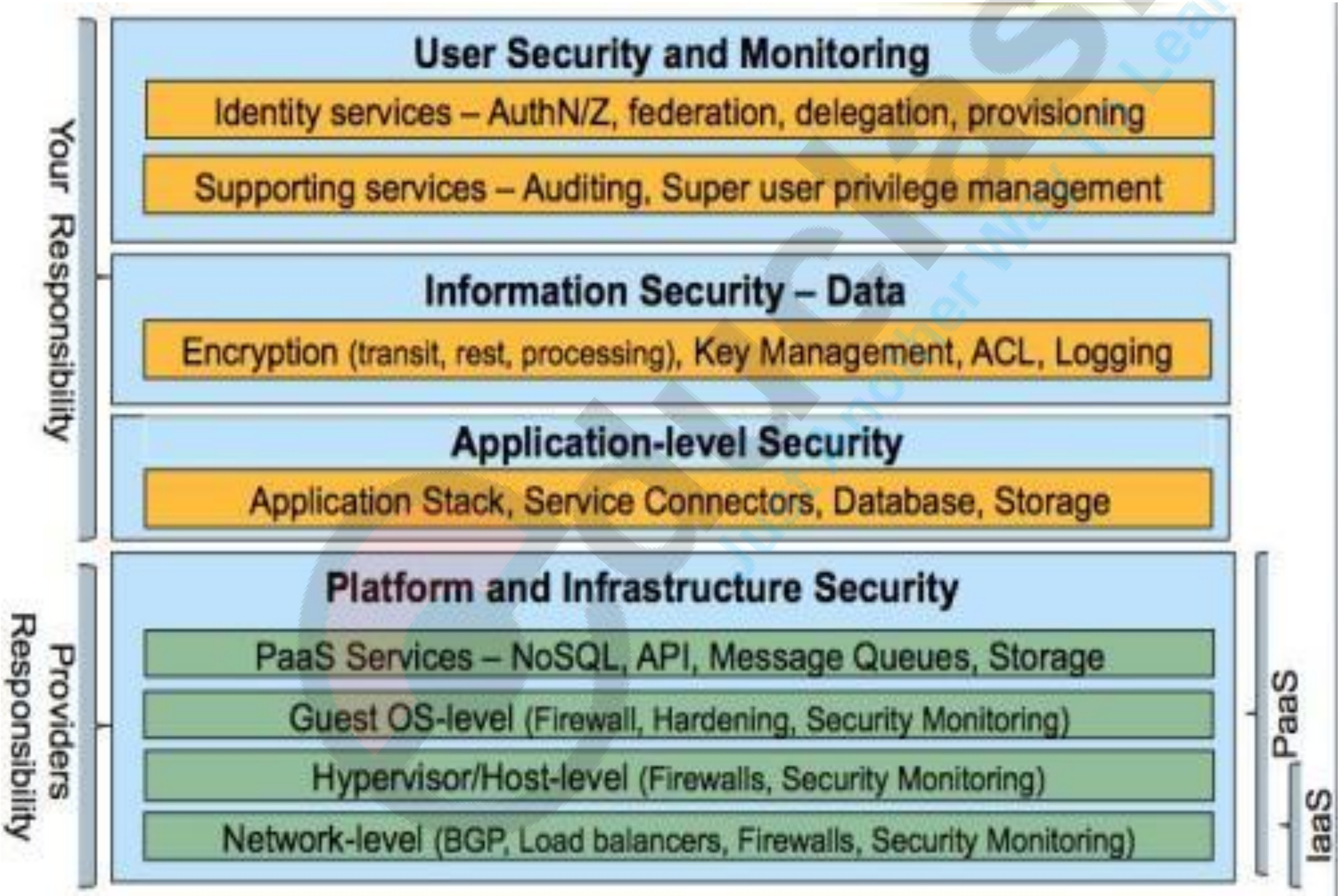
- Application Security – applications available as service are secure.
- Privacy – access given only to authorized users.
- Legal Issues – legal issues such as contracts must be considered.

compliance

- Cloud providers comply appropriately with these regulations:
  - Business Continuity and Data Recovery – ensures that service can be maintained in case of disaster and emergency also.
  - Logs and Audit – logs and audit must be maintained securely for as long as customer needs it.

- **LEGAL AND CONTRACTUAL ISSUES** – cloud providers and their customers need to negotiate terms around how incident involving data loss or any compromise will be resolved.

Security architecture



Your Responsibility

User Security and Monitoring

Identity services – AuthN/Z, federation, delegation, provisioning

Supporting services – Auditing, Super user privilege management

Information Security – Data

Encryption (transit, rest, processing), Key Management, ACL, Logging

Application-level Security

Application Stack, Service Connectors, Database, Storage

Providers Responsibility

Platform and Infrastructure Security

PaaS Services – NoSQL, API, Message Queues, Storage

Guest OS-level (Firewall, Hardening, Security Monitoring)

Hypervisor/Host-level (Firewalls, Security Monitoring)

Network-level (BGP, Load balancers, Firewalls, Security Monitoring)

PaaS

IaaS

Security at various levels

- At infrastructure level: system administrator have all the access rights and can attack the system. System can also be attacked by other unauthorized users.
- Protection Measures:
  - No single person must have all the privileges.
  - Stringent security devices should be deployed.
  - Remote Attestation can be used, a mechanism to detect changes to the user's computers by authorized parties.

- Security at Platform Level: security model on this level relies more on the provider to maintain data integrity and availability. Following security aspects must be taken care of:
  - Integrity
  - Confidentiality
  - Authentication
  - Defense against intrusion
  - SLA

- At application level:
  - Data Security
  - Network Security
  - Regulatory Compliance
  - Data Segregation
  - Availability
  - Backup/Recovery
  - Identity Management and Sign-on Process
- At Data Level: Security from
  - Data corruption
  - Data Loss
  - How to deal??
    - Encryption
    - Periodic Audits
    - Ethical Hacking
    - Vulnerability Testing

Cloud service provider principles

- Security concerns remains number 1 barrier for enterprise cloud adoption.
- Cloud services can be delivered in many flavors, hence the cloud concerns and solutions are context dependent.
- Set of principles applied when evaluating a cloud service provider security maturity.
  - **Disclosure of security policies, compliance and practices - cloud provider follows standard framework such as ISO 27001, SS16 and CSA cloud controls matrix. Scope of control must be disclosed.**

- Disclosure when mandated – cloud service provider should disclose relevant data when disclosure is imperative due to legal or regulatory needs.
- Security Architecture – service provider should disclose security architectural details
- Security Automation – cloud service provider should support security automation, activities such as, exporting/importing security event logs, firewall policies.
- Governance and Security responsibility – responsibility of customers/providers should be clearly articulated.

Identity management and access control

- A single entity can have many identities.
- Identity Management – describes management of individual identities, their authentication, authorization, roles, and privileges/permissions within or across the system.
- Related to how humans are authenticated and authorized across the network.
- Perspectives on IDM
  - The Pure Identity Paradigm
  - The User Access Paradigm
  - The Service Paradigm

Practices to mitigate security risks

- Architect for Security-as-a-service
- Implement sound identity, access management architecture and practice
- Always encrypt or mask sensitive data
- Log, log, log
- Continuously monitor cloud services

Cloud security principles

- Services should follow principles of least privileges.
- Isolation between various security zones should be guaranteed using firewalls
- Applications should use end-to-end transport level encryption (SSL,TLS etc.)
- Applications should externalize authentication and authorization to trusted security services.
- Data masking and encryption should be employed based on data sensitivity.

Probable Questions

- Discuss security architecture of cloud
- What is Identity Management? Discuss different perspectives for that.
- What are the challenges faced for implementing cloud security?
- What are issues in data security in cloud computing? How data can be protected in cloud?