COMPLETE CYBERSECURITY NOTES

TABLE OF CONTENTS

---

1. INTRODUCTION TO CYBERSECURITY

Definition: Cyber security is the practice of protecting systems, networks, programs, and data from digital attacks, damage, or unauthorized access.

Key Objectives:

- Protect confidentiality, integrity, and availability of information
- Ensure business continuity
- Minimize risk and damage from security breaches

Types of Security:

- **Network Security** - Protecting network infrastructure
- **Application Security** - Securing software applications
- **Information Security** - Protecting data integrity and privacy
- **Operational Security** - Processes and decisions for handling data
- **Cloud Security** - Securing cloud-based systems
- **Endpoint Security** - Protecting end-user devices

---

2. THE CIA TRIAD (CORE PRINCIPLES)

A. Confidentiality

Definition: Ensuring data is accessible only to authorized parties

Threats to Confidentiality:

- Unauthorized access
- Data breaches
- Eavesdropping
- Shoulder surfing
- Man-in-the-middle attacks

Protection Mechanisms:

- Encryption (AES, RSA)
- Access Control Lists (ACLs)
- Steganography (hiding data within other data)
- Multi-factor authentication
- Biometric verification

B. Integrity

Definition: Ensuring data is trustworthy and has not been altered by unauthorized parties

Threats to Integrity:

- Data tampering
- Malware injection
- Man-in-the-middle attacks
- Session hijacking

Protection Mechanisms:

- Hashing (SHA-256, MD5)
- Digital signatures
- Checksums and parity bits
- Version control systems
- Audit trails

C. Availability

Definition: Ensuring systems and data are accessible when needed by authorized users

Threats to Availability:

- Denial of Service (DoS) attacks
- Distributed Denial of Service (DDoS)
- Power outages
- Hardware failure
- Natural disasters
- Ransomware

Protection Mechanisms:

- Redundant systems
- Load balancers
- Backup and disaster recovery
- RAID configurations
- UPS (Uninterruptible Power Supply)
- Failover clusters

The DAD Triad (Opposites of CIA)

- **Disclosure** - Unauthorized release of information
- **Alteration** - Unauthorized modification of data
- **Denial** - Prevention of authorized access

---

3. AUTHENTICATION & AUTHORIZATION

Authentication (Who you are)

Definition: The process of verifying the identity of a user, device, or system

Three Authentication Factors:

Factor	Description	Examples
Something you KNOW	Knowledge-based	Password, PIN, Security answers
Something you HAVE	Possession-based	Smart card, Token, Phone, Key fob
Something you ARE	Biometric	Fingerprint, Retina scan, Voice recognition

Multi-Factor Authentication (MFA): Using two or more different factors

Single Sign-On (SSO): One authentication credential to access multiple systems

Authorization (What you can do)

Definition: Determining what resources an authenticated user can access

Authorization Methods:

- Access Control Lists (ACLs)
- Role-based permissions
- Attribute-based access control

Accounting (What you did)

Definition: Tracking and logging user activities for audit purposes

Information Logged:

- Timestamps
- User IDs
- Actions performed
- Resources accessed
- IP addresses

AAA Framework

- **Authentication** = Prove identity
- **Authorization** = Grant permissions
- **Accounting** = Log activities

---

4. ACCESS CONTROL MODELS

A. Access Control Matrix (ACM)

Definition: A theoretical table where rows represent Subjects (users) and columns represent Objects (files/folders)

Structure:

```
text
          | File A | File B | Printer |
----------|--------|--------|---------|
User 1    |  R,W   |   R    |   -     |
User 2    |   R    |  R,W   |  Print  |
Admin     |  R,W,X |  R,W,X | Print   |

R = Read, W = Write, X = Execute
```

B. Discretionary Access Control (DAC)

Definition: The owner of the data decides who has access

Characteristics:

- Owner-controlled
- Flexible and intuitive
- Common in personal systems

Examples:

- Windows file permissions
- Linux chmod command
- Google Drive sharing

C. Mandatory Access Control (MAC)

Definition: The system enforces a global policy based on classifications

Security Levels:

- Top Secret
- Secret
- Confidential
- Unclassified

Characteristics:

- System-enforced
- Used in military and government
- No user override

Examples:

- SELinux
- MLS (Multi-Level Security)

D. Role-Based Access Control (RBAC)

Definition: Access is based on the user's job "Role" rather than identity

Common Roles:

- Administrator - Full access
- Manager - Department access
- Employee - Basic access
- Guest - Limited access

Benefits:

- Easier management
- Scales well
- Follows organizational structure

E. Rule-Based Access Control

Definition: Access is determined by global rules or policies

Examples:

- Firewall rules
- Time-based access
- Location-based restrictions

---

5. CRYPTOGRAPHY

A. Symmetric Encryption

Definition: The SAME key is used to encrypt and decrypt data

How it works:

```
text
Plaintext + Key → Encryption → Ciphertext
Ciphertext + Same Key → Decryption → Plaintext
```

Algorithms:

Algorithm	Key Size	Strength
AES	128,192,256 bits	Very Strong
DES	56 bits	Weak (Deprecated)
3DES	168 bits	Moderate
ChaCha20	256 bits	Strong

Advantages:

- Fast and efficient
- Suitable for large data volumes

Disadvantages:

- Key distribution problem
- Need secure channel for key exchange

B. Asymmetric Encryption (Public Key)

Definition: Uses a KEY PAIR (Public key to encrypt, Private Key to decrypt)

How it works:

```
text
Plaintext + Public Key → Encryption → Ciphertext
Ciphertext + Private Key → Decryption → Plaintext
```

Algorithms:

Algorithm	Key Size	Use Case
RSA	2048-4096 bits	Digital signatures, Key exchange
ECC	256-521 bits	Mobile devices, IoT
Diffie-Hellman	2048+ bits	Secure key exchange

Advantages:

- No key distribution problem
- Enables digital signatures

Disadvantages:

- Slower than symmetric
- Computationally intensive

C. Hashing

Definition: A one-way function that turns data into a fixed-length "digest"

Properties:

- Deterministic (same input = same output)
- Irreversible (cannot recover original data)
- Collision-resistant (different inputs produce different outputs)

Algorithms:

Algorithm	Output Size	Status
MD5	128 bits	Broken (Not secure)
SHA-1	160 bits	Deprecated
SHA-256	256 bits	Secure
SHA-512	512 bits	Very Secure

Use Cases:

- Password storage
- File integrity verification
- Digital signatures
- Block chain

D. Digital Signatures

Definition: Combines hashing with asymmetric encryption to verify authenticity

Process:

1. Hash the document
2. Encrypt hash with sender's Private Key
3. Send document + encrypted hash
4. Receiver decrypts hash with sender's Public Key

5. Receiver hashes the document
6. Compare hashes to verify

E. SSL/TLS (Secure Sockets Layer / Transport Layer Security)

Definition: Protocols for secure communication over networks

How HTTPS works:

1. Client requests secure connection
2. Server sends SSL certificate
3. Client verifies certificate
4. Session key exchange
5. Encrypted communication begins

---

6. NETWORK SECURITY

A. Firewalls

Definition: A barrier between trusted internal network and untrusted external networks

Types of Firewalls:

Type	Description	Pros	Cons
Packet Filtering	Examines packet headers	Fast, Simple	Limited inspection
Stateful Inspection	Tracks connection state	More secure	Slower
Application Gateway	Deep packet inspection	Very secure	Resource intensive
Next-Gen Firewall	Integrated IDS/IPS	Comprehensive	Expensive

B. Intrusion Detection & Prevention

IDS (Intrusion Detection System)

- **Role:** Passive monitoring and alerting
- **Action:** Logs and alerts

- **Position:** Off to the side (mirrored traffic)

IPS (Intrusion Prevention System)

- **Role:** Active blocking of threats
- **Action:** Blocks in real-time
- **Position:** Inline (traffic passes through)

Detection Methods:

- **Signature-based:** Matches known attack patterns
- **Anomaly-based:** Detects deviation from normal behaviour
- **Policy-based:** Enforces security policies

C. VPN (Virtual Private Network)

Definition: Encrypts traffic between your device and a secure server

Types of VPN:

- **Remote Access VPN** - Individual users connecting to corporate network
- **Site-to-Site VPN** - Connecting entire networks
- **SSL VPN** - Through web browser
- **IPsec VPN** - Network layer encryption

D. Network Segmentation

Definition: Dividing a network into smaller, isolated segments

Benefits:

- Limits breach spread
- Improves performance
- Simplifies compliance

Techniques:

- VLANs (Virtual Local Area Networks)
- Subnetting
- DMZ (Demilitarized Zone)

E. DMZ (Demilitarized Zone)

Definition: A neutral zone between internal and external networks

Purpose: Host public-facing services (web servers, email) safely

Typical Setup:

```
text
Internet → Firewall → DMZ (Web Server, Email) → Firewall → Internal Network
```

---

7. MALWARE & ATTACK VECTORS

A. Types of Malware

Malware	Description	Symptoms
Virus	Attaches to clean files, spreads when executed	File corruption, Slow performance
Worm	Self-replicates across networks	Network congestion, Bandwidth issues
Trojan	Disguised as legitimate software	Backdoors, Data theft
Ransomware	Encrypts files, demands payment	Files inaccessible, Ransom note
Spyware	Secretly monitors user activity	Slow system, Unusual network traffic
Adware	Displays unwanted advertisements	Pop-ups, Browser redirects
Rootkit	Hides deep in operating system	System instability, Hidden processes
Keylogger	Records keystrokes	Password theft, Credential compromise
Botnet	Network of infected devices	DDoS attacks, Spam distribution

B. Attack Vectors

1. Phishing / Social Engineering

- Manipulating humans into revealing secrets
- **Types:** Email phishing, Spear phishing, Smishing (SMS), Vishing (Voice)

2. Man-in-the-Middle (MITM)

- Intercepting communication between two parties
- **Examples:** Evil twin Wi-Fi, Session hijacking, SSL stripping

3. Denial of Service (DoS/DDoS)

- Overwhelming systems with traffic
- **Types:** Volume-based, Protocol-based, Application layer

4. Buffer Overflow

- Writing more data to memory than allocated
- **Result:** Crash or arbitrary code execution

5. Password Attacks

- **Brute Force:** Trying all combinations
- **Dictionary:** Using common words
- **Credential Stuffing:** Using stolen credentials

6. Zero-Day Attack

- Exploiting unknown vulnerabilities before they are patched

C. Attack Lifecycle (Cyber Kill Chain)

Phase	Description
1. Reconnaissance	Gathering information about target
2. Weaponization	Creating exploit and payload
3. Delivery	Sending payload to target
4. Exploitation	Triggering the exploit
5. Installation	Installing malware

Phase	Description
6. Command & Control	Establishing remote control
7. Actions on Objective	Achieving attacker's goal

---

8. WEB APPLICATION SECURITY

A. OWASP Top 10 (Most Critical Risks)

1. **Broken Access Control** - Users can access unauthorized resources
2. **Cryptographic Failures** - Weak or missing encryption
3. **Injection (SQL, NoSQL, OS Command)** - Untrusted data sent to interpreter
4. **Insecure Design** - Security flaws at design phase
5. **Security Misconfiguration** - Default configurations, verbose errors
6. **Vulnerable Components** - Outdated libraries and frameworks
7. **Identification Failures** - Weak session management
8. **Software Integrity Failures** - Untrusted software updates
9. **Monitoring Failures** - Insufficient logging and monitoring
10. **SSRF (Server-Side Request Forgery)** - Server makes unauthorized requests

B. Common Web Attacks

SQL Injection (SQLi)

```sql
-- Vulnerable query
SELECT * FROM users WHERE username = '$username'

-- Attack input
' OR '1'='1' --

-- Resulting query
SELECT * FROM users WHERE username = '' OR '1'='1' --'
```

Cross-Site Scripting (XSS)

```javascript
// Vulnerable code
<div>Search results for: <?php echo $_GET['search']; ?></div>
```

```
// Attack input
<script>alert('Hacked');</script>

// Types: Stored, Reflected, DOM-based
```

Cross-Site Request Forgery (CSRF)

- Tricking user into executing unwanted actions
- Attack uses user's existing authentication

C. Secure Coding Practices

1. **Input Validation** - Validate all user input
2. **Output Encoding** - Encode output to prevent injection
3. **Parameterized Queries** - Use prepared statements
4. **Content Security Policy (CSP)** - Prevent XSS
5. **Secure Headers** - HSTS, X-Frame-Options, X-XSS-Protection

---

9. SECURITY BEST PRACTICES

A. Password Security

Strong Password Requirements:

- Minimum 12 characters
- Mix of uppercase, lowercase, numbers, symbols
- No dictionary words
- No personal information
- Unique for each account

Password Management:

- Use password managers (Bitwarden, LastPass, 1Password)
- Enable Multi-Factor Authentication (MFA)
- Regular password changes (for sensitive accounts)

B. Data Protection

Data Classification Levels:

- **Public** - No protection needed
- **Internal** - For internal use only
- **Confidential** - Sensitive business data
- **Restricted** - Highly sensitive (PII, PHI)

Data Protection Methods:

- Encryption at rest (stored data)
- Encryption in transit (network data)
- Data masking and anonymization
- Data loss prevention (DLP)

C. Backup Strategy

3-2-1 Backup Rule:

- **3** copies of data
- **2** different media types
- **1** offsite copy

Backup Types:

- Full backup - Complete copy
- Incremental - Changes since last backup
- Differential - Changes since last full backup

D. Patch Management

Process:

1. Inventory systems
2. Monitor for patches
3. Test patches
4. Deploy patches
5. Verify deployment

E. Security Awareness Training

Topics to Cover:

- Phishing identification
- Password hygiene
- Physical security
- Incident reporting

- Remote work security

---

10. INCIDENT RESPONSE

A. Incident Response Lifecycle (NIST)

Phase	Activities
1. Preparation	Train teams, Create playbooks, Install tools
2. Detection & Analysis	Monitor alerts, Investigate, Determine scope
3. Containment	Isolate systems, Block traffic, Disable accounts
4. Eradication	Remove malware, Patch vulnerabilities
5. Recovery	Restore from backup, Monitor for recurrence
6. Lessons Learned	Document, Improve processes, Update policies

B. Incident Response Team Roles

- **Incident Commander** - Overall coordination
- **Technical Lead** - Technical investigation
- **Communications Lead** - Internal/external communication
- **Legal Counsel** - Legal and compliance
- **Forensics Analyst** - Evidence collection

C. Evidence Collection

Order of Volatility (collect first):

1. CPU registers, cache
2. Routing tables, ARP cache
3. Process tables, kernel statistics
4. Memory (RAM)
5. Temporary file systems
6. Disk storage

7. Remote logging data
8. Physical configuration

Chain of Custody:

- Document every person who handled evidence
- Track timestamps and locations
- Maintain tamper-proof seals

---

11. LEGAL & ETHICAL CONSIDERATIONS

A. Major Regulations

Regulation	Region	Focus
GDPR	European Union	Data privacy, User consent
HIPAA	USA	Healthcare data protection
PCI DSS	Global	Payment card security
SOX	USA	Financial reporting controls
CCPA	California	Consumer privacy rights
FISMA	USA	Federal information security

B. Cybercrime Laws

- **Computer Fraud and Abuse Act (CFAA)** - USA computer crime law
- **Cybercrime Prevention Act** - Various countries
- **Data Protection Act** - Data handling regulations

C. Ethics in Cyber Security

Ethical Hacking Principles:

- Obtain proper authorization

- Respect privacy
- Report findings responsibly
- Do no harm
- Maintain confidentiality

Certified Ethical Hacker (CEH) Code of Ethics:

1. Protect the public
2. Act with integrity
3. Maintain competence
4. Respect confidentiality
5. Avoid conflicts of interest

---

12. EXAM CHEAT SHEET

Quick Reference Formulas & Concepts

```
text
CIA Triad = Confidentiality + Integrity + Availability
DAD Triad = Disclosure + Alteration + Denial
AAA Framework = Authentication + Authorization + Accounting
```

Access Control Comparison

Model	Control	Owner	Example
DAC	Discretionary	Data Owner	Windows files
MAC	Mandatory	System	SELinux
RBAC	Role-based	Administrator	Corporate roles

Encryption Comparison

Type	Key Type	Speed	Use
Symmetric	Single key	Fast	Large data

Type	Key Type	Speed	Use
Asymmetric	Key pair	Slow	Key exchange

Attack Types Quick Reference

Attack	Target	Mitigation
SQLi	Database	Parameterized queries
XSS	Users	Input validation, CSP
DoS/DDoS	Availability	Firewalls, Rate limiting
MITM	Communication	TLS/SSL, VPN
Phishing	Humans	Training, MFA

Port Numbers to Remember

Port	Protocol	Service
20,21	FTP	File Transfer
22	SSH	Secure Shell
23	Telnet	Remote Access (Insecure)
25	SMTP	Email
53	DNS	Domain Name System
80	HTTP	Web (Insecure)
110	POP3	Email
143	IMAP	Email
443	HTTPS	Web (Secure)

Port	Protocol	Service
3389	RDP	Remote Desktop

Security Terms Glossary

Term	Definition
Asset	Anything valuable to an organization
Threat	Potential danger to an asset
Vulnerability	Weakness that can be exploited
Risk	Likelihood × Impact of a threat
Exploit	Code that takes advantage of a vulnerability
Payload	Malicious action performed by exploit
Zero-day	Unknown vulnerability
PII	Personally Identifiable Information
PHI	Protected Health Information
SOC	Security Operations Center
SIEM	Security Information Event Management

Risk Calculation Formula

```
text
Risk = Threat × Vulnerability × Impact

Or more simply:
Risk = Probability × Impact

Risk Level = High / Medium / Low
```

Common Security Tools

Tool Type	Examples
Antivirus	Norton, McAfee, Windows Defender
Firewall	pfSense, Windows Firewall, iptables
IDS/IPS	Snort, Suricata, Zeek
SIEM	Splunk, ELK Stack, QRadar
Penetration Testing	Metasploit, Burp Suite, Nmap
Vulnerability Scanner	Nessus, OpenVAS, Qualys

END OF NOTES

These notes cover the essential topics for cybersecurity fundamentals. For advanced topics, refer to specialized resources.