POSTS AND TELECOMMINICATIONS INSTITUTE OF TECHNOLOGY

Department of Information Technology 1

Final Report

Subject: type of security attacks

Student : **Nguyễn Bình Minh**
Student's ID : **B22DCDT192**
Class : **E22HTTT**

Hà Nội – 2025

Introduction

In the digital era, information systems and data have become valuable assets for individuals, enterprises, and governments. Alongside the benefits of digitalization come significant risks of cyberattacks—attempts to steal data, disrupt services, or damage systems. This paper provides a concise overview of common types of security attacks, their mechanisms, impacts, and key preventive measures. It is designed to fit a four-page printed booklet for educational or reference purposes.

1. Overview of Security Attacks

A **security attack** refers to any deliberate or accidental action aimed at breaching the confidentiality, integrity, or availability of information systems. These three elements—known as the **CIA Triad**—are the foundation of information security:

- **Confidentiality:** Preventing unauthorized access to data.
- **Integrity:** Ensuring data accuracy and consistency.
- **Availability:** Guaranteeing that services and data remain accessible to authorized users.

Attackers, or **threat actors**, include cybercriminals, hacktivists, insider threats, and state-sponsored groups. Attack vectors range from phishing emails and malicious websites to compromised devices, software vulnerabilities, or insider misuse.

2. Main Categories of Attacks

2.1 Passive vs. Active Attacks

- **Passive attacks** monitor or intercept communications (e.g., eavesdropping, traffic analysis).

- **Active attacks** alter, inject, or destroy data, or disrupt normal service operation.

2.2 Common Attack Vectors

1. **Malware:** Viruses, worms, trojans, and ransomware designed to damage or control systems.
2. **Phishing & Social Engineering:** Tricks victims into revealing credentials or sensitive data.
3. **Man-in-the-Middle (MITM):** Intercepting data between two parties.
4. **Denial-of-Service (DoS/DDoS):** Overwhelming resources to make a service unavailable.
5. **Injection Attacks (SQLi, Command Injection):** Inserting malicious code into vulnerable inputs.
6. **Cross-Site Scripting (XSS):** Injecting harmful scripts into websites.
7. **Brute-force & Credential Stuffing:** Automated password-guessing or use of leaked credentials.
8. **Zero-day Exploits & RCE:** Exploiting unknown vulnerabilities to execute code remotely.
9. **Supply-Chain Attacks:** Compromising trusted third-party software or hardware.
10. **Insider Threats:** Malicious or careless actions from internal personnel.
11. **Physical Attacks:** Direct physical tampering or theft of equipment.

3. Examples and Real-World Incidents

3.1 WannaCry Ransomware (2017)

A global ransomware outbreak exploited an SMB protocol vulnerability in Windows (EternalBlue). Hundreds of thousands of machines were encrypted, demanding Bitcoin ransom. **Lesson:** timely patching, offline backups, and network segmentation are vital.

3.2 Equifax Data Breach (2017)

Due to an unpatched Apache Struts vulnerability, attackers stole personal data of over 140 million users. **Lesson:** maintain asset inventory, enforce patch management, and deploy web application firewalls.

3.3 SolarWinds Supply‑Chain Attack (2020)

Attackers injected malicious code into legitimate software updates, affecting multiple U.S. government agencies. **Lesson:** verify supply‑chain integrity, code‑signing, and strict build‑process controls.

4. Prevention, Detection, and Response

4.1 Prevention Principles

- **Defense in Depth:** Multi‑layered protection at network, host, and application levels.
- **Least Privilege:** Grant only necessary access rights.
- **Patch Management:** Regularly update systems to eliminate vulnerabilities.
- **Multi‑Factor Authentication (MFA):** Reduces credential theft risk.
- **Encryption:** Protects data in transit and at rest.
- **Secure Development Lifecycle (SDLC):** Incorporate security in every software stage.

4.2 Detection and Monitoring

- **SIEM:** Aggregates logs for threat correlation.
- **IDS/IPS:** Identifies and blocks suspicious activities.
- **EDR:** Monitors endpoint behavior for malware and anomalies.
- **Threat Intelligence:** Updates known indicators of compromise (IOCs).

4.3 Incident Response (IR)

1. **Preparation:** Build incident‑response playbooks and contact lists.

2. **Detection & Analysis:** Quickly identify scope and impact.
3. **Containment & Eradication:** Isolate infected systems and remove malicious code.
4. **Recovery:** Restore operations from clean backups.
5. **Lessons Learned:** Post‑incident review to strengthen defenses.

4.4 Human and Organizational Aspects

- Regular employee awareness training (anti‑phishing simulations).
- Clear password and BYOD (Bring‑Your‑Own‑Device) policies.
- Periodic penetration testing, vulnerability scanning, and security audits.