Prof. Alessandro Carrega
alessandro.carrega@unige.it

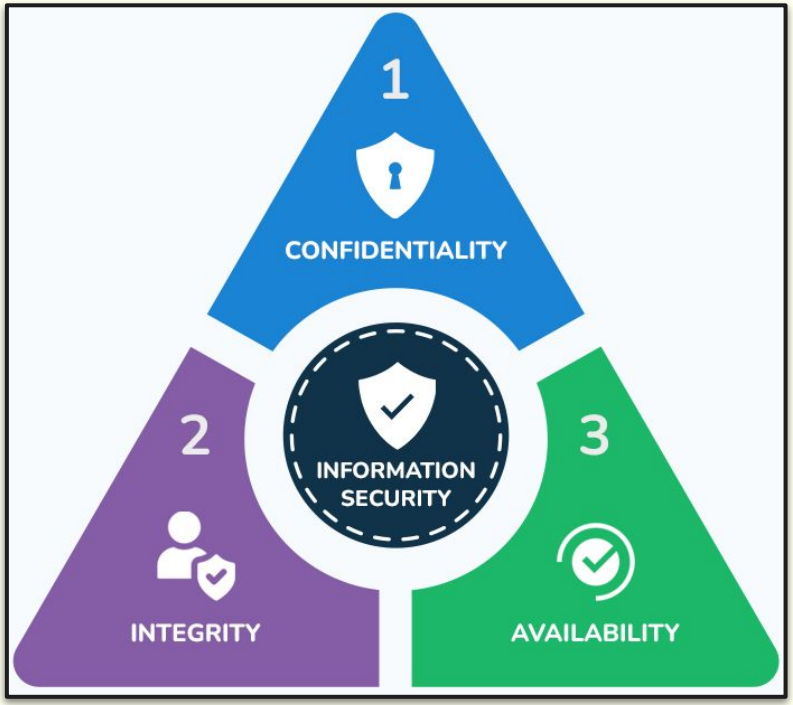
Lesson 03

Fundamental Network Security Concepts

Ph.D. Course in Cyber Security for Cloud Computing
from zero to hero

The CIA triad forms the foundation of information security

By safeguarding confidentiality, integrity, and availability, organizations can protect their critical assets and maintain business continuity.



Network Security

CIA Confidentiality

Protecting information from unauthorized access

Ensuring sensitive data is accessible only to authorized individuals

Examples encryption, access controls, firewalls

Network Security

CIA Integrity

Ensuring the accuracy and completeness of information

Preventing unauthorized modification or deletion of data

Examples hashing, digital signatures, intrusion detection systems

Network Security

CIA Integrity

Ensuring information is accessible when needed

Minimizing system downtime and maximizing uptime

Examples redundancy, load balancing, disaster recovery

Encryption Techniques

A

6

Asymmetric vs Symmetric

Asymmetric

- Key Pair uses a pair of keys: a public key for encryption and a private key for decryption
- Security extremely secure for key exchange and digital signatures, as the private key is never shared
- Speed Slower than symmetric encryption, making it less suitable for large data sets
- Common Algorithms: RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) are popular choices

Symmetric

- Single Key uses one key for both encrypting and decrypting data
- Speed very fast, making it ideal for large data sets
- Security highly secure if the key is kept secret, but key distribution becomes a challenge over long distances or unsecured channels
- Common Algorithms AES (Advanced Encryption Standard) is the most widely used

Encryption Techniques

B

7

Key Exchange

Challenge

How to securely share the encryption key between parties without compromising its secrecy

Diffie-Hellman

- ✖ Famous method where two parties can generate a shared secret key over an insecure channel.
- ✖ Based on mathematical properties of modular arithmetic.

Encryption Techniques

C

8

Hybrid

Combining Strengths	*Key Exchange*	*Data Encryption*
Many systems use a combination of symmetric and asymmetric encryption	Asymmetric encryption is used to securely exchange a symmetric key	The symmetric key is then used to encrypt/decrypt the actual data, leveraging its speed

Encryption Techniques

D

9

Which to Choose?

Symmetric	*Asymmetric*	*Hybrid*
Best for large data sets where key distribution can be managed securely	Ideal for key exchange, digital signatures, and small amounts of data	Often the most practical approach, combining the best of both worlds

Digital Signatures and Certificates

A

10

Main Concept

Digital Signatures

- A mathematical technique used to validate the authenticity and integrity of a digital message or document
- Created using a private key to encrypt a hash of the message
- The recipient verifies the signature using the sender's public key

Digital Certificates

- Electronic documents issued by a trusted third-party Certificate Authority (CA)
- Contain the public key of the certificate holder and information about their identity
- Used to verify the authenticity of digital signatures

Digital Signatures and Certificates

B

11

Authentication and Non-Repudiation

Authentication

- ✖ Verifying the identity of the sender of a message or the owner of a digital certificate
- ✖ Ensures that the message or document originated from a legitimate source

Non-Repudiation

- ✖ Preventing the sender of a message or the signer of a document from denying their actions
- ✖ Provides legal proof of the sender's identity and intent

In the realm of cloud computing, security is paramount

Firewalls and Intrusion Detection Systems (IDS) are two key technologies that play a crucial role in safeguarding cloud infrastructure and applications

Firewalls and IDS

B

13

Firewall

General	*Network*	*Application*
✖ Firewalls act as security barriers, controlling incoming and outgoing network traffic ✖ They examine each packet of data and determine whether to allow or deny its passage based on predefined security rules	• Operate at the network layer of the OSI model, inspecting traffic based on IP addresses, port numbers, and protocol types • They are well-suited for protecting the perimeter of cloud networks	• Operate at the application layer, analyzing the content of traffic to identify and block malicious attacks, such as SQL injection and cross-site scripting (XSS) • Particularly useful in protecting web applications deployed in the cloud

Firewalls and IDS

C

14

IDS

General	*Network-Based IDS (NISD)*	*Host-Based IDS (HIDS)*
✖ Monitors network traffic and system activity for signs of malicious activity ✖ Analyze network packets and system logs to identify potential threats, such as unauthorized access, malware, and denial-of-service (DoS) attacks	✖ Monitor network traffic for suspicious patterns, such as unusual port scans or excessive traffic volume ✖ Deployed at strategic points within the cloud network to capture and analyze traffic.	Monitor the activity on individual hosts, such as virtual machines or servers, to detect signs of compromise, such as unauthorized file access or unusual system behavior

Firewalls and IDS

D

15

Cloud-Specific Considerations

Dynamic Nature

- ✖ Cloud environments are highly dynamic, with resources being constantly provisioned and de-provisioned
- ✖ Security solutions must be able to adapt to these changes automatically

Shared Infrastructure

- ✖ Cloud providers often share physical infrastructure among multiple tenants
- ✖ Robust security measures to isolate tenants and prevent unauthorized access

Distributed Systems

- ✖ Cloud applications are often distributed across multiple servers and data centers
- ✖ Security solutions must be able to monitor and protect these distributed components

In cloud environments, firewalls and IDS must be adapted to the unique characteristics of cloud infrastructure

Firewalls and IDS

E

16

Key Challenges and Best Practices

Configuration Complexity	*Evolving Threat Landscape*	*Performance Impact*
✖ Misconfigurations can leave systems vulnerable to attacks ✖ Essential to implement strong configuration management practices	✖ Cyber threats are constantly evolving ✖ Security solutions must be updated regularly to address new vulnerabilities and attack techniques	✖ Security solutions can impact the performance of cloud systems ✖ Important to choose solutions that have minimal performance overhead

A Virtual Private Network (VPN) is a technology that creates a secure, encrypted connection over a public network, typically the internet

Allows users to send and receive data privately, protecting it from potential interception and unauthorized access

VPN

B

18

How it works?

Encryption	*Tunneling*	*Remote Access*
VPNs encrypt data before it's transmitted over the network, making it unreadable to anyone who might intercept it	The encrypted data is encapsulated within a secure *tunnel* that traverses the public network	VPNs enable remote access to private networks, allowing users to connect to their workplace network from anywhere with an internet connection

VPN

C

19

Types

Remote Access	*Site-to-Site*	*Cloud-Based*
Allows individual users to connect to a private network from a remote location, such as their home or a public Wi-Fi hotspot	Connects two or more private networks over a public network, enabling secure communication between them	Service delivered over the internet, eliminating the need for on-premises hardware and software

VPN

Tunneling Protocols are the methods used to establish and maintain secure VPN connections

D

20

Point-to-Point Tunneling Protocol (PPTP)

Relatively simple but less secure than newer protocols

Layer Two Tunneling Protocol (L2TP)

Provides a framework for tunneling data but relies on other protocols for encryption

IPsec (Internet Protocol Security)

Suite of protocols that provides encryption, authentication, and integrity for IP traffic

Secure Socket Tunneling Protocol (SSTP)

Microsoft protocol that encrypts VPN traffic within an SSL/TLS tunnel

OpenVPN

Open-source protocol that offers strong security and flexibility

WireGuard

Relatively new protocol, known for its simplicity, speed, and security

VPN

E

21

Key Benefits in Cloud Environments

- ✖ Crucial role in cloud computing by providing secure access to cloud resources and protecting sensitive data
- ✖ Cloud providers often offer VPN services as part of their platform, allowing users to connect to their virtual networks and resources securely

Enhanced Security

VPNs encrypt data, making it difficult for unauthorized individuals to intercept and decrypt

Anonymity

Can mask your IP address, making it harder for others to track your online activities

Remote Access

Enable remote access to private networks, improving flexibility and productivity

Bypassing Geo-Restrictions

Can help you bypass geographic restrictions and access content that may be blocked in your region

RBAC

A

22

How it works in the Cloud

Role Definition

Cloud providers define predefined roles (e.g., Administrator, Developer, User) or allow organizations to create custom roles with specific permissions

Role Assignment

Users are assigned to appropriate roles based on their job functions and responsibilities

Permission Inheritance

Users inherit the permissions associated with their assigned roles

Access Enforcement

Cloud platform enforces access controls by verifying a user's role and permissions before granting access to resources

RBAC

B

Least Privilege Principle

- ✖ The least privilege principle dictates that users should be granted only the minimum level of access necessary to perform their tasks
- ✖ This principle helps mitigate the risk of unauthorized access and data breaches

RBAC

C

24

Applying Least Privilege in Cloud Environments

Role-Based Access Control

- ✖ Define granular roles with specific permissions
- ✖ Assign roles to users based on their job requirements
- ✖ Regularly review and update role assignments to ensure they remain appropriate

Resource-Level Permissions

- ✖ Implement fine-grained access controls at the resource level (e.g., specific files, databases, virtual machines)
- ✖ Limit access to resources to only those who need it

Time-Based Access Controls

- ✖ Implement time-based access controls to restrict access to specific time periods
- ✖ Use multi-factor authentication (MFA) for additional security

Regular Review and Auditing

- ✖ Regularly review and audit access controls to identify and address potential vulnerabilities
- ✖ Monitor user activity and log access attempts to detect and respond to security incidents

RBAC

D

25

Benefits

Enhanced Security

reduces the risk of unauthorized access and data breaches

Improved Efficiency

streamlines access management and reduces administrative overhead

Compliance Adherence

helps organizations comply with regulatory requirements.

Scalability

Easily adapts to changing business needs and organizational growth

SIEM

A | for Cloud Security | 26

A Security Information and Event Management (SIEM) system is a critical tool for enhancing security in cloud environments

It consolidates and analyzes security data from various sources, including cloud infrastructure, applications, and network devices

This centralized approach enables organizations to detect and respond to potential threats more efficiently

SIEM

B

Key Features and Benefits

27

Automated Incident Response

- ✖ Triggers automated responses to detected threats, such as blocking IP addresses or terminating compromised accounts
- ✖ Integrates with security orchestration, automation, and response (SOAR) platforms for streamlined incident handling

Centralized Log Management

- ✖ Collects and aggregates logs from diverse sources (cloud providers, virtual machines, applications)
- ✖ Normalizes and indexes logs for efficient search and analysis

Real-time Threat Detection

- ✖ Utilizes advanced analytics and machine learning to identify anomalies and potential security breaches
- ✖ Correlates events across different systems to uncover complex attack patterns

Compliance and Audit

- ✖ Provides detailed reports and audit trails to ensure compliance with industry regulations (e.g., HIPAA, PCI DSS, GDPR)
- ✖ Facilitates security audits and assessments

Enhanced Visibility

- ✖ Offers a unified view of security posture across the entire cloud environment
- ✖ Identifies security gaps and misconfigurations

SIEM

C

28

Cloud-Native Solutions

Cloud-native SIEM solutions are specifically designed for cloud environments, offering the following advantages

Security

built with robust security measures to protect sensitive data

Cost-Effectiveness

pay-as-you-go pricing models and reduced infrastructure overhead

Scalability

Easily adapts to changing workloads and data volumes

Performance

Leverages cloud infrastructure for high-performance analysis

SIEM

Scalability

Ensure the solution can handle your organization's growing data volumes and evolving security needs

Incident Response Automation

Support automated response actions to minimize the impact of security incidents

Integration Capabilities

SIEM should integrate seamlessly with your cloud infrastructure, security tools, and identity and access management (IAM) systems

Compliance and Reporting

Should provide comprehensive reporting and auditing capabilities to meet regulatory requirements

Threat Detection Capabilities

Look for advanced analytics, machine learning, and behavioral analytics features to detect sophisticated threats

User Interface and Experience

User-friendly interface can significantly improve security analysts' efficiency

IRDR

In today's cloud-centric world, ensuring business continuity and minimizing downtime in the face of incidents or disasters is paramount

A robust Incident Response and Disaster Recovery (IRDR) strategy is essential for organizations leveraging cloud services

Incident Response

Coordinated set of procedures to detect, analyze, and contain security breaches or other IT incidents

Disaster Recovery

Plan to restore IT systems and operations in the event of a disaster, such as a natural disaster or cyberattack

End of Lesson

Q/A