INFORMATION SECURITY

Suhendro Y.Irianto

23 MAY 2026

Information security

Safeguarding Data and Digital Assets in a Connected World

Definition of Information Security

- Information security refers to practices that protect data from unauthorized access, misuse, alteration, or destruction.
- Example: Protecting student records from unauthorized access.

The CIA Triad

- Confidentiality: Limit access to authorized users.
- Example: Password-protected documents.

- Integrity: Ensure accuracy of data.
- Example: Tamper protection on academic records.

- Availability: Data accessible when needed.
- Example: Servers running 24/7.

The CIA Triad

A model that describes the fundamental goals of information security.

CONFIDENTIALITY | INTEGRITY | AVAILABILITY = INFORMATION SECURITY

Core Security Principles

- Authentication: Verifying identity.
- Example: Logging in with a password.

- Authorization: Determining access rights.
- Example: Admins can edit data; students cannot.

- Accountability: Tracking user actions.
- Example: System activity logs.

Common Threats

- Malware, phishing, DDoS, insider attacks, password attacks.
- Example: Fake bank emails that trick users.

DDoS

DISTRIBUTED DENIAL OF SERVICE

A DDoS attack aims to make a target system, server, or network resource **unavailable** by **overwhelming** it with massive amounts of traffic from multiple sources.

1. ATTACKERS

The attacker uses control servers to command a botnet of compromised devices.

2. BOTNET

The botnet consists of many infected devices (zombies) controlled by the attacker. These devices send traffic to the target.

3. VICTIM

The target server or network is overwhelmed with traffic and becomes slow or completely unavailable.

ATTACKER

COMPROMISED DEVICES (BOTNET)

TARGET SERVER (VICTIM)

HOW IT WORKS

Attacker creates or controls a botnet.

Malware infects many devices.

Botnet sends massive amounts of traffic.

Target is overwhelmed and becomes unavailable.

IMPACT

- Service downtime
- Financial loss
- Reputation damage
- Users cannot access the service

COMMON TYPES

- Serumeric Attacks (e.g., UDP Flood, ICMP Flood)
- Protocol Attacks (e.g., SYN Flood, Smurf)
- Application Layer Attacks (e.g., HTTP Flood)

DDoS attacks can be **mitigated** using **firewalls**, **rate limiting**, **traffic filtering**, **CDNs**, and dedicated **DDoS protection services**.

DDoS

DISTRIBUTED DENIAL OF SERVICE

A DDoS attack is an attempt to make an online service unavailable by overwhelming it with a flood of internet traffic from multiple sources.

HOW A DDOS ATTACK WORKS

1. ATTACKER

The attacker uses control servers to command a botnet of compromised devices.

2. BOTNET

The botnet consists of many infected devices (zombies) controlled by the attacker. These devices send traffic to the target.

3. VICTIM

The target server or network is overwhelmed with traffic and becomes slow or completely unavailable.

COMMON TYPES OF DDOS ATTACKS

VOLUME-BASED ATTACKS

Send large volumes of traffic to consume bandwidth.

- UDP Flood
- ICMP Flood
- DNS Amplification

PROTOCOL ATTACKS

Exploit weaknesses in network protocols and infrastructure.

- SYN Flood
- Ping of Death
- Smurf Attack

APPLICATION LAYER ATTACKS

Target web applications and services at Layer 7 (HTTP/HTTPS).

- HTTP Flood
- Slowloris
- DNS Query Flood

MULTI-VECTOR ATTACKS

Combine multiple attack vectors to maximize impact.

- Blend of volume, protocol, and application attacks

IMPACT OF DDOS ATTACKS

SERVICE DOWNTIME
Websites, apps, or services become slow or completely unavailable.

FINANCIAL LOSS
Revenue loss, recovery costs, and potential legal penalties.

REPUTATION DAMAGE
Loss of customer trust and damage to brand reputation.

OPERATIONAL DISRUPTION
Affects business operations and productivity.

HOW TO MITIGATE DDOS ATTACKS

FIREWALLS & WAF
Filter and block malicious traffic.

RATE LIMITING
Limit requests per IP or per user.

TRAFFIC FILTERING
Use blacklist, whitelist, and anomaly detection.

CDN
Distribute traffic across multiple servers.

DDOS PROTECTION SERVICES
Use cloud-based DDoS protection (e.g., Cloudflare, AWS Shield, Azure DDoS).

BEST PRACTICES

- Keep systems, software, and patches up to date.
- Monitor network traffic and set up alerts.
- Have an incident response and DDoS mitigation plan.
- Work with your ISP and DDoS protection providers.
- Regularly test and review your security posture.

KEY TAKEAWAY

DDoS attacks can cripple online services, but with proper preparation, monitoring, and protection, you can minimize their impact and keep your services available.

DDoS attacks are increasing in frequency and size.
Proactive defense is the key to resilience.

Stay prepared. Stay protected.

Real Cyber Attack Scenarios

- Ransomware in hospitals, e-commerce data breaches, government websites attacked.
- Example: WannaCry ransomware attack in 2017.

System Vulnerabilities

- Outdated software, weak passwords, misconfigurations, human error.
- Example: Unpatched computers targeted by malware.

Risk Management

- Identify risks, analyze impact, apply mitigation strategies.
- Example: Using antivirus to reduce malware risk.

Security Controls

- Administrative controls: Policies.
- Example: Strong password policy.

- Technical controls: Firewalls, encryption.
- Example: Firewall blocking suspicious IPs.

- Physical controls: Locks, CCTV.
- Example: Locked server room.

Security Technologies

- Firewalls, IDS/IPS, MFA, encryption, VPN.
- Example: MFA to secure Gmail accounts.

Password & Identity Management

- Use strong passwords, avoid reuse, use password managers, enable MFA.
- Example: 'F0rum@2025!' is stronger than '123456'.

Data Protection Strategies

- Encryption, masking, access control, backups.
- Example: Encrypting student grades stored in the cloud.

Security Policies

- Rules on passwords, data classification, device manageme incident response.
- Example: Employees must change passwords every 90 days.

Human Factor in Security

- Most security breaches involve human error.
- Example: Opening malicious email attachments.

Incident Response Steps

- Identify, contain, eradicate, recover, learn.
- Example: Isolating infected computers to prevent malware spread.

Standards & Frameworks

- ISO 27001, NIST CSF, COBIT, GDPR.
- Example: Organizations adopt ISO 27001 for structured data protection.

Security in Daily Life

- Update devices, avoid public Wi-Fi, don't click suspicious links, backup data.
- Example: Using personal hotspot for mobile banking.

Security in Organizations

- Network segmentation, audits, staff training, monitoring.
- Example: Conducting security audits every 6 months.

Future Trends

- AI-based defense, Zero-Trust, quantum-safe encryption, IoT security.
- Example: AI detecting unusual login activity.

Conclusion

- Information security requires technology, policies, and user awareness.
- Example: Campus data stays safe through firewalls, SOPs, and staff training.