# 2025 CISSP Mentor Program

## SESSION 8

**John Kennedy, Sec +, CISSP**

# INTRODUCTION

**Agenda**

- Welcome
- Reminders
- Introduction
- Chapter 12 - Secure Communications and Network Attacks/Domain 4 – Communication and Network Security
- Chapter 13 - Managing Identity and Authentication/Domain 5 – Identity and Access Management (IAM)

# FRSECURE CISSP MENTOR PROGRAM LIVE STREAM

THANK YOU!

## Quick housekeeping reminder.

- The online/live chat that's provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.
- At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.
- Please do not chat about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.
- Failure to abide by the rules may result in disabling chat for you.
- **DO NOT share or post copywritten materials. (pdf of book)**

# GETTING GOING...

**Managing Risk!**

## Study Tips:

- Study in small amounts frequently (20-30 min)
- Flash card and practice test apps help
- Take naps after heavy topics (aka Security Models)
- Write things down, say them out loud, explain them to others
- Use the Discord Channels
- Exercise or get fresh air in between study sessions

**Let's get going!**

# SCHEDULE

*[Our plan]*

| Class Number | Date | Topic | Lead Mentor |
|---|---|---|---|
| 1 | 4/23/25 | Session 1 – CISSP Mentor Program Introduction | Evan |
| 2 | 4/30/25 | Session 2 – Chapter 1 & 2 (pg. 1–114) | Evan |
| 3 | 5/7/25 | Session 3 – Chapter 3, 4, & 5 (pg. 121–221) | Christophe |
| 4 | 5/14/25 | Session 4 – Chapter 6 & 7 (pg. 227-311) | Evan |
| 5 | 5/21/25 | Session 5 – Chapter 8 & 10 (pg. 317-353, 443-483) | Christophe |
| 6 | 5/28/25 | Session 6 – Chapter 9 (pg. 359-435) | Brad |
| 7 | 6/4/25 | Session 7 – Chapter 11 (pg. 491-574) | Evan |
| 8 | 6/11/25 | Session 8 – Chapter 12 & 13 (pg. 581-674) | John |
| 9 | 6/18/25 | Session 9 – Chapter 14 & 15 (pg. 681-764) | Jacob |
| 10 | 6/25/25 | Session 10 – Chapter 16 & 17 (pg. 769-862) | Brad |
| 11 | 7/2/25 | Session 11 – Chapter 18 & 19 (pg. 869-945) | Evan |
| 12 | 7/9/25 | Session 12 – Chapter 20 & 21 (pg. 951-1048) | Evan |
| 13 | 7/16/25 | Session 13 – Practice Tests & Final Prep | All |
| 14 | 7/23/25 | Session 13 – Practice Tests & Final Prep | All |

# WHO AM I


[LinkedIn Profile]

# AGENDA – SESSION 8

## Chapter 12 (from the book)

### Chapter 12 - Secure Communications and Network Attacks

THE CISSP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

- Domain 4: Communication and Network Security
  - 4.1 Apply secure design principles in network architectures
    - 4.1.7 Performance metrics (e.g., bandwidth, latency, jitter, throughput, signal-to-noise ratio)
    - 4.1.18 Monitoring and management (e.g., network observability, traffic flow/shaping, capacity management, fault detection and handling)
  - 4.3 Implement secure communication channels according to design
    - 4.3.1 Voice, video, and collaboration (e.g., conferencing, Zoom rooms)
    - 4.3.2 Remote access (e.g., network administrative functions)
    - 4.3.3 Data communications (e.g., backhaul networks, satellite)
    - 4.3.4 Third-party connectivity (e.g., telecom providers, hardware support)

**Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 581**

2025 CISSP MENTOR PROGRAM

# AGENDA – SESSION 8

## Chapter 13 (from the book)

### Chapter 13 - Managing Identity and Authentication

THE CISSP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

- Domain 5: Identity and Access Management (IAM)
- 5.1 Control physical and logical access to assets
  - 5.1.1 Information
  - 5.1.2 Systems
  - 5.1.3 Devices
  - 5.1.4 Facilities
  - 5.1.5 Applications
  - 5.1.6 Services
- 5.2 Design identification and authentication strategy (e.g., people, devices, and services)
  - 5.2.1 Groups and Roles
  - 5.2.2 Authentication, Authorization and Accounting (AAA) (e.g., multi-factor authentication (MFA), password-less authentication)
  - 5.2.3 Session management
  - 5.2.4 Registration, proofing, and establishment of identity
  - 5.2.5 Federated Identity Management (FIM)
  - 5.2.6 Credential management systems (e.g., Password vault)

# AGENDA – SESSION 8

## Chapter 13 (from the book)

### Chapter 13 - Managing Identity and Authentication

THE CISSP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

- 5.2.7 Single Sign On (SSO)
- 5.2.8 Just-In-Time
- 5.3 Federated identity with a third-party service
  - 5.3.1 On-premise
  - 5.3.2 Cloud
  - 5.3.3 Hybrid
- 5.5 Manage the identity and access provisioning lifecycle
  - 5.5.1 Account access review (e.g., user, system, service)
  - 5.5.2 Provisioning and deprovisioning (e.g., on/off boarding and transfers)
  - 5.5.3 Role definition and transition (e.g., people assigned to new roles)
  - 5.5.5 Service accounts management

# CHAPTER 12

## Secure Communications and Network Attacks

- Communication security is designed to detect, prevent, and even correct data transportation errors (that is, it provides integrity protection as well as confidentiality). Communication security is used to sustain the security of networks while supporting the need to exchange and share data. This chapter covers the many forms of communication security, vulnerabilities, and countermeasures.

- The Communication and Network Security domain deals with topics related to network components (i.e., network devices and protocols), specifically how they function and how they are relevant to security. This domain is discussed in this chapter and in Chapter 11, "Secure Network Architecture and Components." Be sure to read and study the material in both chapters to ensure complete coverage of the essential material.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 581

# CHAPTER 12

## Secure Communications and Network Attacks

### Protocol Security Mechanisms

**TCP/IP is the core protocol suite** used on most networks and the internet.

While robust, **TCP/IP has inherent security flaws**.

To improve protection, **many subprotocols and tools** have been developed.

These mechanisms help ensure:

- **Confidentiality**
- **Integrity**
- **Availability**
- **Authentication & Access Control**

The internet relies on **hundreds of protocols** — some secure data, others manage access.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 582

# CHAPTER 12

## Secure Communications and Network Attacks

### Authentication Protocols

**Point-to-Point Protocol (PPP)**

- Encapsulation protocol for **IP over dial-up or point-to-point links**
- Operates at the **Data Link Layer**
- Rarely used on Ethernet today; defined in **RFC 1661**
- **Replaced SLIP**
- Supports authentication via **PAP, CHAP, and EAP**

| Protocol | Purpose & Key Traits |
|---|---|
| PAP | Transmits **usernames & passwords in cleartext**; no encryption; only transports credentials |
| CHAP | Uses **challenge-response** with password hash; resistant to replay; **reauthenticates periodically**; based on **MD5** (insecure) |
| EAP | **Authentication framework**, not a single protocol; supports **smartcards, biometrics, tokens**; security varies by method |
| | ➤ **40+ EAP types:** LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, etc. |

*For a more extensive list of EAP methods, see http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

**Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 582-583**

# CHAPTER 12

## Secure Communications and Network Attacks

### Port Security

**Port Security Has Multiple Meanings**:

- **Physical Port Security**: Restricting physical access to network ports (e.g., RJ-45 jacks, patch panels) to prevent unauthorized connections.
- **Logical Port Security**: Managing **TCP/UDP ports**—only ports assigned to active services should be open. All others should be closed.
- **Authentication-Based Port Security**: Often refers to **IEEE 802.1X**, where a user/device must **authenticate before gaining network access** (usually via a switch or wireless AP).

**Common Security Tools:**

- Firewalls, IDS/IPS can detect and respond to port scans.
- These tools can **block scans or return false information** to confuse attackers.

**For the full discussion of network access control (NAC), see Chapter 11.**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 585

# CHAPTER 12

## Secure Communications and Network Attacks

### Quality of Service (QoS)

Oversight and management of network communication efficiency and performance to protect data network availability under load and meet business requirements.

**Some of the performance metrics or factors contributing to QoS are as follows:**

| Metric | Description |
|---|---|
| **Bandwidth** | Network capacity available to carry communications |
| **Latency** | Time for a packet to travel from source to destination |
| **Jitter** | Variation in latency between different packets |
| **Packet Loss** | Packets lost requiring retransmission |
| **Interference** | Signal corruption from electrical noise or faulty equipment |
| **Throughput** | Actual data successfully transmitted over time |
| **Signal-to-Noise Ratio (SNR)** | Signal quality measure comparing desired signal strength to background noise |

**Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 585**

# CHAPTER 12

## Secure Communications and Network Attacks

### Secure Voice Communications

- **Telephony:** Collection of methods by which telephone services are provided to organizations for voice and/or data communications.

**Telephony Technologies**

| Technology | Description |
|---|---|
| **PSTN** | Public Switched Telephone Network (Plain Old Telephone Service - POTS) |
| **PBX** | Private Branch Exchange - Internal organizational phone system |
| **Mobile/Cellular** | Wireless communication services |
| **VoIP** | Voice over Internet Protocol - Voice communications over IP networks |

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 585-586

# CHAPTER 12

## Secure Communications and Network Attacks

### Voice over Internet Protocol (VoIP)

**What is VoIP?**

- VoIP (Voice over IP) encapsulates audio into IP packets for transmission over TCP/IP networks
- Powers services beyond voice: multimedia messaging, video, chat, file sharing, etc.

**Security Considerations**

- VoIP encryption (e.g., **SRTP**) is available but **rarely end-to-end**
- Most VoIP solutions only encrypt traffic between the device and the provider, not across different providers
- **VoIP ≠ Single Technology**: Uses common standards, but vendor implementations vary
- Limited interoperability reduces the effectiveness of end-to-end encryption

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 587

# CHAPTER 12

## Secure Communications and Network Attacks

### Vishing and Phreaking

**Key Concepts:**

- **Social Engineering**: Manipulation technique used by attackers to gain unauthorized access by exploiting human trust.
- **VoIP Vulnerabilities**:
  - Enables cheap or free calls to any number.
  - **Caller ID spoofing** allows attackers to disguise their identity.
- **Vishing (Voice Phishing)**:
  - Attackers use phone calls to deceive victims into revealing sensitive information.
  - Targets include landlines (PSTN), business lines (PBX), mobile phones, and VoIP users.
- **Takeaway:**
  Any voice communication channel can be exploited for social engineering — awareness and verification are your best defenses.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 588-589

# CHAPTER 12

## Secure Communications and Network Attacks

### Vishing and Phreaking (cont.)

**Defending Against Vishing & Phreaking**

- **User Awareness is Key:**
- Train users to **identify suspicious calls** and respond cautiously.
- Treat **unexpected or unusual calls** as potential threats.

**Security Best Practices:**

- **Verify identity** before discussing sensitive topics.
- Use **callback authorization** for all voice-only network change requests.
- **Classify data** and define what can/cannot be shared over the phone.
- Never **share or change passwords** through voice-only communication.
- **Question unusual requests**, even from known individuals; re-verify identity.
- **Report suspicious calls** to the security team immediately.

**Technical Measures:**

- **Block known malicious numbers**.
- Don’t trust **Caller ID** — it can be spoofed.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 588-589

# CHAPTER 12

## Secure Communications and Network Attacks

### Vishing and Phreaking (cont.)

**Phreaking Defined:**

- Attacks targeting **phone systems**, not just users.
- Aimed at:
  - Free long-distance calls
  - Service manipulation/disruption
  - VoIP, PBX, mobile, and traditional PSTN systems
- Tools range from **devices** to **manual techniques**.

✅ **Still Relevant – But Modernized:**

- While classic phreaking (like using a "blue box" to make free calls on PSTN lines) is mostly obsolete, the **core idea—abusing phone systems—is very much alive.**
- Modern phreakers target **VoIP**, **PBX**, **mobile networks**, and **unified communications systems** using updated tools and techniques.

🚨 **Why It Matters for CISSPs:**

- Telephony is still integrated into most corporate environments.
- Voice systems often **lack strong authentication or logging**, making them attractive targets.

**Takeaway:**
Voice systems are vulnerable. Combine **user training** with **technical controls** to defend against social engineering and telephony-based attacks.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 588-589

# CHAPTER 12

## Secure Communications and Network Attacks

### PBX Fraud and Abuse

**What is PBX?**

- **Private Branch Exchange (PBX):**
  - Internal phone system for organizations.
  - Connects multiple internal phones to limited external PSTN lines.
  - Supports features like:
    - **Extension dialing**
    - **Voicemail per extension**
    - **Remote calling (hoteling)**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 590

# CHAPTER 12

## Secure Communications and Network Attacks

### PBX Fraud and Abuse (cont.)

**Remote Calling (Hoteling):**

- Allows users to dial into the PBX remotely to access an outbound line.
- Originally designed to **reduce long-distance costs** for remote employees.

**Security Risks & Abuse:**

- **Toll fraud**: Attackers use PBX to place unauthorized long-distance/international calls.
- **Identity masking**: Malicious users can hide their origin using PBX systems.
- **Voicemail abuse**:
  - Unauthorized access to mailboxes
  - Message redirection or deletion
  - Blocking legitimate users
- **Call redirection**: Incoming/outgoing calls can be hijacked or rerouted.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 590

# CHAPTER 12

## Secure Communications and Network Attacks

### PBX Fraud and Abuse (cont.)

📞 **Remote Access Controls:**

- **Replace PBX-based remote calling** with calling card systems.
- **Restrict dial-in/dial-out** to only authorized personnel.
- **Use unpublished numbers** for dial-in modems, outside of main number block.
- **Block remote dialing** where not needed.

📜 **Policies & Monitoring:**

- Define and enforce an **Acceptable Use Policy (AUP)**.
- **Train users** on secure and proper PBX usage.
- **Log & audit** all PBX activity regularly.
- 🛠️ **System Hardening:**
- Apply **vendor updates and patches** promptly.
- Use **DISA (Direct Inward System Access)** to secure external access to internal dial tones.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 589

# CHAPTER 12

## Secure Communications and Network Attacks

### DISA & PBX Security Considerations

**DISA (Direct Inward System Access):**

- Adds **authentication** to external PBX connections.
- **Proper configuration is critical**—simply enabling DISA isn't enough.

**DISA Security Best Practices:**

- **Disable unnecessary features**.
- Use **strong, complex user codes/passwords**.
- **Enable auditing** to monitor all PBX activity.

**Physical Security:**

- Restrict access to:
  - PBX connection centers
  - Phone portals
  - Wiring closets

**Modern PBX = Software-Based Systems:**

- Many PBX platforms now run as **software solutions** managing PSTN and VoIP.
- These are vulnerable to common network and application attacks:
  - **Buffer overflows**
  - **Malware**
  - **Denial of Service (DoS)**
  - **Adversary-in-the-Middle (AitM)**
  - **Hijacking & eavesdropping**

Source: ChatGPT

# CHAPTER 12

## Secure Communications and Network Attacks

### Remote Access Security Management

🔑 **What is Remote Access?**
Allows a remote (offsite) client to securely connect to an internal network or system.

🛠️ **Common Remote Access Methods:**

1. **VPN over the Internet** – Secure tunnel from remote client to LAN.
2. **WAP Access** – Wireless Access Points may be treated as "remote."
3. **Thin Clients to Central Systems** – Access via:
   - Terminal servers
   - Mainframes
   - VPC endpoints
   - VDI or VMI platforms
4. **Remote Desktop Services** – Control an office PC remotely.
5. **Cloud-Based Virtual Desktops** – Virtualized desktop environments online.
6. **Dial-up via Modem** – Legacy method; rarely used but still testable.

Note: The first three examples use fully capable clients. They establish connections just as if they were directly connected to the LAN. In the last three examples, all computing activities occur on the connected central system rather than on the remote client.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 590-591

# CHAPTER 12

## Secure Communications and Network Attacks

### Remote Access and Telecommuting Techniques

**What is Telecommuting?**
Performing work from a remote location outside the primary office, requiring secure connectivity to central resources.

**Types of Remote Access**

1. **Service-Specific Access**
   - Access to **one specific service** (e.g., webmail, database).
   - ✅ **Least privilege** by design.
   - 🧠 *CISSP Tip:* Minimizes exposure—**use when possible**.
2. **Remote Control**
   - User **fully controls a distant system** (e.g., RDP, TeamViewer).
   - Acts as if local—**keyboard/mouse/monitor are redirected**.
   - 🧠 *CISSP Tip:* High risk—**requires strong authentication, session encryption, and audit logging**.
3. **Remote Node Operation**
   - Remote client **connects directly to LAN** via VPN, wireless, or dial-up.
   - Client acts as **full network node** with access to internal resources.
   - 🧠 *CISSP Tip:* Considered **full client** access—requires endpoint protection & strong network segmentation.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 590-591

# CHAPTER 12

## Secure Communications and Network Attacks

### Remote Access and Telecommuting Techniques (cont.)

**Remote Connection Security**

🔐 **Security Is Essential for Remote Access**

Deploying remote access without proper security can **bypass physical security** and increase the attack surface.

**Best Practices for Securing Remote Connections**

1. **Strong Authentication**
   - Grant access **only to authorized users** with job-related need.
   - Implement **MFA** wherever possible.
2. **Encrypted Communication**
   - Encrypt **both authentication and data transmission** (e.g., TLS, IPSec).
   - **Never transmit sensitive data over unprotected links**.
3. **Access Control & Limitation**
   - Use **least privilege** principles.
   - Enforce **access control lists (ACLs)** and **network segmentation**.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 592

# CHAPTER 12

## Secure Communications and Network Attacks

### Remote Access and Telecommuting Techniques (cont.)

#### 📋 Planning a Remote Access Security Policy

**1. Evaluate Remote Connectivity Technology**

- Consider **all access types**: PSTN, DSL, cable, fiber, wireless, cellular, satellite.
- Each tech introduces **unique security challenges**.

**2. Ensure Transmission Protection**

- Use **VPNs, TLS**, and other **encryption protocols** to secure remote traffic.
- Match encryption level to **sensitivity of data** and **connection type**.

**3. Strengthen Authentication Protection**

- Use **secure authentication protocols**.
- Implement **centralized remote authentication systems**.
- **Mandate MFA** for all remote access.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 593

# CHAPTER 12

## Secure Communications and Network Attacks

### Planning a Remote Access Security Policy (cont.)

**4. Provide Remote User Assistance**

- Ensure **support for software, hardware, and training** needs.
- Lack of support increases risk of:
  - Productivity loss
  - Device compromise
  - Organizational breaches

**5. Ban Unauthorized Modems & Secondary Connections**

- **No unauthorized modems** or wireless/cellular access.
- Require **hardware profiles** to disable unapproved interfaces.

**6. Access Control Measures**

- Control remote access using:
  - **User & device identity**
  - **Protocol/application filtering**
  - **Time-of-day restrictions**
  - **Attribute-Based Access Control (ABAC)**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 593

# CHAPTER 12

## Secure Communications and Network Attacks

### 🛠️ Network Administrative Functions via Remote Access

#### 🌐 Purpose Beyond Telecommuting

- Remote access supports not just users but **network administrators**
- Enables secure management of infrastructure **from any location**

#### 🧩 1. Configuration Management

- Remotely configure and modify:
  - **Routers**
  - **Switches**
  - **Firewalls**
- Used to update settings and deploy changes to meet evolving needs

#### 📊 2. Monitoring & Analysis

- Use remote tools to:
  - Track **network performance**
  - Analyze **traffic patterns**
  - Identify **security threats or anomalies**
- Supports **log analysis** and **alert response**

#### 🔍 3. Troubleshooting & Diagnostics

Admins can:

- **Access devices**
- Run **remote diagnostic tests**
- Examine **logs**
- Resolve **connectivity & performance issues**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 594

# CHAPTER 12

## Secure Communications and Network Attacks

### Remote Administrative Security Functions

**1. Security Management**

- Remotely configure:
  - **Security policies**
  - **Access controls**
  - **Authentication mechanisms**
- Manage **firewalls, VPNs**, and other protective measures

**2. User Account Management**

- Remote tasks include:
  - **Create/modify/deactivate** accounts
  - **Reset passwords**
  - Assign or restrict **access rights**

**3. Patch & Update Management**

- Deploy **software updates and security patches**
- Close known vulnerabilities
- Ensure **compliance** and **performance**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 594

# CHAPTER 12

## Secure Communications and Network Attacks

### Remote Administrative Security Functions (cont.)

**4. Backup & Recovery**

- Schedule and verify **remote backups**
- Implement recovery protocols during **data loss or system failure**

**5. Policy Enforcement**

- Ensure configs match:
  - **Security policies**
  - **Organizational standards**
  - **Regulatory requirements**
- Maintain compliance **remotely**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 594

# CHAPTER 12

## Secure Communications and Network Attacks

### Multimedia Collaboration & Security

#### What is Multimedia Collaboration?

- **Remote team collaboration** using:
  - Email, chat, VoIP, video conferencing
  - Whiteboards, online editing, real-time file sharing
  - Version control, document tracking
- Supports **real-time** & **asynchronous** teamwork

#### Collaboration Tools & SaaS Considerations

- Tools include: **Zoom, Teams, Google Meet, Webex**
- **Review all tools** against organizational **security policies**
- **Security is not optional** — even in remote settings

#### Security Best Practices

- **Encrypted connections** required
- Use **robust MFA (Multifactor Authentication)**
- Ensure **auditing & tracking** capabilities
- Enforce **access control** and **session management**

#### Zoom Rooms & Hybrid Collaboration

- **Zoom Room** = tech-enabled physical space for video meetings
- Features: HD video/audio, touchscreen controls, AV integration
- Enables **immersive virtual meetings** and **team presentations**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 594-595

# CHAPTER 12

## Secure Communications and Network Attacks

### Remote Meeting

#### What Is Remote Meeting Technology?

- **Tools** for collaboration & interaction between remote users:
  - Video conferencing (e.g., Zoom, Teams)
  - Shared whiteboards
  - Virtual training tools
  - Collaborative document editing
- Known as: **Virtual Meetings**, **Digital Collaboration**, **Software Collaboration**

#### Best Practices

- Choose platforms that support **end-to-end encryption**
- Enforce **MFA and user verification**
- Train users on **secure usage** and **policy compliance**
- Avoid platforms with excessive tracking or ad integrations

#### Security Evaluation Checklist

Before deployment, ask:

- ✅ Does it use **strong authentication**?
- ✅ Is **communication encrypted**? (Open vs. secure tunnel vs. end-to-end)
- ✅ Are **user activities logged** and **auditable**?
- ✅ Can content be **truly deleted**?
- ✅ Are meetings **protected from unauthorized access**?
- ✅ Can attendees **inject media/files** into sessions?
- ✅ Are there **ads, tracking, or data collection** concerns?
- ✅ Are **recordings controlled** and **access managed**?

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 594-595

# CHAPTER 12

## Secure Communications and Network Attacks

### Instant Messaging (IM) and Chat

**What Is IM?**

- Real-time text-based communication between two or more users
- May include:
  - File transfer, Multimedia sharing, Voice/video conferencing
- Architectures:
  - **Peer-to-peer**: harder to control or secure
  - **Centralized/cloud-based**: easier deployment, harder corporate management

**Security Risks of IM**

- ❌ Susceptible to **eavesdropping** & **packet sniffing**
- ❌ Often lacks:
  - **Encryption**
  - **Multifactor Authentication (MFA)**
  - **Privacy protection**
- ❌ Vulnerable to:
  - **Malware infections** via file transfers
  - **Social engineering attacks** (e.g., phishing, impersonation)

**Best Practices**

- Use enterprise-grade messaging with:
  - End-to-end encryption
  - MFA and secure authentication
  - Logging & audit capabilities
- Train users to:
- Recognize social engineering
- Avoid sharing sensitive data via chat
- Avoid opening suspicious links/files

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 596

# CHAPTER 12

## Secure Communications and Network Attacks

### Monitoring and Management

**Core Concepts**

- **Network Monitoring & Observability**
  - Gathers metrics, logs, and traces
  - Provides visibility into internal network behavior
  - Enables issue detection and performance optimization
- **Traffic Flow & Shaping**
  - Controls data flow to avoid congestion
  - Prioritizes critical traffic
  - Ensures consistent user experience
- **Capacity Management**
  - Plans for current/future demand
  - Allocates network resources efficiently
  - Supports scalability and performance
- **Fault Detection & Handling**
  - Identifies and responds to errors/failures
  - Minimizes downtime via automation (alerts/notifications)
  - Implements fault tolerance and resilience strategies

**Tools & Technologies**

- Network monitoring software
- Traffic shaping mechanisms
- Predictive analytics

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 596-597

# CHAPTER 12

## Secure Communications and Network Attacks

### Load Balancing in Network Security

#### Purpose of Load Balancing

- Optimize infrastructure utilization
- Minimize response time
- Maximize throughput
- Eliminate overloading
- Prevent bottlenecks

#### What Load Balancers Do

- Distribute network traffic across multiple:
  - Links
  - Devices
  - Servers (e.g., server farms or clusters)
- Improve availability, reliability, and performance

#### Types & Features

- **Types:**
  - Software-based
  - Hardware-based
- **Common Features:**
  - Caching
  - TLS offloading
  - Compression & buffering
  - Error checking
  - Filtering
  - Firewall/IDS integration

**Load Balancing Methods (Scheduling Techniques)**

- Round-robin
- Least connections
- Weighted distribution
- IP-hash-based methods
  *(Refer to Table 12.1 for specifics)*

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 597

# CHAPTER 12

## Secure Communications and Network Attacks

**TABLE 12.1** Common load-balancing scheduling techniques

| Technique | Description |
|---|---|
| Random choice | Each packet or connection is assigned a destination randomly. |
| Round robin | Each packet or connection is assigned the next destination in order, such as 1, 2, 3, 4, 5, 1, 2, 3, 4, 5, and so on. |
| Load monitoring | Each packet or connection is assigned a destination based on the current load or capacity of the targets. The device/path with the lowest current load receives the next packet or connection. |
| Preferencing or weighted | Each packet or connection is assigned a destination based on a subjective preference or known capacity difference. For example, suppose system 1 can handle twice the capacity of systems 2 and 3; in this case, preferencing would look like 1, 2, 1, 3, 1, 2, 1, 3, 1, and so on. |
| Least connections/traffic/latency | Each packet or connection is assigned a destination based on the least number of active connections, traffic load, or latency. |
| Locality based (geographic) | Each packet or connection is assigned a destination based on the destination's relative distance from the load balancer (used when cluster members are geographically separated or across numerous router hops). |
| Locality based (affinity) | Each packet or connection is assigned a destination based on previous connections from the same client, so subsequent requests go to the same destination to optimize continuity of service. Aka persistence. |


TLS offloading is the process of removing the TLS-based encryption from incoming traffic to relieve a web server of the processing burden of decrypting and/or encrypting traffic sent.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 597-598

# CHAPTER 12

## Secure Communications and Network Attacks

### Virtual IP Addresses (VIPs) & Load Balancing

#### What Are Virtual IPs (VIPs)?

- Not tied to a specific interface — mapped to a server cluster.
- Entry point for clients; load balancer redirects traffic to backend servers.
- Ensures **even traffic distribution** and prevents bottlenecks.

#### Benefits of VIPs in Load Balancing

- **Optimized Resource Utilization:** Distributes requests using algorithms/schedules.
- **High Availability:** Supports automatic failover to healthy servers.
- **Scalability:** Easily add/remove servers with no client disruption.
- **Redundancy:** Seamless service continuity during outages or failures.

#### Advanced Load Balancing Capabilities

- **SSL/TLS Termination:** Decrypts traffic at the VIP before distribution.
- **Content Switching:** Routes traffic based on:
  - Content type
  - Application-specific services

#### Global Server Load Balancing (GSLB)

- VIPs distribute traffic **across multiple data centers globally**.
- Considers:
  - **Proximity**
  - **Server health**
  - **Performance & availability criteria**
- Improves **resiliency**, **latency**, and **global user experience**.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 594-595

# CHAPTER 12

## Secure Communications and Network Attacks

### Active-Active vs. Active-Passive Load Balancing

**Active-Active Load Balancing**

- All systems/pathways are active and share traffic under **normal operations**.
- In case of failure, remaining active components handle the full load.
- Focuses on **maximum performance and resource utilization**.
- **Reduced availability** may occur under failure conditions due to redistributed load.
- Used when **throughput and efficiency** are prioritized during normal operations.

**Active-Passive Load Balancing**

- Primary systems handle all traffic; backup systems remain **dormant** until needed.
- Upon failure, passive systems are activated to take over the workload.
- Focuses on **availability consistency** even during adverse conditions.
- Often used in environments with **strict uptime and service continuity requirements**.
- Ideal for **critical systems** where **predictable performance** is essential.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 598-599

# CHAPTER 12

## Secure Communications and Network Attacks

### Manage Email Security

**Core Email Infrastructure**

- **SMTP (TCP port 25)**: Transports email from clients to servers and between servers.
- **POP3 (TCP port 110)** & **IMAP4 (TCP port 143)**: Retrieve email from server inboxes.
- **X.400**: Standard for addressing and handling Internet-compatible email.

**Common Email Servers**

- **Postfix**: Dominant SMTP server for Unix systems (replaced Sendmail).
- **Microsoft Exchange**: Most common for Windows systems.
- **All conform to SMTP standards and support core functionality.**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 599-600

# CHAPTER 12

## Secure Communications and Network Attacks

### Manage Email Security (cont.)

**SMTP Server Security**

- **Avoid Open Relays**:
  - Open Relay = No sender authentication → prime target for **spammers**.
  - Solution: Implement **authenticated relays** with **strong authentication**.
- **Attack Techniques on Email**:
  - Social engineering
  - Credential stuffing/spraying/guessing
  - Hijacking authenticated session

**SaaS Email Solutions**

- **Examples**: Gmail (Workspace), Outlook/Exchange Online
- **Benefits**:
  - High availability & distributed architecture
  - Simplified access & standardized configurations
  - Physical location independence
- **Risks**:
  - Blocklisting, rate limiting
  - Add-on restrictions
  - Limited control over advanced security mechanisms

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 599-600

# CHAPTER 12

## Secure Communications and Network Attacks

### Email Security Goals

**Why Basic Email is Insecure**

- Internet-standard email lacks:
  - 🔒 **Confidentiality**
  - ✅ **Integrity**
  - 📪 **Availability**
- Requires **supplemental controls** for security.

**Primary Email Security Objectives**

- 🔐 **Confidentiality**: Restrict access to intended recipients only.
- 🧩 **Integrity**: Ensure message content is not altered.
- 📜 **Authentication**: Verify the source of messages.
- ✍️ **Nonrepudiation**: Prevent sender from denying a message.
- 📦 **Verified Delivery**: Confirm message was received.
- 🗂️ **Content Classification**: Flag and protect sensitive information.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 599

# CHAPTER 12

## Secure Communications and Network Attacks

### Email Security Goals (cont.)

**Availability Considerations**

- No absolute guarantee, but mitigate via:
  - **Multiple access vectors** (LAN, Internet, mobile)
  - **Redundant infrastructure**
  - **Verified delivery mechanisms**

**Policy-Driven Email Security**

Starts with a **formal security policy**, approved by senior management:

1. **Acceptable Use Policies (AUPs)**
2. **Access Control & Privacy Guidelines**
3. **Email Management Procedures**
4. **Backup & Retention Requirements**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 600-601

# CHAPTER 12

## Secure Communications and Network Attacks

### Understand Email Security Issues

#### Protocol Weaknesses

- **SMTP, POP3, IMAP** transmit messages in **plaintext**
- No **native encryption**, **integrity**, or **authentication**
- Susceptible to:
  - **Eavesdropping**
  - **In-transit message tampering**
  - **Source spoofing**

#### Malicious Content Threats

- Common delivery method for:
  - **Viruses**, **worms**, **Trojans**, **malicious macros**
- HTML email = risk vector:
  - Auto-rendered **JavaScript**
  - **Hyperlinks** that auto-download & execute code

#### Source & Header Spoofing

- Easy to **spoof sender address**
- Headers can be altered **at origin or in transit**
- Emails can be injected **directly into SMTP inboxes**

#### Denial of Service (DoS) Attacks via Email

- **Mail Bombing**: Flood inbox/SMTP with messages
  - Fills storage, maxes out processing power
- **Mail Storm**: Reply-All chain reaction
  - Amplified by **auto-responders**

#### Spam as an Attack Vector

- **Spam = Unsolicited, irrelevant, or inappropriate emails**
- Wastes resources, clogs systems
- Often **spoofed sources** → hard to block

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 601

# CHAPTER 12

## Secure Communications and Network Attacks

### Email Security Solutions

**Purpose of Email Security**

- Tailor security to **message sensitivity**
- Goal: Ensure **confidentiality**, **integrity**, **authentication**, and **nonrepudiation**
- Enhance security **without overhauling** the SMTP infrastructure

**S/MIME (Secure/Multipurpose Internet Mail Extensions)**

- **Standards-based** (IETF): Adds **PKI-based security** to email
- Provides:
  - **Authentication** (X.509 certificates from trusted CAs)
  - **Confidentiality** (PKCS-based encryption)
  - **Integrity** and **Nonrepudiation**
- **Message Types**:
  - **Signed** → integrity, authentication, nonrepudiation
  - **Enveloped** → confidentiality, recipient authentication

**PGP (Pretty Good Privacy)**

- **Peer-to-peer** encryption system (not standards-based)
- Uses **public-private key encryption** for email & files
- Relies on:
  - **User-generated key pairs**
  - **Web of trust** instead of hierarchical CAs
- Considered a **de facto standard**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 602

# CHAPTER 12

## Secure Communications and Network Attacks

### Email Authentication Protocols – DKIM, SPF, DMARC

**DKIM (DomainKeys Identified Mail)**

- **Digitally signs** outbound messages using **private key**
- Recipient verifies signature using **public key in DNS**
- Ensures:
  - **Message integrity**
  - **Sender authenticity**
- Prevents: **spoofing, tampering, phishing**

**SPF (Sender Policy Framework)**

- Lists **authorized email servers** for a domain via **DNS records**
- Receiving mail server checks if the **sending server IP is allowed**
- Prevents:
  - **Sender forgery**
  - **Unauthorized server use**

**Why Authentication Matters**

- Email spoofing enables phishing, BEC (Business Email Compromise), and spam
- These protocols provide a **layered approach** to verifying email legitimacy

**DMARC (Domain-based Message Authentication Reporting & Conformance)**

- Builds on **SPF** and **DKIM**
- Domain owner:
  - Publishes **policy** on handling failed auth (none/quarantine/reject)
  - Receives **reports** on spoofing attempts
- Helps defend against:
  - **Phishing**
  - **BEC**
  - **Spoofed domain attacks**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 602-603

# CHAPTER 12

## Secure Communications and Network Attacks

### STARTTLS vs. Implicit SMTPS – Securing Email Transport

**Why Secure SMTP Matters**

- Native email protocols (SMTP, POP3, IMAP) **transmit data in plaintext**
- Threats: **Eavesdropping**, **Tampering**, **Spoofing**

**STARTTLS (Explicit TLS / Opportunistic TLS)**

- **SMTP command**, not a protocol
- Begins with a **plaintext connection** (typically on **TCP port 587**)
- If TLS is supported:
  - **Negotiates encryption mid-session**
- If TLS is **not** supported:
  - Falls back to plaintext (unless configured to reject)
- Also used with:
  - **IMAP** (port 143)
  - **POP3** (via **STLS**, port 110)

**Implicit SMTPS (Secure SMTP)**

- Connection **starts encrypted** (TLS required from the start)
- Uses **TCP port 465**
- If TLS is **not** supported:
  - Connection is **rejected**
- More secure by default, but **less flexible** than STARTTLS

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 604

# CHAPTER 12

## Secure Communications and Network Attacks

### Free PGP Solutions – OpenPGP & GnuPG

**PGP and Its Variants**

- **Pretty Good Privacy (PGP)**:
  - Originally **free** encryption software for securing emails and files
  - Now a **commercial product** (e.g., Symantec PGP)

**OpenPGP – Open Standard**

- Based on original PGP concepts
- Defined as a **standard for encryption and signing**
- Enables **interoperability** among compliant systems

**GnuPG (GPG) – Free and Open Source**

- **GNU Privacy Guard** (https://gnupg.org)
- Compliant with the **OpenPGP standard**
- Free, actively maintained tool for:
  - Encrypting/Decrypting emails and files
  - Digital signatures
- Works with email clients like:
  - Thunderbird (via **Enigmail** or **OpenPGP integration**)
  - Outlook (via plugins)

**PGP** = commercial | **OpenPGP** = standard | **GnuPG (GPG)** = FOSS implementation

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 603

# CHAPTER 12

## Secure Communications and Network Attacks

### Email Threat Mitigation Techniques

**Security Mechanisms to Reduce Email Vulnerabilities**

- **Digital Signatures** → Prevent impersonation & support **nonrepudiation**
- **Encryption (e.g., S/MIME, PGP/GPG)** → Protect message **confidentiality** from eavesdropping
- **Attachment Controls**:
  - Block all or **specific extensions** (.exe, .js, .vbs, etc.)
  - Apply **100% no-attachments policy** or **conditional filtering**
  - Pair with **user awareness training** & **antimalware scanning**

**Spam & Malicious Email Mitigation**

- **Email Filters**:
  - **Content & pattern filters** (e.g., SpamAssassin)
  - **Challenge/Response** filters for unknown senders
- **Block List Services**:
  - Prevent mail from known abusers
  - Examples: Spamhaus ZEN, BRBL, Symantec Email Security.cloud
- **Email Reputation Filtering**:
  - Grade senders based on trust & past behavior
  - Examples:
    - Sender Score
    - Cisco SenderBase
    - Barracuda Reputation Block List

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 603

# CHAPTER 12

## Secure Communications and Network Attacks

### Fax Security Considerations

**Fax Communications Risks**

- **Eavesdropping**: Like other telephone transmissions, faxes can be intercepted
- **Physical Exposure**: Auto-printed faxes may be viewed by unauthorized individuals
- **Data Residue**: Faxes stored in device memory or local storage may be retrievable later

**Fax Security Controls**

- **Fax Encrypters**: Encrypt fax signals before transmission
- **Link Encryption**: Use **VPNs** or **secure phone lines** for transmission paths
- **Activity Logs & Exception Reports**: Monitor and alert on abnormal faxing behavior

**Secure Fax Reception Practices**

- **Disable Auto-Print**: Prevent unattended sensitive documents in output trays
- **Avoid Retention in Memory/Storage**: Use devices that do not save fax images
- **Use Digital Routing**: Forward faxes to secure **email inboxes** instead of physical printing

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 604

# CHAPTER 12

## Secure Communications and Network Attacks

### Virtual Private Network (VPN)

**What is a VPN?**

- A **secure communication channel** across an untrusted network (e.g., the Internet)
- Provides:
  - **Access control**
  - **Authentication**
  - **Confidentiality**
  - **Integrity**
- *Encryption is common but not required*

**VPN Technologies**

- **VPN Concentrator** (aka VPN server/gateway/firewall/proxy/appliance)
  - Handles **hundreds to thousands** of VPN sessions
  - Offers **scalability**, **availability**, and **performance**
  - Makes VPN usage **transparent to hosts**

**Limitations**

- VPNs **do not guarantee availability**
- VPN traffic still subject to **DoS attacks** or **network outages**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 605

# CHAPTER 12

## Secure Communications and Network Attacks

### Tunneling – Foundation of VPN Communication

**What is Tunneling?**

- **Encapsulation** of one protocol inside another
- Creates a "**logical tunnel**" through an untrusted network
- Provides **secure delivery** and optional **encryption**
- Example: Letter in envelope analogy (content + protective layer)

**Use Cases for Tunneling**

- Secure communication over **untrusted networks** (e.g., Internet)
- Bypass **firewalls, proxies, or traffic control devices**
- Link networks across different **protocols** or **non-routable** environments
- Enable **remote access** via dial-up, WANs, or temporary links

**Security Benefits**

- **Confidentiality** and **integrity** if encryption is used
- Allows **legacy/non-routable protocols** to communicate over IP
- Supports secure data delivery even through restrictive networks

**Challenges & Limitations**

- **Inefficiency**: Overhead from double protocol management
- **Larger packet sizes → Higher bandwidth consumption**
- **No broadcast support**
- **Opaque to security tools** (e.g., firewalls, IDS, AV)
  - Tools must operate **outside the VPN tunnel**, post-decryption

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 605-606

# CHAPTER 12

## Secure Communications and Network Attacks

### How VPNs Work – Secure Remote Connectivity

🌐 **VPN Fundamentals**

- Creates a **secure tunnel** over untrusted networks (e.g., Internet)
- Simulates a **direct LAN connection** for remote systems
- Can connect:
  - 🔷 Two **individual hosts**
  - 🔷 Two **entire networks**
- Used with any connection: LAN, WAN, dial-up, wireless, Internet

🔐 **What Gets Protected?**

- Data is **only encrypted inside the VPN tunnel**
- Traffic is:
  - ❌ **Unprotected** inside source LAN
  - ✅ **Protected** across the VPN tunnel
  - ❌ **Unprotected** again in destination LAN
- Border devices like **VPN firewalls or concentrators** act as tunnel endpoints

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 607-608

# CHAPTER 12

## Secure Communications and Network Attacks

### How VPNs Work – Secure Remote Connectivity (cont.)

**Remote Node Operation**

- Remote client uses VPN to act like it's **locally connected**
- Can access network resources **as if physically present**

**VPN vs. Traditional WAN**

- VPNs are a **cost-effective** alternative to leased lines
- Two high-speed ISP links can support a **secure, low-cost WAN**

**VPN Modes**

| Mode | Description | Use Case |
|---|---|---|
| **Transport** | Encrypts **payload only**, header remains intact | Host-to-host on **trusted** networks |
| **Tunnel** | Encrypts **entire packet** (header + payload) | Secure comms over **untrusted** networks |

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 607-608

# CHAPTER 12

## Secure Communications and Network Attacks

### How VPNs Work – Secure Remote Connectivity (cont.)

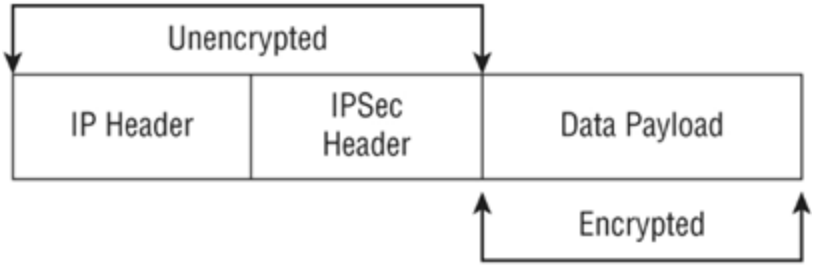



**FIGURE 12.1 IPSec's encryption of a packet in transport mode**

In transport mode, IPSec provides encryption protection for just the payload and leaves the original message header intact (see Figure 12.1). This type of VPN is also known as a host-to-host VPN or an end-to-end encrypted VPN, since the communication remains encrypted while it is in transit between the connected hosts.

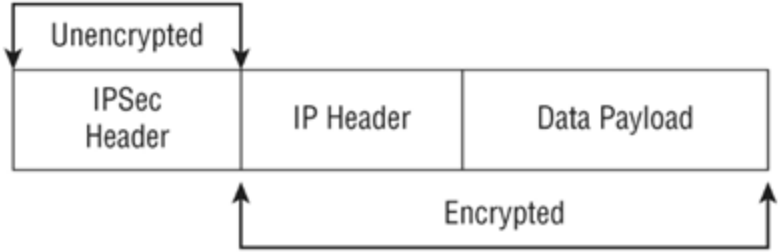



**FIGURE 12.2 IPSec's encryption of a packet in tunnel mode**

Tunnel mode links or VPNs terminate (i.e., are anchored or end) at VPN devices on the boundaries of the connected networks (or one remote device). In tunnel mode, IPSec provides encryption protection for both the payload and message header by encapsulating the entire original LAN protocol packet and adding its own temporary IPSec header (see Figure 12.2).

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 608

# CHAPTER 12

## Secure Communications and Network Attacks

### How VPNs Work – Secure Remote Connectivity (cont.)

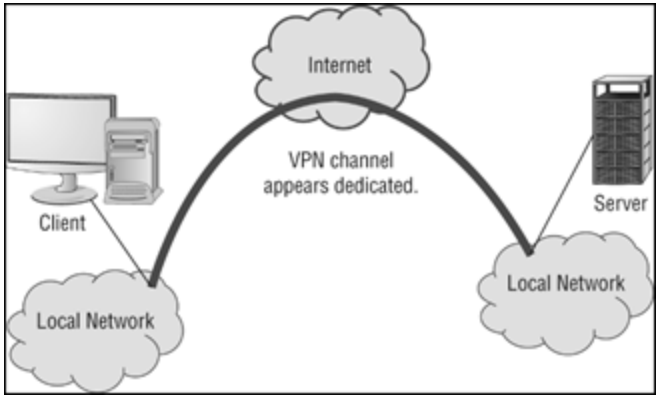



**FIGURE 12.3 Two LANs being connected using a tunnel-mode VPN across the Internet**

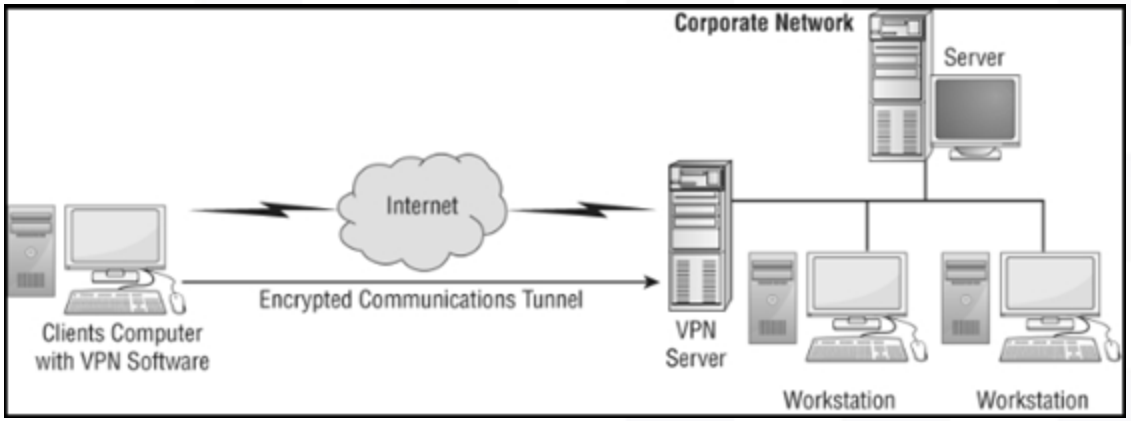



**FIGURE 12.4 A client connecting to a network via a remote-access/tunnel VPN across the Internet**

Numerous scenarios lend themselves to the deployment of tunnel mode VPNs; for example, VPNs can be used to connect two networks across the Internet (see Figure 12.3) (aka site-to-site VPN) or to allow distant clients to connect to an office local area network (LAN) across the Internet (see Figure 12.4) (aka remote access VPN). Once a VPN link is established, the network connectivity for the VPN client is the same as a local LAN connection. A remote access VPN is a variant of the site-to-site VPN. This type of VPN is also known as a link encryption VPN, since encryption is only provided when the communication is in the VPN link or portion of the communication. There may be network segments before and after the VPN, which are not secured by the VPN.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 609-610

# CHAPTER 12

## Joke break

Why did the **CAN**, **MAN**, and **WAN** go to therapy?

Because the **CAN** had control issues,

the **MAN** was always in the middle of things,

and the **WAN** just couldn't handle the distance!

Source: ChatGPT

# CHAPTER 12

## Secure Communications and Network Attacks


TIP

A *wide area network* (*WAN*) is a network over a long distance. A *metropolitan area network* (*MAN*) is a network within a town or city. A *campus area network* (*CAN*) is a network within a college campus or a business park. A VPN can be used over any type of network.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 609

# CHAPTER 12

## Secure Communications and Network Attacks

### Always-On VPN & Tunnel Configurations

**Always-On VPN**

- **Auto-connects** to VPN whenever a network becomes active
- Common on **mobile devices** and laptops
- Configurable triggers:
  - When **Internet** becomes active
  - When **Wi-Fi** is detected (vs. wired)
- Protects users on **untrusted public networks**
- Ensures **consistent encryption & security** without user action

**Split Tunnel VPN**

- Simultaneous access to:
  - **Internet (unsecured)** via local ISP
  - **Organization LAN (secured)** via VPN
- **Security risk**: Creates a **bridge** between Internet and LAN
  - Can bypass firewall protections
  - Easier **pathway for malware, intrusions, data leaks**
- Not ideal for sensitive environments

**Full Tunnel VPN**

- **All client traffic** sent through the VPN to org's network
- Internet access routed via:
  - **Org's firewall**
  - **Proxy or security tools**
- Ensures **centralized filtering**, logging, and threat prevention
- **More secure**, but can introduce latency

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 609-610

# CHAPTER 12

## Secure Communications and Network Attacks

### Common VPN Protocols

**Common VPN Protocols Overview**

- **VPNs** can be implemented via software or hardware. Common protocols include:
  - **PPTP**, **L2TP**, **SSH**, **OpenVPN (TLS)**, **IPSec**

**Point-to-Point Tunneling Protocol (PPTP)**

- **Layer:** OSI Layer 2 (Data Link)
- **Port:** TCP 1723
- **Auth:** PPP-based – PAP, CHAP, EAP, MS-CHAPv2
- **Encryption:**
  - Initial tunnel setup **not encrypted**
  - Uses **MPPE** with MS-CHAPv2
- **Status: Obsolete**, weak security, but still supported in legacy systems
- **CISSP Tip:** Do **not** recommend PPTP for secure environments.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 610-612

# CHAPTER 12

## Secure Communications and Network Attacks

### Password Authentication Protocol (PAP)

- **Oldest and simplest authentication protocol**
- Sends **username and password in cleartext**
- Vulnerable to interception and replay attacks
- Rarely used in modern systems

### Challenge Handshake Authentication Protocol (CHAP)

- Uses a **challenge-response** mechanism to authenticate
- Password is never sent over the network
- Periodic re-authentication
- More secure than PAP

### Extensible Authentication Protocol (EAP)

- **Framework protocol** that supports multiple authentication methods:
  - Passwords, Digital certificates, Smart cards, Kerberos, Token devices
- Commonly used in wireless networks (e.g., WPA2-Enterprise)

### Microsoft CHAP v2 (MS-CHAPv2)

- **Microsoft's enhanced version of CHAP**
- Offers mutual authentication
- Compatible with Microsoft remote access and VPN solutions
- Includes **stronger encryption algorithms**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 610

# CHAPTER 12

## Secure Communications and Network Attacks

### Common VPN Protocols (cont.)

🌐 **Layer 2 Tunneling Protocol (L2TP)**

- **Layer:** OSI Layer 2
- **Port:** UDP 1701
- **Developed From:** PPTP + Cisco L2F
- **Auth:** IEEE 802.1X (EAP derivative), supports RADIUS/TACACS+
- **Encryption:**
  - No native encryption
  - Commonly paired with **IPSec ESP** for secure payload
- 📝 **CISSP Tip: Use with IPSec** for confidentiality, integrity, and authentication.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 610-612

# CHAPTER 12

## Secure Communications and Network Attacks

### Common VPN Protocols (cont.)


🔐 **Secure Shell (SSH)**

- **Layer:** Application Layer
- **Port:** TCP 22
- **Use Cases:**
  - Secure replacement for Telnet, rsh, rlogin, etc.
  - Remote management of systems (firewalls, servers, routers)
- **Security:**
  - All transmissions (auth + data) are **encrypted**
  - Tools like **PuTTY**, **Minicom**, and **OpenSSH** used for access
- **As a VPN:**
  - Can function as a **VPN in transport mode only** (host-to-host)
  - Encrypts specific sessions or protocols (e.g., SCP, SFTP)
- 📝 **CISSP Tip:** SSH is excellent for **secure remote access**, but limited for **site-to-site VPN** functionality.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 610-612

# CHAPTER 12

## Secure Communications and Network Attacks

### Common VPN Protocols (cont.)

**OpenVPN**

**Overview:**

- Open-source VPN solution based on **TLS (formerly SSL)**.
- Offers **strong encryption** and flexible authentication methods.

**Authentication Options:**

- **Preshared keys (PSK)**: Easier to set up, suitable for smaller environments.
- **Certificates**: More secure, scalable for enterprise use.

**Advantages:**

- **Robust security** with TLS encryption.
- **Easy configuration** for both client and server.
- **Cross-platform compatibility** (Windows, macOS, Linux, iOS, Android).
- **WAP Integration**: Many wireless access points support OpenVPN as a VPN gateway.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 610-612

# CHAPTER 12

## Secure Communications and Network Attacks

### Introduction to IPSec

**IP Security Protocol (IPSec)**

- IPSec is a suite of security protocols for IP networks
- **Integrated into IPv6**, optional in IPv4
- Primary use: **VPN** creation between hosts or networks
- Provides:
  - **Authentication**
  - **Encryption**
  - **Access control**
  - **Message integrity**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 612

# CHAPTER 12

## Secure Communications and Network Attacks

### IPSec Protocol Components

**IPSec includes the following protocols:**

- **AH (Authentication Header)**:
  - Ensures **message integrity**, **nonrepudiation**, and prevents **replay attacks**
- **ESP (Encapsulating Security Payload)**:
  - Provides **confidentiality (encryption)** and limited authentication
  - Supports **transport** and **tunnel** modes
- **HMAC (Hash-based Message Authentication Code)**:
  - HMAC– **integrity validation**
- **IPComp (IP Payload Compression)**:
  - **Compression** before encryption to improve speed
- **IKE (Internet Key Exchange)**:
  - Manages **cryptographic key exchange**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 612

# CHAPTER 12

## Secure Communications and Network Attacks

### IKE and Key Exchange

**IKE (Internet Key Exchange)** uses:

- **OAKLEY** – Key generation/exchange (like Diffie–Hellman)
- **SKEME** – Key exchange method (digital envelope)
- **ISAKMP** – Manages and negotiates keying material and **Security Associations (SAs)**
- **Modern IKE may use**:
- **ECDHE** – Ephemeral key exchange for forward secrecy
- 🔐 **Security Associations (SAs)**:
- Each VPN requires **two SAs** (one for inbound, one for outbound)
- SAs are **simplex** – one-way secure communication channels

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 612

# CHAPTER 12

## Secure Communications and Network Attacks

### IPSec Modes

**Transport Mode**:
- Encrypts **payload only**
- Used for **end-to-end host communication**

**Tunnel Mode**:
- Encrypts **entire IP packet**
- Common in **VPNs between gateways**

### IPSec Cryptographic Features

- **Hybrid cryptography**:
  - Uses **public-key cryptography** for key exchange
  - Uses **symmetric cryptography** for payload encryption
- Offers:
  - **Encryption (confidentiality)**
  - **Authentication**
  - **Integrity**
  - **Nonrepudiation**
  - **Replay protection**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 612

# CHAPTER 12

## Secure Communications and Network Attacks

### Switching and VLANs

#### Switch Basics

- Operate at **Layer 2 (Data Link)**; **Layer 3 switches** include routing capabilities.
- Key switch functions:
  - **Learning**: Builds CAM table using source MAC addresses.
  - **Forwarding**: Sends frame to destination port if MAC is known.
  - **Dropping**: Discards frame if source/destination port is the same.
  - **Flooding**: Broadcasts frame when destination MAC is unknown.
- **CAM Table**
- Stores **MAC-to-port mappings**.
- Enables efficient switching without unnecessary broadcasting.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 613-614

# CHAPTER 12

## Secure Communications and Network Attacks

### Switching and VLANs (cont.)

**Security & Performance Uses**

- Segment user, management, and guest traffic.
- Enforce **“deny by default, allow by exception”**.
- Reduce broadcast domains and **limit attack surfaces**.
- Common VLAN filters:
  - By **port**, **MAC**, **IP subnet**, or **authentication**.

**Modern Considerations**

- **Virtual switches** in cloud or VMs use **software-defined VLANs**.
- VLANs are examples of **virtualized networks**, not subnets.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 613-614

# CHAPTER 12

## Secure Communications and Network Attacks

### VLAN Security Features & Network Virtualization

**VLANs Reduce Broadcast Vulnerabilities**

- VLANs are **treated as isolated networks** by switches.
- **Broadcasts do not cross VLANs** due to Layer 3 routing restrictions.
- Helps prevent **broadcast storms** (floods of unwanted Layer 2 traffic).

**Private VLANs (Port Isolation)**

- Devices in a private VLAN can only:
  - Communicate **within the VLAN**.
  - Use a **dedicated uplink port** for outside access.
- Common in **hotels**, **shared offices**, etc.

**Trunk Ports & VLAN Tagging**

- **Trunk Port**: Used to link switches; supports **multiple VLANs**.
- **IEEE 802.1Q (Dot1q)**: Adds **VLAN tag** to Ethernet frame headers:
  - Standard header: [Dst MAC | Src MAC | Ethertype]
  - Tagged header: [Dst MAC | Src MAC | VLAN | Ethertype]
- Only **trunk ports** understand VLAN tags.


Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 614-615

# CHAPTER 12

## Secure Communications and Network Attacks

### Switch Eavesdropping Techniques

**Port Mirroring (SPAN)**

- **SPAN = Switched Port Analyzer**
- Duplicates traffic from **one or more switch ports** to a designated port.
- Enables real-time traffic monitoring or packet capture.
- Used by:
  - **IDS/IPS systems**
  - **Forensics tools**
  - **Security analysts**

**Port Tap (Inline Tap)**

- Hardware device **physically inserted** into a network link.
- **Duplicates traffic** without disrupting transmission.
- Useful when:
  - SPAN isn't available.
  - Need to monitor a **non-switch connection**.
- Replaces legacy **vampire taps**.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 615

# CHAPTER 12

## Secure Communications and Network Attacks

### MAC Flooding Attack

💣 **What Is It?**

- An **attack on Layer 2 (Data Link Layer)** targeting switches.
- The attacker **floods the switch** with Ethernet frames using **randomized source MAC addresses**.

📉 **Impact on the Switch**

- The switch tries to **learn** each new MAC and fills up the **CAM (Content Addressable Memory) table**.
- When CAM table is full:
  - **Legitimate entries are dropped** (FIFO behavior).
  - Switch **can't forward frames properly**.
  - Switch **reverts to flooding mode**, sending all traffic out of all ports (like a hub).

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 615-616

# CHAPTER 12

## Secure Communications and Network Attacks

### MAC Flooding Attack (cont.)

**Goal of the Attacker**

- Not man-in-the-middle.
- Instead:
  - Makes the switch **broadcast traffic to all ports**.
  - Attacker **eavesdrops** on sensitive communications.
  - All connected devices are now **exposed to interception**.

**Defenses**

- ✅ **MAC Limiting** (on managed switches):
  - Limits the **number of unique MAC addresses** per port.
- ✅ **NIDS (Network Intrusion Detection System)**:
  - Alerts on unusual MAC address volume/activity.
- ✅ **Port Security Policies**:
  - Disable ports when abuse is detected.
  - Lock down to **known MAC addresses** if possible.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 615-616

# CHAPTER 12

## Secure Communications and Network Attacks

### 🧬 MAC Cloning (Spoofing)

**🔍 What Is It?**

- **MAC Cloning** is when an attacker **spoofs** or **falsifies** a device's MAC address.
- This is done by altering the **software-defined MAC** on the NIC to **imitate another device's address**.

**⚠️ Why It Matters**

- Every device on a local Ethernet broadcast domain **must have a unique MAC address**.
- Duplicate MACs = **conflicts**, **communication errors**, and **security risks**.

**🛠️ How It's Done**

- An attacker:
  1. **Eavesdrops** on network traffic.
  2. Identifies a **valid MAC** in use.
  3. **Modifies** their NIC to use that MAC.
     - Tools: ifconfig, ip link, MAC spoofing tools.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 616-617

# CHAPTER 12

## Secure Communications and Network Attacks

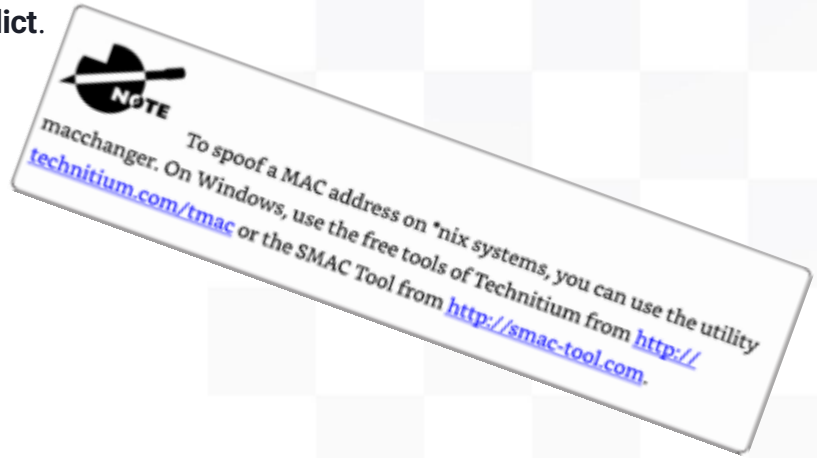
### MAC Cloning (Spoofing) (cont.)

**Risks & Attacks**

- **Impersonation**: Spoof trusted devices to bypass access controls (e.g., port security).
- **Bypass MAC filters** (on switches, firewalls, or Wi-Fi networks).
- **Session hijacking**: Replace a legitimate device on the network.
- Can cause **DoS** to the cloned device due to **MAC address conflict**.

**Defensive Measures**

- ✅ **MAC Filtering + Authentication** (e.g., 802.1X).
- ✅ **Port Security** (bind MACs to ports on managed switches).
- ✅ **Network Scanning**: Identify duplicate/conflicting MACs.
- ✅ **NIDS/IPS**: Alert on suspicious MAC activity or changes.




Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 616-617

# CHAPTER 12

## Secure Communications and Network Attacks

### 🧱 Network Address Translation (NAT)

🎯 **Goals:**

- Hide internal client identities & network design
- Reduce public IPv4 leasing costs
- Enable private networks to access public Internet

🛡️ **NAT Functions**

- Substitutes internal IPv4 addresses with external public ones
- Hides RFC 1918 private IP addresses from Internet
- Masks network topography and structure
- Enforces **one-way firewall behavior**
  - Only allows return traffic for connections initiated internally

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 616-619

# CHAPTER 12

## Secure Communications and Network Attacks

### Network Address Translation (NAT) (cont.)

#### Types of NAT

| Type | Description |
|---|---|
| **Dynamic NAT (DNAT)** | Maps private IP to public IP dynamically (1-to-1) |
| **Source NAT (SNAT)** | Maps a specific public IP/socket to an internal IP/socket (used for port forwarding) |
| **PAT (Port Address Translation)** | Maps multiple internal clients over a single public IP using port numbers (many-to-1) |
| **NAT66** | NAT for IPv6 (private → public IPv6) |

⚠ **Note:** NAT is often used interchangeably with PAT in modern systems.

#### Security Benefits

- **Egress-only traffic**: Blocks unsolicited inbound traffic by default
- **Basic anonymity**: External entities see only the public IP
- **Intrusion mitigation**: Reduces exposure surface for internal systems

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 616-619

# CHAPTER 12

## Secure Communications and Network Attacks

### 🔄 NAT Limitations & Solutions

| Issue | Description |
|---|---|
| **VPN Compatibility** | Traditional NAT breaks IPSec |
| **Fix:** NAT Traversal (NAT-T, RFC 3947) supports IPSec, L2TP | |
| **Statefulness** | NAT maintains connection state for each session |
| **Inbound Access (Static NAT)** | Not recommended for internal systems (use DMZ/screened subnet) |

### 📦 NAT in Practice

- Found in **routers**, **firewalls**, **proxies**, **gateways**, and **WAPs**
- Supports scalable Internet access with minimal public IPs
- Enables **virtualized networking** by abstracting internal IP schema

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 616-619

# CHAPTER 12

## Secure Communications and Network Attacks

### Private IP Addresses (RFC 1918)

**Why Private IPs?**

- IPv4 exhaustion due to high global demand.
- Reserved ranges allow internal use without requiring public IPs.

**RFC 1918 Private IP Ranges:**

| Class | Range | Notes |
|---|---|---|
| A | 10.0.0.0 – 10.255.255.255 | Single large block |
| B | 172.16.0.0 – 172.31.255.255 | 16 smaller subnets |
| C | 192.168.0.0 – 192.168.255.255 | Common in home networks |

WARNING Attempting to use the RFC 1918 private IPv4 addresses directly on the Internet is futile because all publicly accessible routers will drop data packets containing a source IPv4 address from these RFC 1918 ranges.

**Routing Behavior:**

- Not routed on the public Internet.
- Routers **drop** traffic with private IPs by default.

**Use in Private Networks:**

- Ideal for **LANs**, **intranets**, and **internal-only** systems.
- Can be routed internally with proper router config.

**Private IPs + NAT = ✅**

- Enables Internet access via **fewer public IPs**.
- Greatly **reduces ISP costs**.
- Adds **basic security** through IP hiding.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 619-620

# CHAPTER 12

## Secure Communications and Network Attacks

### 🌐 Stateful NAT

1. 🧠 **How It Works:**
- **Request Phase:**
  - Internal client sends a request to an Internet service.
  - NAT changes the **source IP** (private → public).
  - Stores session info:
    Internal IP ↔ External IP (destination)
2. **Reply Phase:**
- Internet server responds to NAT's public IP.
- NAT **looks up session state** in mapping table.
- Translates destination back to the original **internal client IP**.

🔄 **Key Behavior:**
- Maintains **session state**: tracks active connections.
- Ensures proper return of data to initiating client.
- Mapping is **temporary** and **removed** after session ends.

🔐 **Security Benefit:**
- Prevents unsolicited inbound connections by default.
- Functions similarly to a **basic firewall** (connection tracking).

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 621

# CHAPTER 12

## Secure Communications and Network Attacks

### Automatic Private IP Addressing (APIPA)

*Also known as IPv4 Link-Local Addressing (RFC 3927)*

🔄 **When It Happens:**
- DHCP (Dynamic Host Configuration Protocol) **assignment fails**
- System assigns itself an IP address automatically

🌐 **Address Range:**
- **169.254.0.1 – 169.254.255.254**
- Subnet mask: **255.255.0.0** (Class B)

📢 **Communication Scope:**
- Works **only within the same broadcast domain**
- **No routing** – cannot communicate across routers
- Can only talk to **other APIPA-configured systems**

💻 **Platform-Specific:**
- **Primarily used in Windows**
- **Limited support** on non-Windows systems


Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 621

# CHAPTER 12

## Secure Communications and Network Attacks

### 🔗 Third-Party Connectivity & WAN Technologies

🤝 **Third-Party Risks**

- Most orgs depend on **external partners** (vendors, cloud providers, remote workers)
- **Direct interconnection = shared risks**
  - Threats from one party can propagate to the other
  - Requires formal planning and security documentation

📝 **Key Agreements**

- **MOU (Memorandum Of Understanding) / MOA (Memorandum Of Agreement)**: Formalized *intent* or understanding; **non-binding**
- **ISA (Interconnection Security Agreement)**: Defines *technical and security* parameters of interconnection; **binding in scope**

🔐 **Risk Management**

- **Perform risk assessments** before linking environments
- Use alternatives to direct connection:
  - **Extranet w/ VPN**
  - **Shared private cloud**
  - **Secure file/email/media tools**
- Maintain security posture **even under time pressure**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 621-624

# CHAPTER 12

## Secure Communications and Network Attacks

### Third-Party Connectivity & WAN Technologies (cont.)

**Cloud Considerations**

- SaaS, IaaS = increasing direct connectivity
- Use **CASBs** to enforce policies
- Apply same caution as with other third parties
- **Remote Workers**

Require **justification** and clear access control

- Prefer **company-owned, managed equipment**
- Limit access to **extranet/public systems**

**WAN Technologies & Telecom Providers**

**Connectivity Options**

- **Leased Lines**: Private, dedicated point-to-point
- **MPLS**: Efficient routing w/ **QoS**, secure over shared networks
- **VPNs**: Secure tunnels over public infrastructure

**Hardware Support**

- **Routers, switches, WAN appliances**
- Internal or 3rd-party managed
- Essential for **troubleshooting, maintenance, redundancy**

**Modern WAN – SD-WAN**

- Software-defined, dynamic traffic routing
- **Optimizes cost and performance**
- Increasingly offered by telecoms

**Redundancy & Failover**

- Multiple providers and paths = **high availability**
- Must be planned and tested

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 621-624

# CHAPTER 12

## Secure Communications and Network Attacks

### 🔁 Switching Technologies

🔌 **Circuit Switching**

- **Dedicated path** established for the full session
- Path is **exclusive** and constant during communication
- Originally used in **PSTN (public switched telephone network)**
- Not commonly used today for data; still exists in **rail yards, irrigation, and power systems**

✅ **Advantages**:

- Fixed delays, high quality, no interruptions
- Connection-oriented, stable for voice

❌ **Disadvantages**:

- **Inefficient** – resources locked for entire session
- Disrupted if physical path fails

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 624-626

# CHAPTER 12

## Secure Communications and Network Attacks

### 🔁 Switching Technologies (cont.)

**📦 Packet Switching**

- Data split into **packets or cells**
- Each packet contains **its own header** for routing
- Uses **shared channels** — path used only while data is transmitted
- Common in **modern data networks** (e.g., internet, VoIP, etc.)

**✅ Advantages**:

- **Efficient use** of bandwidth
- **Dynamic routing** — can recover from path failures
- Supports **any data type** (voice, video, text, etc.)

**❌ Disadvantages**:

- Variable delays (latency, jitter)
- More **sensitive to data loss**

**🔒 Security Considerations**

- **Packet switching = shared channels**
  - Potential for **data leakage, eavesdropping, corruption**
- Use:
  - **Encryption**
  - **Traffic isolation**
  - **Connection management**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 624-626

# CHAPTER 12

## Secure Communications and Network Attacks

### Switching Technologies (cont.)

### Circuit vs. Packet Switching

| Feature | Circuit Switching | Packet Switching |
|---|---|---|
| Traffic | Constant | Bursty |
| Delay | Fixed | Variable |
| Connection | Connection-oriented | Connectionless |
| Loss Sensitivity | Connection | Data |
| Usage | Voice (legacy) | Any traffic |
| Path Use | Exclusive | Shared |

TABLE 12.2

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 624-626

# CHAPTER 12

## Secure Communications and Network Attacks

### 🔁 Switching Technologies (cont.)

🔁 **Virtual Circuits**

🧠 **Definition:** A **virtual circuit** is a **logical communication path** between two endpoints on a **packet-switched network**. It ensures all packets reach the destination, regardless of the physical route.

Two types:

1. **PVC – Permanent Virtual Circuit**
2. **SVC – Switched Virtual Circuit**

🔔 **Permanent Virtual Circuit (PVC)**

- **Always available**, predefined path
- Acts like a **dedicated line**
- **Remains in place** even when not in use
- Reopens instantly when needed

🟢 **Analogy**: Like a **walkie-talkie**

▶ Press to talk—predefined frequency always ready.

📈 **Switched Virtual Circuit (SVC)**

- Created **on demand** for each session
- **Dynamic routing** using current best path
- **Torn down after use**

🔁 **Analogy**: Like a **ham radio**

▶ Must tune each time to a new frequency.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 625-626

# CHAPTER 12

## Secure Communications and Network Attacks

### Switching Technologies (cont.)

#### Key Characteristics

| Feature | PVC (Permanent Virtual Circuit) | SVC (Switched Virtual Circuit) |
|---|---|---|
| Availability | Always available | Created on demand |
| Setup Time | Instant | Requires setup per session |
| Routing | Predefined | Dynamic (best current path) |
| Use Case | Frequent, consistent traffic | Occasional or bursty traffic |
| Resource Usage | More predictable | More flexible |

**Security Considerations**

- Both depend on **packet-switched networks**
- Security must address:
  - **Data integrity and confidentiality**
  - **Session management**
  - **Encryption** across virtual circuits

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 626

# CHAPTER 12

## Secure Communications and Network Attacks

### WAN Technologies

**Purpose of WANs**

WANs connect **distant networks, nodes, or devices**, enabling:

- Scalable, long-distance communication
- Centralized resource access
- Remote business operations

**Security Needs**:

- Proper connection management
- **Encryption over public links**
- Redundancy planning for fault tolerance


Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 626-628

# CHAPTER 12

## Secure Communications and Network Attacks

### WAN Technologies (cont.)

**Dedicated vs Nondedicated Lines**

| Type | Dedicated Line | Nondedicated Line |
|---|---|---|
| Access | Always on (leased, reserved) | Must connect before use |
| Connection | Point-to-point | On-demand |
| Use Case | Business sites, constant communication | General users, infrequent use |
| Examples | T1, DS3, ATM, Frame Relay (legacy) | Dial-up, DSL |

**Security Tip**: Dedicated lines are more stable but still need **encryption** if crossing public carriers.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 626-628

# CHAPTER 12

## Secure Communications and Network Attacks

### WAN Technologies (cont.)

**Fault Tolerance with Carrier Networks**

- Use **redundant connections**
- Prefer **different providers** & avoid shared backbone
- Watch for **physical path overlap** (backhoe risk!)
- If budget-limited, use **nondedicated failover line**


**Common WAN Technologies**

**MPLS (Multiprotocol Label Switching)**

- Uses **labels**, not IP addresses, to route traffic
- Efficient, scalable, supports **QoS**
- Great for linking diverse sites across carriers

**Metro Ethernet**

- Ethernet over wide area
- **High bandwidth** & scalability
- Used in backhaul networks (e.g., **cell towers**, data centers)

**Satellite Communications**

- **VSAT** enables remote terminals to access geostationary satellites
- **LEO satellites** (e.g., Starlink):
  - Lower latency than traditional satellites
  - **High-speed internet** to underserved regions

**Broadband over Power Lines (BPL)**

- Uses **existing electrical lines** for broadband
- **Limited adoption** due to interference, regulation, and alternatives

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 626-628

# CHAPTER 12

## Secure Communications and Network Attacks

### 💡 Fiber-Optic Links: Synchronous Digital Hierarchy (SDH) & Synchronous Optical Network (SONET)

🔧 **What Are They?**

- **SDH (Synchronous Digital Hierarchy)**: ITU standard (international)
- **SONET (Synchronous Optical Network)**: ANSI standard (North America)
- Both define **physical layer** optical networking
- Use **Synchronous Time-Division Multiplexing (TDM)** for high-speed, duplex, low-overhead communications

🔁 **Topologies & Use**

- Supports **Mesh** and **Ring** topologies
- Backbone for **telco services**
- Capacity is often **partitioned for subscribers**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 628-629

# CHAPTER 12

## Secure Communications and Network Attacks

### Fiber-Optic Links: SDH & SONET (cont.)

#### Structural Hierarchies

| SONET Level | SDH Level | Data Rate |
|---|---|---|
| STS-1 / OC-1 | STM-0 | 51.84 Mbps |
| STS-3 / OC-3 | STM-1 | 155.52 Mbps |
| STS-12 / OC-12 | STM-4 | 622.08 Mbps |
| STS-48 / OC-48 | STM-16 | 2.488 Gbps |
| STS-96 / OC-96 | STM-32 | 4.876 Gbps |
| STS-192 / OC-192 | STM-64 | 9.953 Gbps |
| STS-768 / OC-768 | STM-256 | 39.813 Gbps |

**Note**: SDH service numbers are **1/3 of SONET**'s at equivalent data rates.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 628-629

# CHAPTER 12

## Secure Communications and Network Attacks

### Prevent or Mitigate Network Attacks

⚠️ **What Constitutes "Harm"?**

- **More than damage**: Includes **disclosure**, **delay**, **denial**, **fraud**, **waste**, **abuse**, and **loss**
- Applies to **data, resources, and personnel**

🧨 **Common Network Attack Types**

- **DoS/DDoS** – Disrupts availability
- **Impersonation** – Pretending to be a trusted identity
- **Replay Attacks** – Re-sending valid data to trick systems
- **ARP Poisoning** – Falsifying MAC/IP associations
- **DNS Poisoning** – Redirects DNS resolution to malicious sites
- **Eavesdropping** – Stealthy interception of network traffic
- **Transmission Modification** – Changes to data in transit

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 629-630

# CHAPTER 12

## Secure Communications and Network Attacks

### Prevent or Mitigate Network Attacks (cont.)

**Eavesdropping Attacks**

- **Passive attack**: Uses sniffers or protocol analyzers (e.g., Wireshark)
- May involve:
  - Cable splicing or open port access
  - Software installed on endpoints
- Goal: **Capture sensitive data** (e.g., passwords, usernames)

**Countermeasures:**

- **Physical security**: Limit physical access
- **Encryption**: IPSec, SSH, TLS
- **One-time auth**: Token devices, OTP pads
- **Application allowlisting**: Block sniffers & rogue software

**Modification Attacks**

- Packets are **altered and replayed** to bypass security
- Goal: **Session hijacking**, **bypass auth**, or **inject commands**

**Countermeasures:**

- **Digital signatures**
- **Packet checksum/integrity checks**
- **TLS/IPSec**: Provides message integrity and authentication

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 629-630

# CHAPTER 12

## Secure Communications and Network Attacks

### Summary

**Securing TCP/IP and Communication Channels**

**TCP/IP Overview**

- Primary protocol suite for networks/Internet
- **Robust, but insecure by default**
- Requires added **authentication and encryption**

### Securing Communication Types

| Communication Type | Security Considerations |
|---|---|
| **Voice** | Harden PSTN, PBX, Mobile, VoIP (use **SRTP**) |
| **Remote Access** | Use secure protocols (IPSec, SSH, TLS), enforce **strong authentication** |
| **Email** | Secure with **S/MIME, PGP**, nonrepudiation, classification, **AV filters** |
| **Multimedia/IM** | Secure channels, control access, audit logs |
| **Virtual Networks** | Use SDNs, VLANs, virtual switches, **NAT**, and **VPNs** |

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 630-632

# CHAPTER 12

## Secure Communications and Network Attacks

### Summary (cont.)

**Remote Access and VPNs**

- **Telecommuting** introduces risks
- Solutions must cover **authentication**, **encryption**, and **policies**
- **VPNs** use **tunneling + encryption**
  - Common protocols: **IPSec, TLS, SSH, L2TP, PPTP**

**Email Security Essentials**

- Insecure by default – must:
  - Restrict access
  - Verify authenticity & delivery
  - Ensure **confidentiality, integrity, and nonrepudiation**
- Defenses:
  - **Spam filters**, **IDS/IPS**, **AV software**
  - **User training** vs. social engineering

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 630-632

# CHAPTER 12

## Secure Communications and Network Attacks

### Summary (cont.)

**Virtual Networks & VLANs**

- **Virtual networks** improve security/performance:
  - **SDNs, VLANs, vSwitches, NAT, port isolation**
- **VLANs**: Logical segmentation by switches
- **NAT**: Hides internal IPs, allows multiple clients via few public Ips

**Third-Party Connectivity & WANs**

- Risks rise with **interconnected organizations**
- Always establish **MOU** → **ISA** before linking
- WAN types:
  - **Dedicated line**: Always-on between two endpoints
  - **Nondedicated**: On-demand (e.g., dial-up, VPN)

**Common Network Attacks**

- **DDoS, Eavesdropping, Spoofing, Replay, ARP/DNS Poisoning**
- Key defenses:
  - **Encryption**
  - **Strong access controls**
  - **Traffic filtering**
  - **IDS/IPS**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 630-632

# CHAPTER 12

## Secure Communications and Network Attacks

### Study Essentials

**Communication & Remote Access Security – Study Essentials**

**PPP & Authentication Protocols**

- **PPP**: Encapsulates IP over dial-up/point-to-point links
  - **PAP**: Sends credentials in cleartext – *insecure*
  - **CHAP**: Challenge-response, prevents replay attacks
  - **EAP**: Framework for extensible/custom auth methods

**IEEE 802.1X & Port Security**

- **IEEE 802.1X**: Port-Based Network Access Control using **EAP**
- **Port Security** can refer to:
  - **Physical access control** (e.g., RJ-45 jacks)
  - **TCP/UDP port management**
  - **Authentication before port use** (e.g., 802.1X)

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 632-634

# CHAPTER 12

## Secure Communications and Network Attacks

### Study Essentials (cont.)

#### Voice Communications Security

| System | Threats | Countermeasures |
|---|---|---|
| **PBX** | Fraud, abuse | Logical, physical, administrative controls |
| **VoIP** | Spoofing, vishing, DoS, MitM, switch hopping | Network hardening, SRTP, firmware integrity |
| **Phreaking** | Free calls, disruption | Secure configurations, usage monitoring |

- Use **encryption** for voice **confidentiality**
- Train users against **social engineering**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 632-634

# CHAPTER 12

## Secure Communications and Network Attacks

### Study Essentials (cont.)

**Remote Access Security**

- Requires protection of:
  - **Hardware/software**
  - **Encryption**
  - **Policies & access controls**
- Must address **dial-up, telecommuting, VDI, virtual apps**

**Multimedia Collaboration**

- Combines VoIP, chat, video conferencing, etc.
- Needs **auth, encryption, and logging** for secure use

**Load Balancing**

| Mode | Description |
|---|---|
| **Active/Active** | All nodes used simultaneously; capacity drops under failure |
| **Active/Passive** | Standby system waits to take over; capacity preserved |

Purpose: Optimize **utilization, speed, reliability**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 632-634

# CHAPTER 12

## Secure Communications and Network Attacks

### Study Essentials (cont.)

**Virtual Networks & Tunneling**

- **Virtualized Networks** include:
  - SDNs, VLANs, VPNs, NAT, virtual switches
- **Tunneling**: Encapsulation of one protocol within another, often encrypted
- **VPNs**: Use tunneling + encryption (e.g., **PPTP, L2TP, IPSec, TLS, SSH**)

| Tunnel Type | Traffic Flow |
|---|---|
| **Split** | Local traffic goes to Internet; sensitive traffic to VPN |
| **Full** | All traffic flows through VPN tunnel |

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 632-634

# CHAPTER 12

## Secure Communications and Network Attacks

### Study Essentials (cont.)

**NAT & Third-Party Connectivity**

- **NAT**:
  - Hides internal IP structure
  - Allows many internal clients → 1 public IP
  - Found on firewalls, routers, WAPs, proxies
- **Third-Party Connectivity**:
  - Includes **vendors, cloud, remote workers**
  - Evaluate risks, formalize with **MOU → ISA**

**Circuit vs. Packet Switching**

| Switching | Description |
|---|---|
| **Circuit** | Dedicated path (e.g., phone call) |
| **Packet** | Message split into packets, routed dynamically |

- **Packet switching** uses:
  - **PVC**: Static path
  - **SVC**: Dynamic, per session

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 632-634

# CHAPTER 12

## Secure Communications and Network Attacks

### Study Essentials (cont.)

**Communication Attacks & Defenses**

| Attack | Description | Countermeasure |
|---|---|---|
| **DDoS** | Floods systems | Firewalls, traffic filtering |
| **Eavesdropping** | Sniffing data | **Encryption** |
| **Spoofing** | Falsifying identity | Auth mechanisms |
| **Replay** | Resending valid data | Timestamps, nonces |
| **MitM (AitM)** | Intercepts/changes data | Encryption, validation |
| **ARP/DNS Attacks** | Redirect traffic | Secure protocols, DNSSEC, DHCP snooping |

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 632-634

# CHAPTER 12

## Secure Communications and Network Attacks

CHAPTER 12

**Secure Communications & Network Attacks**

Knowledge Acquired • Skills Developed • Mission Accomplished

✓ COMPLETED

# AGENDA – SESSION 8

## Chapter 13

### Chapter 13 - Managing Identity and Authentication

THE CISSP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

- Domain 5: Identity and Access Management (IAM)
- 5.1 Control physical and logical access to assets
  - 5.1.1 Information
  - 5.1.2 Systems
  - 5.1.3 Devices
  - 5.1.4 Facilities
  - 5.1.5 Applications
  - 5.1.6 Services
- 5.2 Design identification and authentication strategy (e.g., people, devices, and services)
  - 5.2.1 Groups and Roles
  - 5.2.2 Authentication, Authorization and Accounting (AAA) (e.g., multi-factor authentication (MFA), password-less authentication)
  - 5.2.3 Session management
  - 5.2.4 Registration, proofing, and establishment of identity
  - 5.2.5 Federated Identity Management (FIM)
  - 5.2.6 Credential management systems (e.g., Password vault)

# AGENDA – SESSION 8

## Chapter 13

### Chapter 13 - Managing Identity and Authentication

THE CISSP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

- 5.2.7 Single Sign On (SSO)
- 5.2.8 Just-In-Time
- 5.3 Federated identity with a third-party service
  - 5.3.1 On-premise
  - 5.3.2 Cloud
  - 5.3.3 Hybrid
- 5.5 Manage the identity and access provisioning lifecycle
  - 5.5.1 Account access review (e.g., user, system, service)
  - 5.5.2 Provisioning and deprovisioning (e.g., on/off boarding and transfers)
  - 5.5.3 Role definition and transition (e.g., people assigned to new roles)
  - 5.5.5 Service accounts management

# CHAPTER 13

## Managing Identity and Authentication

**The Identity and Access Management (IAM) domain focuses on issues related to granting and revoking privileges to access data or perform actions on systems. A primary focus is on identification, authentication, authorization, and accounting. In this chapter and Chapter 14, "Controlling and Monitoring Access," we discuss all the objectives in the Identity and Access Management domain. Be sure to read and study the materials from both chapters to ensure complete coverage of this domain's essential material.**


Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 641

# CHAPTER 13

## Managing Identity and Authentication

### Controlling Access to Assets

Access control is essential to security, protecting both tangible and intangible assets. Assets include:

- **Information** (data in files, databases, cloud, or paper)
- **Systems** (IT systems providing services, e.g., servers)
- **Devices** (computers, networking gear, mobile devices—both corporate and personal)
- **Facilities** (physical locations secured by physical controls)
- **Applications** (software that provides data access, controlled via permissions)
- **Services** (organizational offerings like printing or network resources, restricted by access controls)
- Effective access control combines multiple security mechanisms to ensure only authorized users access these assets.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 641-643

# CHAPTER 13

## Managing Identity and Authentication

### Controlling Physical and Logical Access

Protecting assets requires both physical and logical security controls:

- **Physical controls** are tangible measures like fences, locks, guards, HVAC, and fire suppression that safeguard facilities, devices, and systems (e.g., server rooms with restricted access).
- **Logical controls** are technical mechanisms such as authentication, authorization, and permissions that restrict access to information, systems, and applications both on-site and in the cloud.
- Together, these controls prevent unauthorized access and protect critical organizational resources.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 644

# CHAPTER 13

## Managing Identity and Authentication

### The CIA Triad and Access Controls

Access control mechanisms protect against three core IT losses known as the **CIA Triad**:

- **Confidentiality**: Ensures only authorized users can access sensitive data or systems.
- **Integrity**: Prevents unauthorized or undetected modification of data and system configurations.
- **Availability**: Guarantees that authorized users can access systems and data when needed.

Effective access control upholds all three principles to maintain security.


Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 644

# CHAPTER 13

## Managing Identity and Authentication

### The AAA Model

The **AAA Model** defines the three core functions of identity and access management:

- **Authentication** – Verifying the identity of users, systems, or services.
- **Authorization** – Granting or denying access to resources based on identity and permissions.
- **Accounting** – Tracking and logging actions for auditing and monitoring purposes.

These three pillars ensure secure, accountable access control across all systems.

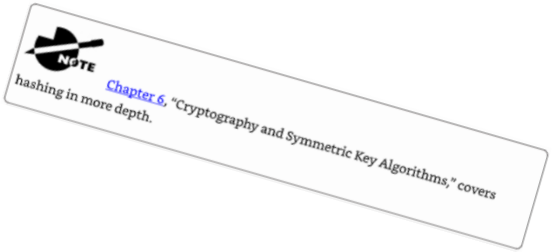
Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 644-645

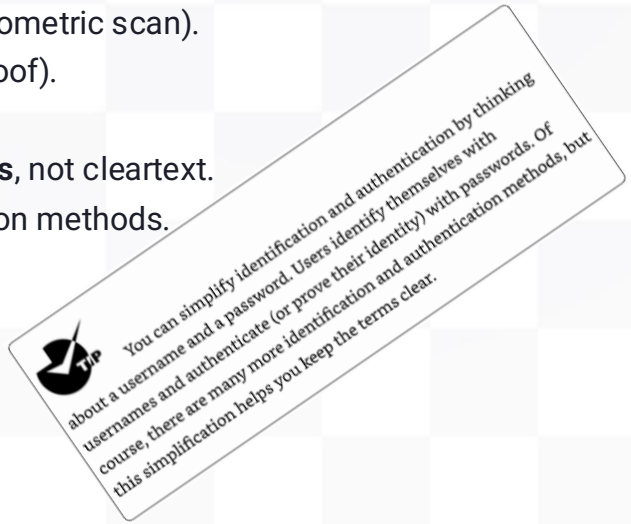
# CHAPTER 13

## Managing Identity and Authentication

### Identification and Authentication Strategy

- **Identification** is claiming an identity (e.g., username, smartcard, biometric input).
- **Authentication** verifies that identity using private information (e.g., password, biometric scan).
- These steps form a **two-part process**: identification (claim) + authentication (proof).
- Unique identities are required for all subjects.
- Authentication must be secure—credentials like passwords are stored as **hashes**, not cleartext.
- Strategies vary by risk: high-security environments require stronger authentication methods.



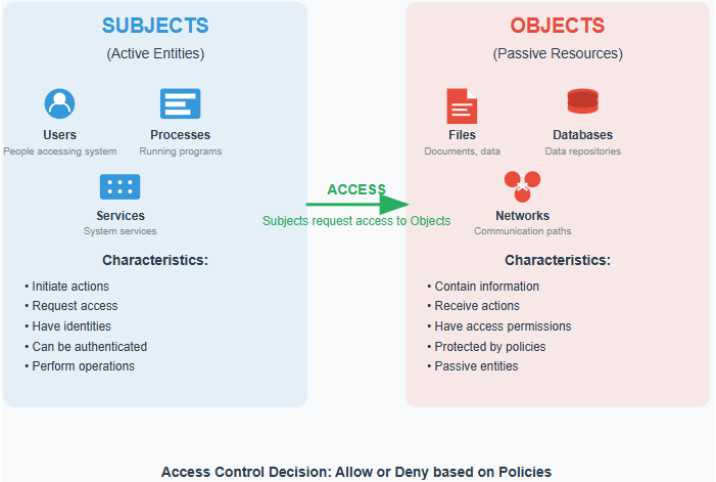

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 645-646

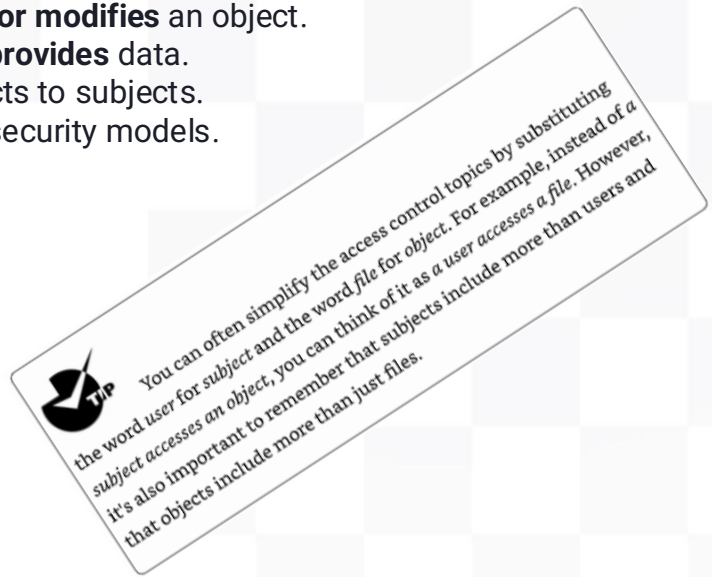
# CHAPTER 13

## Managing Identity and Authentication

### Subjects vs. Objects in Access Control

- **Subject**: An **active** entity (e.g., user, program, process) that **accesses or modifies** an object.
- **Object**: A **passive** entity (e.g., file, database, printer) that **contains or provides** data.
- Access control is about **managing the flow of information** from objects to subjects.
- Understanding this relationship is critical for implementing effective security models.




Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 646

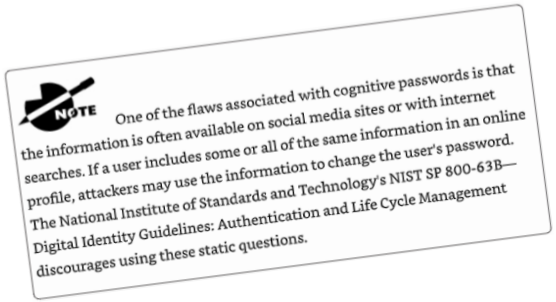
# CHAPTER 13

## Managing Identity and Authentication

### Registration, Proofing, and Establishment of Identity

**Identity Registration and Proofing Methods**

- **In-person proofing** uses physical documents (e.g., passport, ID) to establish identity.
- **Online proofing** often uses **Knowledge-Based Authentication (KBA)**—questions only the individual should know.
- **Cognitive passwords** (e.g., security questions) support self-service password resets.
- **Biometric registration** involves capturing physical traits like fingerprints during onboarding.
- Accurate identity proofing is foundational to trustworthy **authentication**.


NOTE One of the flaws associated with cognitive passwords is that the information is often available on social media sites or with internet searches. If a user includes some or all of the same information in an online profile, attackers may use the information to change the user's password. The National Institute of Standards and Technology's NIST SP 800-63B—Digital Identity Guidelines: Authentication and Life Cycle Management discourages using these static questions.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 647

# CHAPTER 12

## Joke break

**Why did the hacker stay home from the party?**

**Because he couldn’t find a secure “key” to get in!**

# CHAPTER 13

## Managing Identity and Authentication

### Authorization and Accounting

**Authorization and Accounting in Access Control**

- **Authorization**: Grants users permission to access resources based on proven identity. Governed by the **principle of least privilege**.
- **Accounting**: Uses **auditing, logging, and monitoring** to track user actions. Provides **nonrepudiation** and supports **accountability**.
- **Audit logs** record: who did what, when, where, and how—creating an **audit trail**.
- Authorization is **granular** (e.g., read vs. delete), while authentication is **binary** (success/fail).
- Accountability requires identification and authentication, not necessarily authorization.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 648-649

# CHAPTER 13

## Managing Identity and Authentication

### Authentication Factors Overview

**Primary Authentication Factors:**

1. **Something You Know** – Passwords, PINs, passphrases (Type 1)
2. **Something You Have** – Smartcards, tokens, phones (Type 2)
3. **Something You Are** – Biometrics: fingerprints, iris scans (Type 3)

**Additional Factors:**

- **Somewhere You Are** – Location/IP-based validation
- **Somewhere You Aren't** – Suspicious login blocking (e.g., impossible travel)
- **Something You Do** – Gestures, swipes, typing patterns
- **Context-Aware** – Time, location, device, and behavior

**Authentication Types:**

- **Single-Factor** – Uses one type (least secure)
- **Multifactor** – Uses two or more different types (more secure)

**Password Weaknesses:**

- Easily guessed, shared, forgotten, reused
- Susceptible to attacks: sniffing, brute-force, dictionary, spraying
- Can be strengthened with **passphrases**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 649-651

# CHAPTER 13

## Managing Identity and Authentication

### Password Policies & Smartcards

**Password Policy Components**

- **Max Age**: Enforce periodic changes (e.g., 45 days)
- **Complexity**: Use mixed character types (upper/lowercase, numbers, symbols)
- **Length**: Longer is stronger (min 8–12+ characters)
- **Min Age & History**: Prevent quick reuse or cycling of old passwords

**NIST SP 800-63B Guidelines**

- No forced expirations unless compromised
- No mandatory special characters
- Support copy/paste & long passphrases (up to 64 chars)
- Screen against common passwords

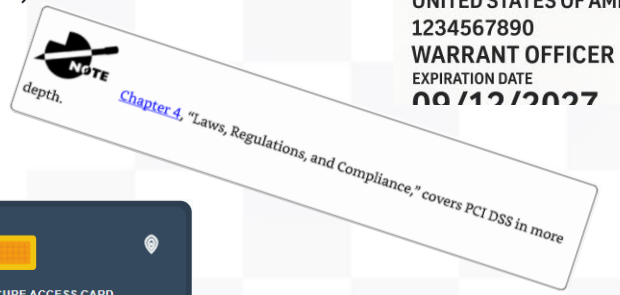
**PCI DSS (v4.0) Requirements**

- Change every 90 days
- Min 12 characters, must include letters + numbers
- Prevent reuse of last 4 passwords

**Something You Have: Smartcards**

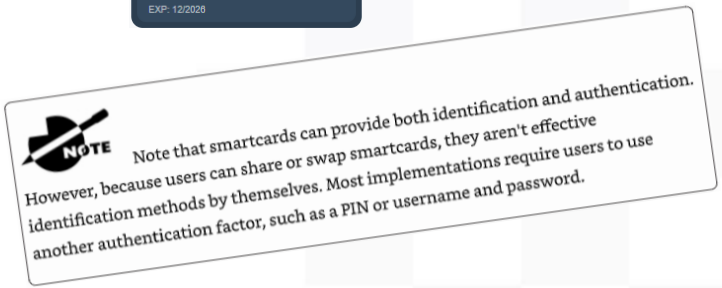
- Tamper-resistant card with embedded chip
- Stores digital certificates & crypto keys
- Used with PIN/password for multifactor authentication












Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 652-654

# CHAPTER 13

## Managing Identity and Authentication

### Authenticators & One-Time Passwords (OTPs)

**Authenticator Overview**

- Devices or apps that generate **One-Time Passwords (OTPs)**
- Used with other factors for **Multifactor Authentication (MFA)**
- Examples: **RSA Token**, **Google Authenticator**

**OTP Types**

- **TOTP (Time-Based)**
  - Syncs with server time
  - New OTP every set interval (e.g., 60 seconds)
  - **Synchronous**

**HOTP (Counter-Based)**

  - Generated on demand via counter
  - Same OTP until used
  - **Asynchronous**

**Limitations**

- Device loss, damage, or battery failure can lock users out


Source: Kevin/Adobe Stock Photos

FIGURE 13.1 Hardware authenticator

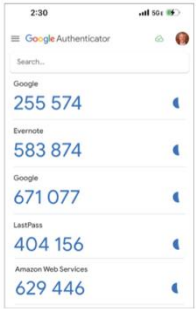



FIGURE 13.2 Software authenticator

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 654-655

# CHAPTER 13

## Managing Identity and Authentication

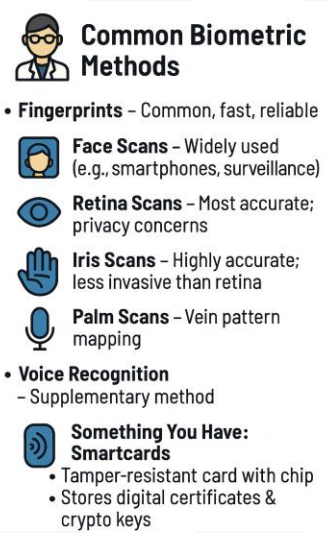
## 🧬 Biometrics – "Something You Are"

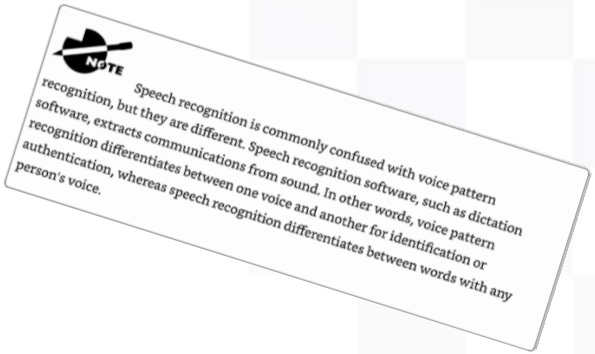
### 🔍 Biometrics Overview

- Type 3 authentication factor: **"Something You Are"**
- Used for **identification** (1:N) or **authentication** (1:1)
- Does **not** provide **authorization** or **accountability**

### 👨🔬 Common Biometric Methods

- **Fingerprints** – Common, fast, reliable
- **Face Scans** – Widely used (e.g., smartphones, surveillance)
- **Retina Scans** – Most accurate; privacy concerns
- **Iris Scans** – Highly accurate; less invasive than retina
- **Palm Scans** – Vein pattern mapping
- **Voice Recognition** – Supplementary method





NOTE

Speech recognition is commonly confused with voice pattern recognition, but they are different. Speech recognition software, such as dictation software, extracts communications from sound. In other words, voice pattern recognition differentiates between one voice and another for identification or authentication, whereas speech recognition differentiates between words with any person's voice.

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 655-657

# CHAPTER 12

## Joke break

**How did the hacker escape the FBI?**

**He ransomware**

# CHAPTER 13

## Managing Identity and Authentication

### 📊 Biometrics – Accuracy, Errors & Performance

#### 🔍 Biometric Accuracy Metrics

- **False Rejection Rate (FRR)** = Type I error
  → Valid user **incorrectly denied** access
- **False Acceptance Rate (FAR)** = Type II error
  → Unauthorized user **incorrectly granted** access
- **Crossover Error Rate (CER/ERR)**
  → Point where **FAR = FRR**
  → **Lower CER = Higher Accuracy**

#### ⚙️ Performance Considerations

- **Sensitivity trade-off:**
  ↑ Sensitivity = ↑ FRR, ↓ FAR (stricter)
  ↓ Sensitivity = ↓ FRR, ↑ FAR (looser)
- **Operational tuning:** Use case dictates priority (e.g., secure vault: prioritize ↓ FAR)

#### 🛠️ Enrollment & Throughput

- **Enrollment** = Initial scan to create reference template
  → Acceptable time: **< 2 minutes**
- **Throughput rate** = Time to scan and authenticate
  → Acceptable time: **~6 seconds or less**
- Factors affecting usability:
  → Changes in voice, face, or signature over time require **re-enrollment**

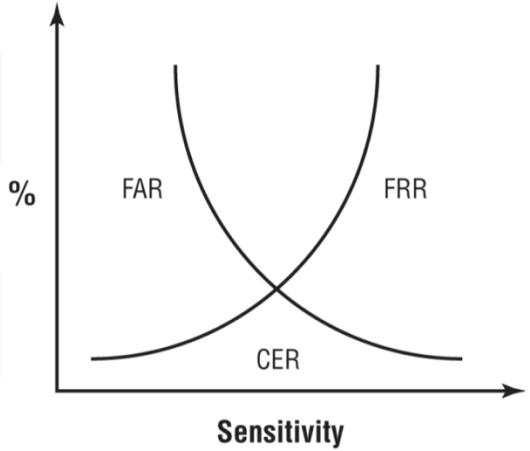



FIGURE 13.3 Graph of FRR and FAR errors indicating the CER point

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 657-658

# CHAPTER 13

## Managing Identity and Authentication

### MFA, Passwordless, Device, and Service Authentication

#### Multifactor Authentication (MFA)

- **2FA = Two different factors**
  - E.g., Smartcard (have) + PIN (know)
- Using **same factor twice** = no real added security
- MFA improves security by requiring **different attack methods**

> **TIP** Multifactor authentication must use multiple types or factors, such as the something you know factor and the something you have factor. In contrast, requiring users to enter a password and a PIN is not multifactor authentication because both methods are from a single authentication factor (something you know).

#### SMS & Passwordless

- **NIST deprecated SMS 2FA** (SP 800-63B)
  - Vulnerable to SIM swap, lock screen access
- **Passwordless Auth**: Uses biometrics, hardware tokens
  - E.g., FIDO2, YubiKey, Face/Fingerprint scan

Source: gguy / Adobe Systems Incorporated

FIGURE 13.4 YubiKey passkey

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 658-662

# CHAPTER 13

## Managing Identity and Authentication

### Service Authentication

**Device Authentication**

- **Device fingerprinting**: Ties user account to device attributes (browser, OS, screen size)
- **802.1X**: Port-based authentication, used in MDM & NAC solutions

**Service Authentication**

- **Service accounts**:
  - Non-interactive
  - Strong, non-expiring passwords
  - Use certs or APIs (e.g., Google, Facebook)
  - **Account reviews** detect issues

**Mutual Authentication**

- **Both client and server authenticate**
  - Prevents rogue endpoints
  - Common with VPN + digital certs

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 658-662

# CHAPTER 13

## Managing Identity and Authentication

### Identity Management Models & SSO

**Identity Management (IdM) Approaches**

- **Centralized Access Control**
  - One entity handles all authorization
  - Easy to manage and scale (e.g., AD), but **single point of failure**
- **Decentralized Access Control**
  - Multiple entities handle authorization
  - Higher overhead, difficult to maintain consistency

**Single Sign-On (SSO)**

- Authenticate once → access many systems
- Reduces user burden & admin load
- **Risk**: Compromise of SSO = broad access
- Commonly supported by **LDAP directories**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 662-664

# CHAPTER 13

## Managing Identity and Authentication

### LDAP, Domains, and PKI Integration

**LDAP in Access Control**
- Protocol for directory services (e.g., AD)
- Stores authentication & authorization data
- Enables SSO and object/resource discovery

**Domains & Trusts**
- **Domain** = boundary with shared security policy
- **Trust** = allows inter-domain access (one-way or two-way)

**LDAP in PKI**
- Used to **query certificate data from CAs**
- Supports certificate validation during secure communications

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 662-664

# CHAPTER 13

## Managing Identity and Authentication

### SSO & Federated Identity Management (FIM)

**Single Sign-On (SSO)**
- Authenticate once → access multiple systems
- Used internally and across cloud apps
- Reduces password fatigue; increases convenience
- **Risk**: If compromised, attacker gains broad access

**Federated Identity Management (FIM)**
- SSO **across organizations**
- User authenticates once → accesses multiple domains via **federated identity**
- Federation = trust-based agreement to share authentication data
- Resources shared **selectively** based on admin policy

**Common Standards**
- **SAML**, **OAuth**, **OIDC** used to implement federation
- Key challenge: agreeing on a **common protocol/language**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 664-665

# CHAPTER 13

## Managing Identity and Authentication

### SSO & Federated Identity Management (FIM)

**Cloud-Based Federation**
- Uses third-party services to match internal login with federated identity
- Example: corporate training portals

**On-Premises Federation**
- Hosted internally; integrates internal networks (e.g., after a merger)
- Offers **maximum control** over identity systems

**Hybrid Federation**
- Combines on-prem and cloud federation (e.g., merger + cloud training access)

**Just-in-Time (JIT) Provisioning**
- Auto-creates user accounts **on first access**
- Eliminates admin overhead
- Often uses **SAML** to exchange identity data

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 664-665

# CHAPTER 13

## Managing Identity and Authentication

### Credential Management Systems & IDaaS

**Credential Management Systems (CMS)**

- Securely store usernames & passwords (e.g., browsers, OS, apps)
- **W3C Credential Management API** (2019):
  - Store credentials post-login
  - Skip sign-in forms
  - Auto-login on future visits

**Federated Identity Integration**

- CMS can support federated SSO (e.g., log in to Zoom with Google)
- Simplifies web SSO using trusted identity providers

**Identity as a Service (IDaaS)**

- Third-party IAM and SSO for cloud apps
- Example:
  - **Google**: One login for Gmail, Drive, YouTube, etc.
  - **Microsoft 365**: One login for desktop + cloud access via OneDrive
- Enterprise IDaaS integrations (e.g., with **Delinea** + **Active Directory**)

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 665-666

# CHAPTER 13

## Managing Identity and Authentication

### Credential Manager Apps & Password Vaults

**Credential Manager (Windows)**

- Stores encrypted credentials for apps & websites
- Retrieves login data automatically for future access

**Third-Party Password Vaults**

- Tools like **KeePass**, **LastPass**, **1Password**:
  - Store credentials in **encrypted** database
  - Unlock with strong **master password**
  - Can auto-fill credentials in login forms
  - **Best practice**: Use MFA and strong, unique master passwords

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 665-666

# CHAPTER 13

## Managing Identity and Authentication

### Scripted Access & SSO Simulation

**Scripted Access**

- Uses logon scripts to automate credential submission
- Simulates **SSO** in environments without native SSO support
- **Risk**: Scripts may store credentials in **cleartext**
- **Mitigation**: Secure script storage and limit access

**Use Case**

- Legacy systems lacking true SSO
- Batch files or shell scripts automate logins

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 666-667

# CHAPTER 13

## Managing Identity and Authentication

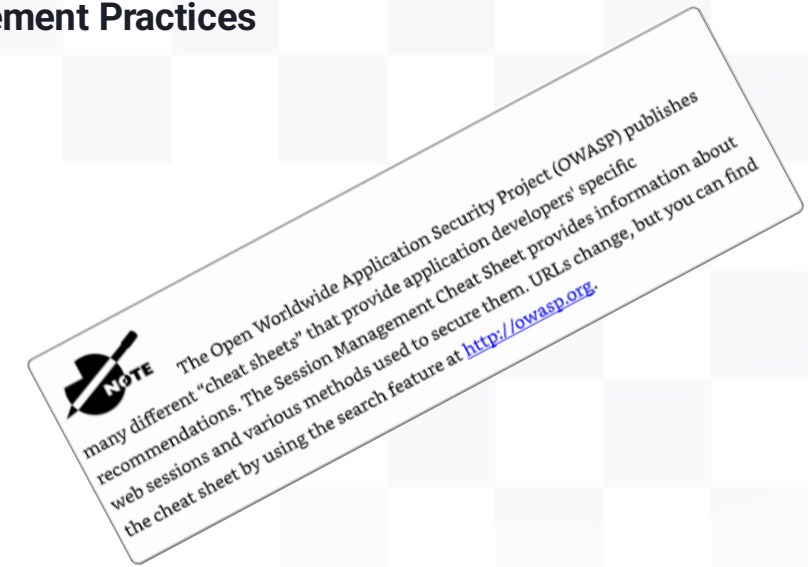
### Session Management Practices

**Desktop Session Management**

- Use screen savers with **password protection**
- Enforce inactivity timeouts (10–20 mins typical)

**Web Session Management**

- Sessions use **unique identifiers**
- Encrypted with **TLS**
- Auto-logout on inactivity:
  - **High-value apps**: 2–5 min timeout
  - **Low-value apps**: 15–30 min timeout
- User prompts for extending session (e.g., banking apps)




Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 666-667

# CHAPTER 13

## Managing Identity and Authentication

### Provisioning & Onboarding

**Identity and Access Provisioning Life Cycle**
- **Phases**: Creation → Management → Review/Audit → Deletion
- Supports **identification, authentication, authorization, and accountability**

**Provisioning**
- Follows formal, policy-based procedures
- Requires **unique identifier** (e.g., username)
- Includes:
  - Account creation
  - Role/group assignment
  - Issuing hardware (laptops, tokens, smartcards)

**Onboarding**
- Acceptable Use Policy (AUP) acknowledgement
- Security awareness (e.g., phishing, 2FA)
- Access to systems, help desk, shared drives
- Password manager and mobile policy review


Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 668-670

# CHAPTER 13

## Managing Identity and Authentication

### Deprovisioning & Offboarding

**Deprovisioning**

- Triggered by **termination, layoff, or transfer**
- Methods:
  - **Account revocation (deletion)** – removes access/data
  - **Account disablement** – retains access for data retrieval

**Best Practices**

- Collect issued hardware
- Recover access to encrypted data
- Monitor logs and close gaps in access
- Disable accounts **immediately** to prevent sabotage

**Offboarding**

- Stop benefits (e.g., healthcare, payroll access)
- Example failure: Univ. of Wisconsin overpaid ~$3M in insurance due to poor offboarding

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 668-670

# CHAPTER 13

## Managing Identity and Authentication

### Role Definition & Transitions

**Why Define Roles?**

- Organizational changes → new roles or reassignments
- Each new role must be **clearly defined** with specific access needs

**Example:**

- New e-commerce project → Create:
  - Web Developer role (application-level access)
  - Linux Admin role (server-level access)
- Assign privileges via **group membership**

**Best Practice:**

- Use **Role-Based Access Control (RBAC)** for scalability and consistency

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 670-671

# CHAPTER 13

## Managing Identity and Authentication

### Account Maintenance & Access Review

**Account Maintenance**

- Required throughout the account's lifecycle
- Common updates:
  - **Modify privileges** based on job changes
  - **Disable inactive accounts** via scripts
  - **Remove outdated group memberships**

**Access Reviews**

- Periodic checks to verify:
  - Principle of **Least Privilege** is enforced
  - Compliance with security policy
  - No misuse of **system/service accounts**

**Key Threats**

- **Excessive Privileges**: More than job requires
- **Privilege Creep**: Retained old access after job transitions

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 670-671

# CHAPTER 13

## Managing Identity and Authentication

### Summary

**Identity and Access Management (IAM) Overview**
- **IAM** governs how subjects (users, devices, services) **gain access** to assets (data, systems, facilities)
- Relies on **physical** and **logical access controls**

**Core IAM Functions**
- **Identification** → Claiming an identity (e.g., username)
- **Authentication** → Verifying identity using:
  - **Something you know** (password)
  - **Something you have** (token)
  - **Something you are** (biometrics)
- **Multifactor Authentication (MFA)** = 2+ **different** factors (Stronger than any one factor alone)

**Access Efficiency Tools**
- **Single Sign-On (SSO):** One login → many systems
- **Federated Identity (FID):** Link identities across organizations for shared SSO

**Provisioning Life Cycle**
- **Provisioning**: Create accounts, assign access, issue hardware
- **Onboarding**: Train, inform, and configure users securely
- **Deprovisioning**: Disable/delete accounts when users leave
- **Offboarding**: Recover issued hardware, terminate benefits

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 671-672

# CHAPTER 13

## Managing Identity and Authentication

### Study Essentials (1 of 7)

### Identity & Access Management (IAM) Overview

- IAM protects assets: people, systems, info, apps
- Physical vs. Logical controls
- Physical: Guards, locks, cameras
- Logical: Authentication, Authorization, Permissions

### Subjects vs. Objects

- Subjects = Active (users, processes)
- Objects = Passive (files, systems)
- Example: User (subject) accesses file (object)

🧠 **Mnemonic Tip:**
**SAD-O = Subject Acts, Data/Object is acted on**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 672-674

# CHAPTER 13

## Managing Identity and Authentication

### Study Essentials (2 of7 )

### AAA of Access Control

- Identification: claim identity (e.g., username)
- Authentication: prove identity (e.g., password, token)
- MFA: combines factors—something you know, have, or are

### Identification vs. Authentication

- **Identification**: Claim identity (e.g., username)
- **Authentication**: Prove identity (e.g., password, biometrics)

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 672-674

# CHAPTER 13

## Managing Identity and Authentication

### Study Essentials (3 of7 )

### Identity Establishment & Proofing

- Establish identity using documents
- HR registers and creates accounts
- **Proofing**: Security Qs, biometrics, KBA

### Authorization vs. Accounting

- **Authorization**: What actions are allowed
- **Accounting**: Log and track user activity

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 672-674

# CHAPTER 13

## Managing Identity and Authentication

### Study Essentials (4 of7 )

### Authentication Factors

- **Something you know**: Password, PIN
- **Something you have**: Token, card
- **Something you are**: Biometric
- MFA = Multiple **different** factors

### Authentication Concepts

- Passwords = weakest factor
- Use complexity policies
- Biometric accuracy = **CER**
- Smartcards store credentials securely

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 672-674

# CHAPTER 13

## Managing Identity and Authentication

### Study Essentials (5 of7 )

### Single Sign-On (SSO)

- Authenticate once, access many systems
- Common for internal networks, cloud services

### Federated Identity & JIT Provisioning

- Federation: Share identity across orgs
- JIT: Account created at first login

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 672-674

# CHAPTER 13

## Managing Identity and Authentication

### Study Essentials (6 of7 )

### Credential & Session Management

- Credential systems auto-fill logins
- Sessions timeout after inactivity

### Identity & Access Lifecycle

- Provisioning: Create accounts, assign access
- Onboarding: Employee setup
- Deprovisioning: Remove access
- Offboarding: Collect hardware

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 672-674

# CHAPTER 13

## Managing Identity and Authentication

### Study Essentials (7 of 7)

### Role & Group Management

- Define roles with appropriate privileges
- Use groups to simplify access control
- Update access during job transitions

### Account Access Reviews

- Periodic audits for:
  - Excessive privileges
  - Inactive accounts
- Supports **least privilege**

Source: CISSP Official Study Guide, 10th Ed., Chapple & Stewart, p. 672-674

# CHAPTER 13

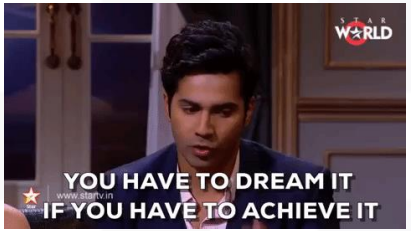
## Managing Identity and Authentication


# YAY! YOU MADE IT!

That was A LOT of information

What's next????
Study, Study, study, take breaks as needed, study some more, game, relax, hike, bike, did you study?


# YAY! YOU MADE IT!




## That was A LOT of information.

## Now what?

- Keep up in the book. We just went through Chapters 12 and 13.
- Be sure to review and focus on the “Study Essentials” sections for each chapter.
- If you’re ambitious, do the “Written Lab” section for each chapter too.
- When you’re ready, take a stab at the “Review Questions” for each chapter.
- If you haven’t already, feel free to check out the CISSP cheat sheet on Discord.
- Jot down your questions, post them in Discord, and/or ask them in the next Live Mentor Session (June 18th)


That’s it for now, **CONGRATS** for making it through this. ☺

**See you Wednesday night.**