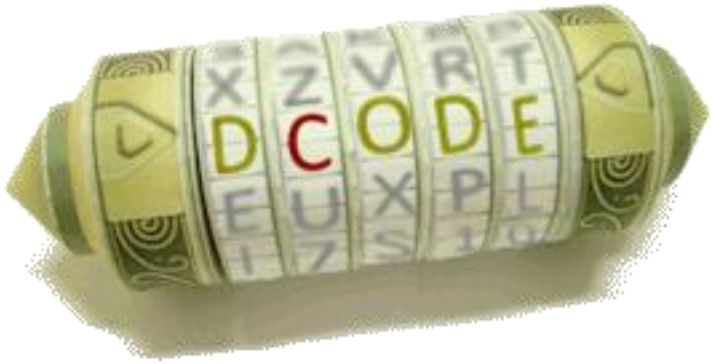
COMPUTER SECURITY

L3 - Computer Systems (2025/2026)

About the Subject

- Coefficient : 3 Credit : 5
- Evaluation :
  - Attendance/5,
  - Participation/3,
  - Test/12,



- Links:
  - Blog: http://cryptosdz.blogspot.com
  - E-mail: mistudents14@gmail.com
  - Course: moodle.univ-dbkm.dz

References

- **Handbook of Applied Cryptography**, A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press

- **Cryptography Theory and Practice**, Douglas R. Stinson, Fourth edition, CRC Press

- **Sécurité informatique : Cours et exercices corrigés**, 3ème edition, Vuibert

- **Cryptographie et sécurité informatique**, Notes de cours, Université de Liège

- **Websites:**
  - Cybrary
  - coursera
  - dcode

PLAN

- Foundations of Cybersecurity
- Classical Cryptography: Substitution and Transposition Ciphers
- Modern Cryptography: Symmetric and Asymmetric Algorithms (DES, AES, RSA)
- Cryptographic Hash Functions
- Digital Signatures
- Principles of Cryptanalysis
- Cryptographic Tools
- Public Key Infrastructure (PKI) and Certificate Management

Introduction to Cybersecurity

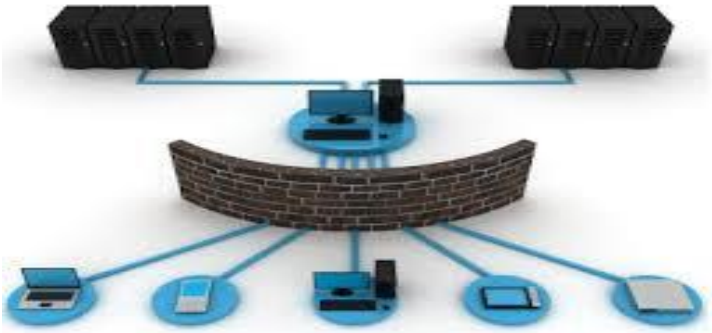
- Definition
- Types of threats
- Security services
- Security mechanisms

DEFINITION

Cybersecurity is the discipline that focuses on **protecting** computer systems, networks, and data from security **threats** such as unauthorized access, attacks, misuse, or damage.

It ensures that information systems operate safely and reliably, even in the presence of malicious actors

- **Technical mechanisms**
- **Organizational policies**
- **Human awareness**



Cybersecurity Services

- **Confidentiality**
  Making information unreadable to unauthorized third parties (Encryption, Access control)
- **Authenticity**
  Identifying the author of a message (Authentication mechanisms)
- **Data Integrity**
  Protecting messages against any form of modification (Hash functions)
- **Non-repudiation**
  Guaranteeing the authenticity of the act (Digital signatures)
- **Access Control**
  Limiting and controlling access to various resources (Privileges)

BASIC CONCEPTS

- **Vulnerability (flaw):**

A weakness in a computer system that allows an attacker to compromise the integrity of that system.
Example: An outdated operating system with unpatched software

- **Threat:**

A potential cause of an incident that may result in harm to the system or organization.
Example: A hacker attempting to steal user data

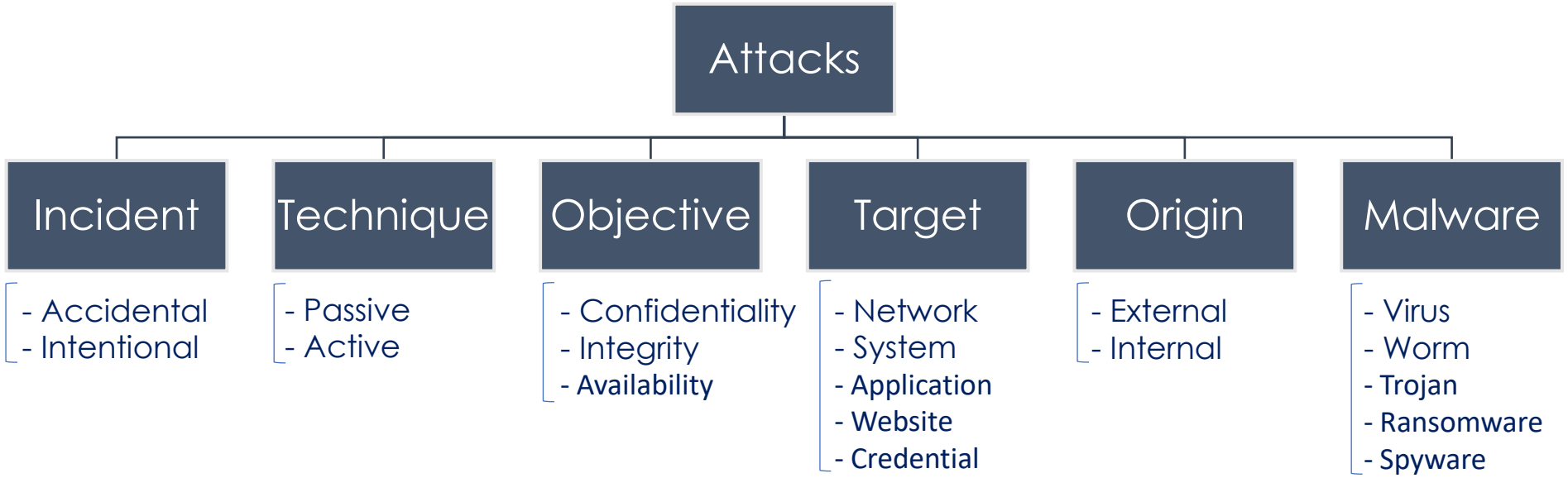
- **Countermeasure:**

A set of actions implemented to prevent the threat.
Example: Installing security patches or using strong authentication

- **Risk:**

The probability that a threat exploits a vulnerability
Example: High risk when weak passwords are used on an exposed server

CYBERATTACKS TAXONOMY



TYPES OF INCIDENTS

- **Accidental Threat**: Action performed by mistake or system malfunction
- **Examples:**
  - Sending confidential emails to the wrong recipient
  - Accidentally deleting critical files
  - Misconfiguring a firewall or server

- **Intentional Threat:** Action performed by an entity to violate security
- **Examples:**
  - Hacking and unauthorized access
  - Malware infection
  - Denial of Service (DoS)

ATTACK TECHNIQUES

- **Passive attack:** Collecting information without altering data
- **Examples:**
  - Eavesdropping
  - Electronic surveillance
  - Wiretapping

  Tools: Wireshark

- **Active attack:** Modify, destroy, or disrupt data or services
- **Examples:**
  - Data modification
  - DoS
  - Session hijacking

Attack Objectives

- **Attacks against confidentiality:**

  Read or disclose sensitive information during transfer

Examples:

- Sniffing
- Phishing
- Spyware

Tools:

- Wireshark
- Social Engineer Toolkit (SET)
- Pegasus, DarkComet

ATTACK OBJECTIVES

- **Attacks against integrity:**

  Alter or manipulate data

Examples:

- SQL injection
- Data tampering
- Website defacement

Tools:

- Ettercap
- SQLmap
- Deface

ATTACK OBJECTIVES

- **Attacks against availability:**

  Make systems or services unavailable

Examples:

- DoS/DDoS
- Ransomware
- Resource exhaustion attacks

Tools:

- LOIC (HTTP/UDP/TCP floods)
- Botnets

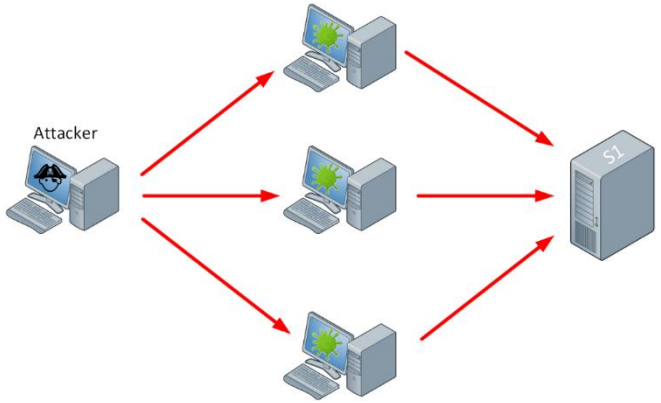
Attack Target

- **Network Attacks:**

  Target communication networks and data in transit (routers, swithes, Links)

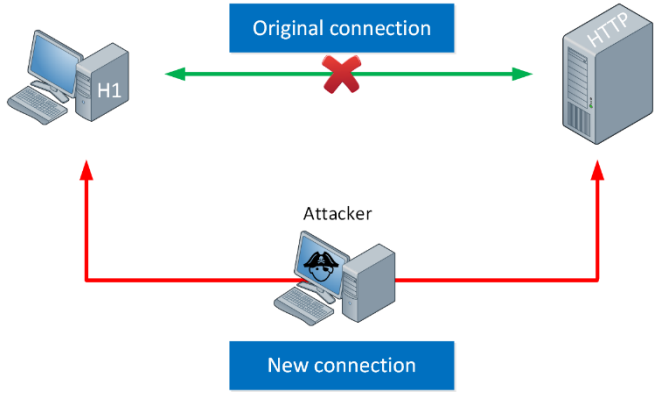
Examples:

- DoS/DDoS
- Man-in-the-Midle (MitM)
- Packet sniffing
- Reconnaissance



Tools:

- Botnets
- Ettercap, Bettercap (ARP Poisoning, Session Hijacking)
- Wireshark
- Nmap, OWASP ZAP



ATTACK TARGET

- **System Attacks:**

  Target operating systems and system resources

Examples:

- Privilege escalation
- Rootkits
- Malware infections

Tools:

- WinPEAS, LinPEAS
- Nidhogg, Metasploit
- KawaiiGPT, Tox

ATTACK TARGET

- **Application Attacks:**

  Exploit vulnerabilities in software applications (Desktop, Mobile)

Examples:

- Buffer overflow
- Code injection
- Insecure APIs

Tools:

- Overflow Helper
- Commix
- Autoswagger

Attack Target

- **Web Attacks:**

  Targeting websites and web services

Examples:

- SQL injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)

```
(http://www.estore.com/items/items.asp?userid=999 or 1=1)

(http://www.estore.com/items/iteams.asp?userid=999; DROP TABLE Users)
```

Tools:

- The go-to, jSQL Injection
- XSStrike, Dalfox

ATTACK TARGET

- **Password Attacks:**

  Compromise authentication mechanisms

Examples:

- Brute force
- Dictionary attacks
- Credential stuffing

Tools:

- Hydra
- Patator
- Medusa

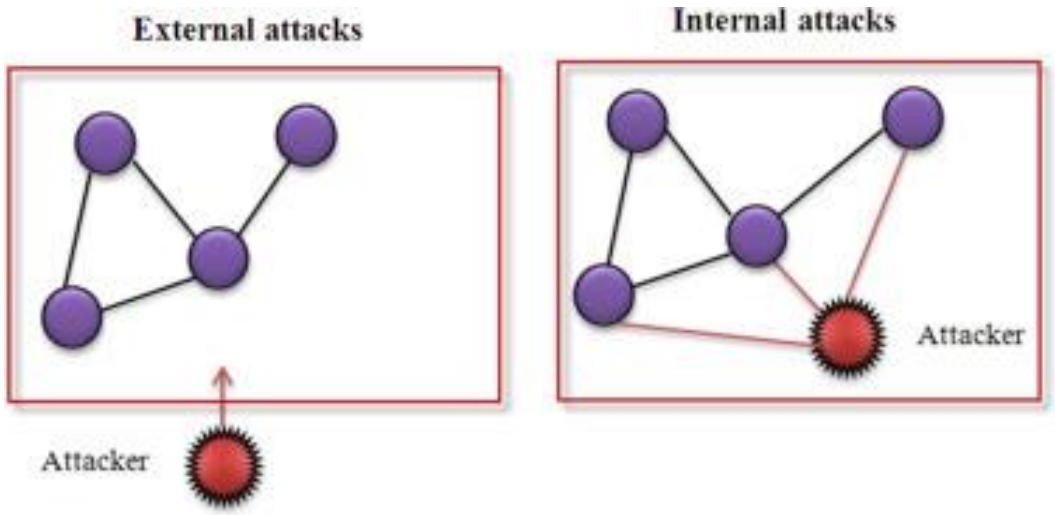
Attack Origin

- **External Attacks:**

  Launched by attackers outside the organization

Examples:

  - Internet-based hacking
  - Botnet attacks
  - Credential stuffing



- **Internal Attacks:**

  Launched by insiders with legitimate access

Examples:

  - Data theft by employees
  - Privilege misuse

Malware-Based Attacks

Malware is software designed to damage or exploit systems

- **Viruses:**

  Viruses attach themselves to legitimate programs and spread when executed

Types:

- Boot sector viruses
- File viruses
- Macro viruses

Examples:

- Wabbit, Melissa
- Fork Bombs

Malware-Based Attacks

Malware is software designed to damage or exploit systems

- **Worms:**

Worms self-replicate and spread automatically over networks

Propagation methods:

- Email
- Network

Examples:

- ILOVEYOU
- WannaCry
- Win32/Autorun, VBS:Agent

Malware-Based Attacks

Malware is software designed to damage or exploit systems

- **Trojan Horses:**

  Trojan Horses appear legitimate but hide malicious functionality

Examples:

- Keyloggers
- Spyware
- Ransomware

Tools:

- Locky
- Pegasus

Security Approaches

Guaranteeing security services

- **Offensive security:** Finds weaknesses
- **Defensive security:** Protects and monitors systems
- **Countermeasures:** Reduce risk
- **Security mechanisms:** Ensure prevention, detection, and recovery

SECURITY APPROACHES

Guaranteeing security services

- **Offensive security:**

  Actively testing systems by simulating attacks(Red teaming)

Techniques:

- Penetration testing
- Ethical hacking
- Vulnerability assessment

Tools:

- Metasploit
- Nmap

SECURITY APPROACHES

Guaranteeing security services

- **Defensive security:**

Preventing attacks, detecting malicious activity, and responding to incidents(Blue teaming)

Techniques:

- Protect systems against known and unknown threats
- Monitor networks and systems
- Detect intrusions and anomalies
- Respond to and recover from incidents

Tools:

- Firewalls
- Antivirus
- Intrusion Detection and Prevention Systems (IDS/IPS)

Security Approaches

Guaranteeing security services

- **Countermeasures:**

  Reduce risk by preventing or limiting attacks

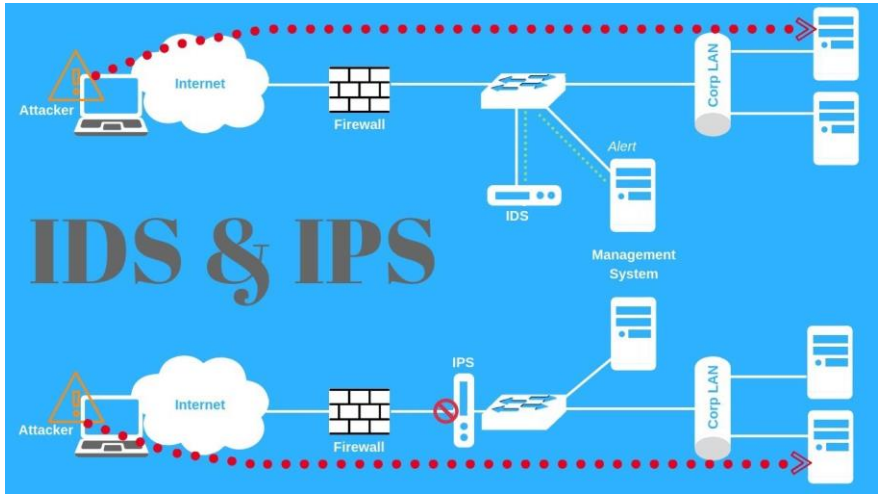
Techniques:

- Network segmentation (VLANs)
- Strong authentication and access control
- Encryption of data in transit and at rest
- Network Address Translation (NAT)
- Regular patching and updates

SECURITY MECHANISMS

How protection is applied throughout the attack lifecycle

- **Prevention:** Stop attacks before they occur
  - Access control
  - Firewalls
  - Authentication mechanisms
- **Detection:** Identify attacks or security violations
  - IDS/IPS
  - Monitoring
  - Log analysis
- **Recovery:** Restore systems after an incident
  - Data backups
  - Disaster recovery plans
  - System restoration procedures



SECURITY OPERATIONS CENTER

Centralized team of security experts that monitors, detects, investigates, and respond to cyber threats 24/7

- **SOC Analyst:**

Monitors events on the organization's network and systems to identify suspicious or expected behavior

- **Incident Responder:**

Investigates and responds to ongoing security incidents within the organization

- **Security Engineer:**

Develops and maintains the essential tools and systems that support the blue team

- **Digital forensics:**

Utilize their expertise to understand what occurred during an incident (gathers information about attacks and attackers)