B.Tech, 6^{th} Sem.,Section: 36 & 38 Computer Networking: Security(CLASS NOTE)

Dr. Laxmidhar Biswal

April 13, 2025

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

1. Chapter 02
   - Introduction
   - CIA
     - Non-Repudiation
     - Access Controls
   - AAA
   - Gap Analysis
   - Zero Trust
   - The Data Plane
   - Physical Security
   - Deception and Disruption Technology

Introduction/Motivation

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Objectives of this chapter

This chapter aims to equip you with a clear understanding of fundamental security concepts. You will learn the core principles of the CIA triad—Confidentiality, Integrity, and Availability—and explore modern approaches like Zero Trust and Deception Technology. The chapter also covers Authentication, Authorization, and Accounting (AAA), along with the concept of Non-repudiation, emphasizing their application in securing systems and users. Additionally, you'll become familiar with physical security measures such as bollards, video surveillance, and access control vestibules. These concepts are essential for protecting both digital and physical environments and will help you confidently answer related questions in your certification exam.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Confidentiality, Integrity, and Availability(CIA)

Confidentiality

- Protects sensitive data from unauthorized access.
- Ensures only authorized users can view or handle information.
- Examples: Encryption, access control, data classification.

Integrity

- Maintains accuracy and consistency of data
- Prevents unauthorized modification or tampering
- Tools: Hashing algorithms (e.g., SHA-1, MD5)

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Confidentiality, Integrity, and Availability(CIA)

Availability

- Ensures data and systems are accessible when needed.
- Prevents downtime or disruption of services.
- Measures: Redundancy, backups, failover systems.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Non-Repudiation

Prevents denial of actions; ensures accountability in digital transactions and communications.

- Digital Signatures: Confirms sender identity and message integrity using cryptographic methods.
- Audit Trails: Records chronological actions for traceability and accountability.
- Use Case: Builds trust in e-commerce by preventing denial of online transactions.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Access Controls

Identification

- Establishes user identity (e.g., username, smart card, biometrics).
- Each user has a unique Security Identifier (SID).

Authentication

- Verifies identity via passwords, PINs, or biometrics.

Authorization

- Grants appropriate access based on user role.
- Follows the principle of least privilege—only minimum required access is provided.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Authentication, Authorization, and Accounting

In digital security, the AAA server is a key component that manages Authentication, Authorization, and Accounting—three pillars of secure access control.

- Authentication (People): Verifies a user's identity before granting access, often using passwords, biometrics, or domain controllers in Windows networks.
- Authentication (Systems): Uses the 802.1X protocol to ensure devices have valid certificates before connecting to the network.
- Authorization:
  - Defines what authenticated users or devices can access.
  - Once authenticated, users or devices are granted access only to specific resources based on their roles and policies.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Authentication, Authorization, and Accounting

- Accounting:
  - Tracks and logs user/device activity: login time, IP, accessed resources.
  - Supports auditing, real-time monitoring, troubleshooting, and compliance.
- AAA Protocols:
  - Remote Authentication Dial-In User Service(RADIUS): Commonly used for remote access; ensures secure communication via a shared secret.
  - Diameter: A modern replacement for RADIUS; supports 4G/5G networks with enhanced capabilities.
  - Terminal Access Controller Access Control System Plus (TACACS+): Developed by Cisco; provides detailed control over network device access.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Gap Analysis

Gap Analysis is a strategic method to compare an organization's current security posture with industry standards, regulations, and best practices, identifying areas for improvement.

- Assessment: Review current security policies, procedures, and technologies.
- Benchmarking: Compare existing practices with standards and compliance frameworks.
- Identification: Spot gaps where current security falls short.
- Prioritization: Rank gaps based on risk and likelihood of exploitation.
- Remediation: Create actionable plans to address and close high-priority gaps.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

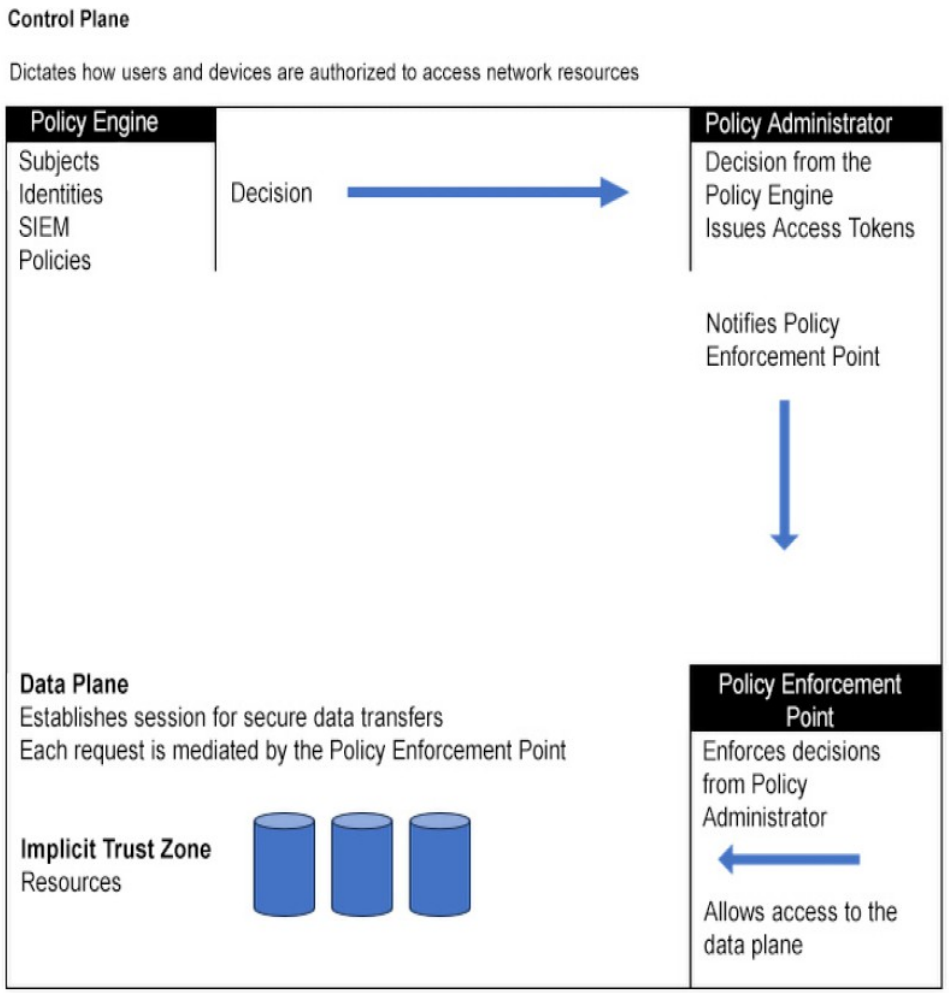
Zero Trust

Zero Trust = "*Never trust, always verify*"
— Every access request must be authenticated, authorized, and continuously validated.

- Control Plane: Decides who can access what, when, and how (authorization, policies).
- Data Plane: Executes actual data transfer, enforcing access decisions.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal



Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Policy Engine

- Inputs: Subjects, Identities, SIEM data, Security Policies.
- Role: Makes access decisions based on contextual information (e.g., user role, device type, behavior).
- Output: Access decision $\rightarrow$ passed to the Policy Administrator.

Policy Administrator

- Responsibilities/roles: Issues access tokens based on Policy Engine's decisions.
- Function: Notifies the Policy Enforcement Point for action.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Adaptive Identity

- Dynamically adjusts access based on behavior, location, device.
- Enhances security and user experience.

Threat Scope Reduction

- Minimizes attack surface (e.g., fewer exposed services, regular patching).
- Prevents threats proactively.

Policy-Driven Access Control

- Automates access enforcement via security policies.
- Ensures consistency and reduces human error.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Policy Enforcement Point

- Role: Enforces access control decisions.
- Acts as: The security gatekeeper, allowing or denying access to the data plane.

Data Plane

- Function: Facilitates secure data transfer sessions.
- Supervised by: The Policy Enforcement Point for every request.

Implicit Trust Zone

- Designated resource area considered secure, but Zero Trust minimizes reliance on such zones.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Data Plane & Trust Zones

Date Plane

- Handles routing, switching, and packet forwarding.
- Executes predefined rules for secure, efficient data transmission.
- Involves subjects (initiators of communication) and systems (routers, switches, firewalls, etc.).

Trust Zones

- Implicit Trust Zone: Trusted internal components communicate without strict checks.
- Internal Network Zone: Behind firewall; assumed trustworthy (e.g., domain controllers).

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Data Plane & Trust Zones

Trust Zones

- DMZ (Demilitarized Zone): Semi-trusted; allows limited access from external networks.
- External Network Zone: Untrusted (e.g., internet); requires strong security.

Physical Security

To understand and implement effective physical security measures that deter, detect, and respond to threats. This includes integrating human and technological solutions—such as surveillance, barriers, access controls, and sensors—to safeguard personnel, assets, and sensitive information in diverse environments.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Physical Security

- Bollards:
  - Strong posts to block unauthorized vehicle access.
  - Used near high-security buildings & infrastructure.
- Access Control Vestibule: Dual-door entry for identity verification before access.
- Fencing:
  - Physical boundary & deterrent.
  - Modern versions use advanced materials & design.
- Video Surveillance:
  - Real-time monitoring + event recording.
  - Uses analytics to detect & investigate threats.
- Security Guards: Human enforcement of protocols, patrols, and incident response.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Physical Security

- Access Badges
  - RFID/smart badges for controlled access.
  - Track entry logs & differentiate guests.
- Lighting: Enhances visibility, deters crime, aids surveillance.
- Visitor Logs: Records entry/exit; crucial for audits and accountability.
- Sensor Technologies: Detect anomalies with minimal human input:
  - Infrared – Detect heat (humans/animals).
  - Pressure – Sense movement via touch/step.
  - Microwave – Detect motion through wave interference.
  - Ultrasonic – Detect via sound waves, even around corners.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Deception and Disruption Technology

To explore how deception and disruption technologies proactively mislead attackers, enabling early threat detection, improved analysis, and robust defense strategies in cybersecurity.

- Honeypot: Simulated system/site to lure attackers; used to observe attack methods or divert attention from real assets.
- Honeynet: A network of honeypots creating a fake environment to study and distract attackers from the real network.
- Honeyfile: A strategically placed file (e.g., named "password") that triggers alerts when accessed by intruders.

Summarize fundamental security concepts

Dr. Laxmidhar Biswal

Deception and Disruption Technology

- Honeytoken: Dummy data designed to detect unauthorized access or insider threats; sets off alarms upon misuse.
- Fake Information: Techniques like DNS sinkholes or fake telemetry mislead attackers and help monitor or nullify malicious actions.

References

https://www.ebooks.com/en-ag/book/210192090/comptia-security-sy0-601-certification-guide/ian-neil/

Question ??

The End