Prof. Alessandro Carrega
alessandro.carrega@unige.it

Lesson 04

Network Security Protocols

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

TLS

A

2

Why is Transport Layer Security critical for Cloud?

- ✖ Fundamental security tool for cloud environments
- ✖ By understanding its role and implementing best practices, organizations can significantly enhance the security of their cloud infrastructure and data

Data Integrity

Ensures that data remains unaltered during transmission, preventing tampering and corruption

Data Confidentiality

Protects sensitive data, such as user credentials, financial information, and intellectual property, from unauthorized access

Authentication

Verifies the identity of the server and client, preventing man-in-the-middle attacks

TLS

B

3

Cloud Environment

Secure API Communication	*Secure Remote Access*	*Secure Data Transfer*
Protects APIs used for data exchange between cloud services and applications	Secures remote access to cloud resources, such as virtual machines and databases	Encrypts data transferred between cloud storage services and client applications

TLS

C

Best Practices in Cloud

4

Strong Cipher Suites

Use strong encryption algorithms and key exchange methods

Certificate Pinning

Pin specific certificates to prevent man-in-the-middle attacks

HSTS

Implement HTTP Strict Transport Security to enforce HTTPS connections

Regular Certificate Renewal

Keep certificates up-to-date to avoid security vulnerabilities

TLS Protocol Version

Use the latest TLS version (TLS 1.3) for enhanced security

IPSEC

A

5

What is it Internet Protocol SECurity?

- Powerful tool for securing cloud networks. By understanding its components and best practices, organizations can protect their cloud infrastructure and data from various threats
- A suite of protocols designed to secure IP network communications
- Provides confidentiality, integrity, and authentication for IP packets

Key IPsec Protocols

- AH (Authentication Header) provides authentication and integrity for IP packets
- ESP (Encapsulating Security Payload) provides confidentiality, integrity, and authentication for IP packets

IPSEC

B

6

Cloud Environment

Secure Virtual Private Networks (VPNs)	*Secure Site-to-Site Connections*	*Secure Remote Access*
Creates secure, encrypted tunnels between cloud resources and on-premises networks	Enables secure communication between different cloud regions and data centers	Secures remote access to cloud resources using IPsec VPNs

IPSEC

C

7

Best Practices in Cloud

Strong Encryption Algorithms

Use strong encryption algorithms like AES-256

IPsec Policy Configuration

Configure IPsec policies to balance security and performance

Key Management

Implement robust key management practices to protect cryptographic keys

Firewall Integration

Integrate IPsec with firewalls to filter traffic and enforce security policies

SSH

A

8

What is Secure Shell?

Fundamental tool for secure remote access to cloud resources

By following best practices, organizations can protect their cloud environments from unauthorized access and data breaches

A cryptographic network protocol for secure remote login to computer systems

Provides a secure channel for remote command-line access and file transfer

SSH

B

9

Cloud Environment

Secure Remote Access	*Configuration Management*	*Automated Scripting*
Enables secure remote access to cloud servers and virtual machines	Facilitates secure deployment and configuration of cloud infrastructure	Allows for secure execution of automated scripts on cloud resources

SSH

C

Best Practices in Cloud

10

Strong Password Policies

Enforce strong, unique passwords or use public-key authentication

SSH Port Scanning Protection

Implement measures to protect against SSH brute-force attacks

Two-Factor Authentication (2FA)

Enable 2FA for additional security

SSH Key Management

Securely store and manage SSH private keys

SSH Configuration

Configure SSH to use strong encryption algorithms and disable weak ciphers

SNMP

1

11

What is Simple Network Management Protocol for Cloud

SNMP

2

Network Device Monitoring	*Cloud Resource Monitoring*	*Fault Detection and Alerting*
Monitors the health and performance of network devices, such as routers, switches, and firewalls	Tracks the utilization of cloud resources, including virtual machines, storage, and network bandwidth	Detects network and system failures and generates alerts

In Cloud Environment

SNMP

C

13

Best Practices in Cloud

- ✖ Valuable tool for monitoring and managing cloud infrastructure
- ✖ By using SNMP effectively, organizations can ensure the reliability and performance of their cloud environments

SNMP Trap Configuration

Configure SNMP traps to receive timely alerts for critical events

SNMP Monitoring Tools

Use robust SNMP monitoring tools to analyze network performance data

Secure SNMP Configuration

Use strong community strings and encryption to protect SNMP traffic

Security Considerations

implement security measures to protect SNMP from unauthorized access

Diameter

A

What is it?

14

Modern networking protocol designed for exchanging Authentication, Authorization, and Accounting (AAA) information

It serves as a robust and scalable replacement for the older RADIUS protocol, addressing many of its limitations.

Diameter is commonly used in 4G/LTE, 5G, and other advanced mobile networks, as well as IP Multimedia Systems (IMS) networks

Diameter

B

15

Key Functions

Authentication	*Authorization*	*Accounting*
• Verifies the identity of a user or device attempting to access network resources • Ensures that only authorized entities can gain access	• Determines the level of access and privileges granted to a successfully authenticated user or device • This involves checking policies and rules to determine what resources can be accessed and under what conditions	• Tracks and records usage information for billing, security auditing, and network management purposes • This includes details like start and stop times, data usage, and other relevant metrics

Diameter

C

16

How it works?

Clients and Servers

- It operates in a client-server model. Network devices (clients) send requests to servers for AAA services
- Common clients include mobile devices, routers, switches, and other network elements

Messages

It uses a variety of message types to communicate between clients and servers

Diameter

D

17

Messages

Request	Initiates a request for authentication, authorization, or accounting
Answer	Provides a response to a request, indicating success or failure
Error	Indicates an error condition
Accounting-Request	Sends usage information to the server
Accounting-Answer	Acknowledges the receipt of accounting information

Diameter

TLS for encrypted communication

Message Authentication Codes (MACs) to verify message integrity

Authentication mechanisms like digital certificates and shared secrets

Diameter

F

19

Advantages

Scalability	Designed to handle large-scale networks and high traffic loads
Answer	Robust security features to protect sensitive information
Flexibility	Can be adapted to various network environments and services
Efficiency	Optimized for performance and resource utilization
Interoperability	Supports a wide range of network technologies and protocols

Diameter

G

Remarks

20

Crucial protocol for modern networks, enabling secure and reliable authentication, authorization, and accounting

Its advanced features and scalability make it well-suited for the demands of today's complex network environments

SCP (Secure Copy Protocol)

A

21

Benefits in Cloud Environments

Versatile tool for secure file transfer, particularly relevant in cloud environments due to their distributed nature and the need for robust security

Flexibility and Portability

Cross-Platform Compatibility SCP can be used on various operating systems (Windows, macOS, Linux) and cloud platforms (AWS, Azure, GCP)
Remote Access securely transfer files to and from cloud instances, virtual machines, and storage services
Scripting and Automation: integrate SCP into automation scripts for efficient file transfers

Enhanced Security

- Encryption SCP leverages SSH encryption to protect data in transit, ensuring confidentiality and integrity
- Authentication strong mechanisms, such as public-key cryptography, safeguard against unauthorized access

- Reliable and Fast SCP offers reliable and efficient file transfer, especially for large files
- Batch Transfers multiple files and directories simultaneously

SCP (Secure Copy Protocol)

B

22

Common Use Cases in Cloud Environments

Deploying Applications transferring application code and configuration files to cloud servers

Data Backups from cloud instances to local storage or other cloud storage services

Data Migration between different cloud storage solutions or on-premises system

Configuration Management transferring configuration files to cloud servers for updates and maintenance

File Sharing securely with other users or teams within a cloud environment

SCP (Secure Copy Protocol)

C

Limited Functionality	*Complexity for Large-Scale Transfers*	*Security Best Practices*
SCP primarily focuses on file transfer, lacking advanced file management features like directory listing and remote file deletion	For large-scale file transfers, consider using more advanced tools like rsync or SFTP, which offer features like incremental transfers and checksum verification	• Strong Passwords or SSH Keys use strong authentication methods to protect access • Keep SSH Software Updated regularly update SSH software to address security vulnerabilities • Limit Access restrict access to sensitive files and directories • Monitor System Logs for any suspicious activity

SCP (Secure Copy Protocol)

D

Remarks

- ✖ SCP remains a valuable tool for secure file transfer in cloud environments
- ✖ By understanding its strengths and limitations, you can effectively leverage SCP to enhance your cloud operations
- ✖ For more complex file transfer scenarios or advanced file management needs, consider using SFTP or rsync

End of Lesson

Q/A