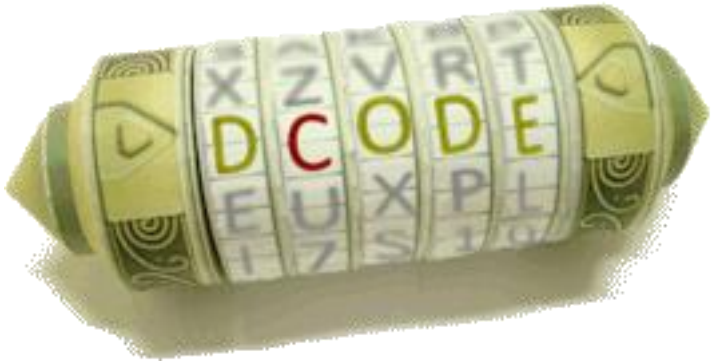
INFORMATION SECURITY

L3 - Computer Systems, 2023/2024

IT Security: Subject matter

- Coefficient : 3 Credit : 5
- Evaluation :
  - Attendance/5,
  - Participation/3,
  - Interrogation/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

- https://www.dcode.fr

PLAN

- Introduction to Cybersecurity
- Classical encryption (Substittion, Transposition)
- Modern encryption (DES, AES, RSA)
- Hash function
- Digital signature
- Cryptanalysis
- Encryption tools
- Blockchain
- PKI (Public Key Infrastructure)

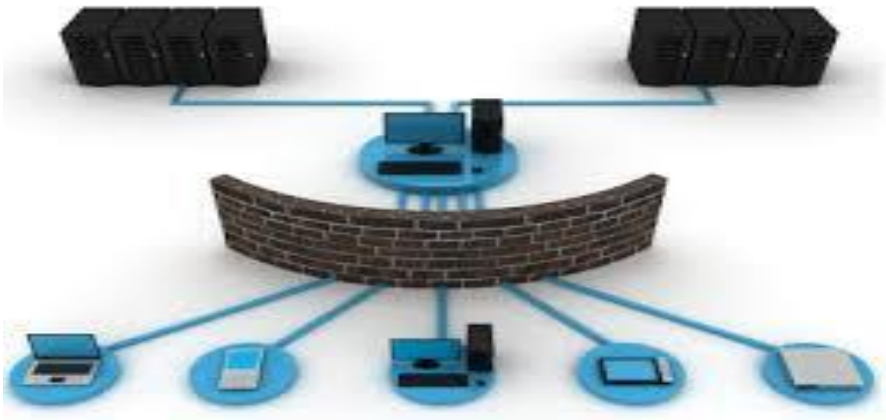
I. INTRODUCTION TO CYBERSECURITY

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

DEFINITION

- Computer security involves protecting hardware and software resources against potential risks (threats, intrusions, etc.).

- It ensures that the hardware and software resources of an organization are used only within the intended scope.



BASIC CONCEPTS

- Vulnerability (flaw): a weakness in a computer system that allows an attacker to compromise the integrity of that system.

- Threat: a potential cause of an incident that may result in harm to the system or organization.

- Countermeasure: a set of actions implemented to prevent the threat.

- Risk: (Threat x Vulnerability)/Countermeasure

TYPES OF THREATS

- Accidental threats
- Intentional threats (attacks)

1. Accidental threat : action performed by mistake

Examples:

- Send advertising messages to someone can generate a flood of unnecessary messages (e.g: spam).
- Send a confidential message to the wrong person by mistake.

TYPES OF THREATS

- Accidental threats
- Intentional threats (attacks)

2. Intentional threat: action performed by an entity to violate security:

- Passive attack: Only allows for the collection of information based on eavesdropping (electronic surveillance, wiretapping).
- Active attack: Can involve the destruction, modification, fabrication, interruption, or interception of data.

Examples of attacks

- Attacks against confidentiality or integrity:

(The content can be read or modified during transfer)

- Unauthorized access to the messaging system:

(Hijacking access control, guessing or stealing a password)

- Identity theft:

(Sending messages using the identity of others)

- Repudiation:

(Denying the sending or receiving of certain messages)

- Attack against availability:

(Bombarding a mail server (TCP-SYN flooding))

- Software attacks:

(Trojans, worms, etc.)

Software attacks

- *Viruses*
- *Worms*
- *Trojan horses*

Virus

DEFINITION:

They are capable of replicating themselves and then spreading to other computers by inserting into other legitimate programs or documents called '**hosts**':

- Boot sector virus
- File virus
- Macro virus
- Script virus

Examples: *Wabbit, Boot,…*

Worm

DEFINITION:

They are capable of sending a copy of themselves to other machines.

- Email worms
- Internet worms
- IRC worms (Internet Relay Chats)
- Network worms

Example: *Loveletter (*ILOVEYOU*), Here you have,…*

Trojan horse

DEFINITION:

It is a malicious software (malware). A seemingly legitimate software that contains malicious functionality.

- Back-door
- Injectors (Droppers)
- Notifiers (Trojan),
- Spyware (keyloggers)

Examples: Rootkit, Ransome

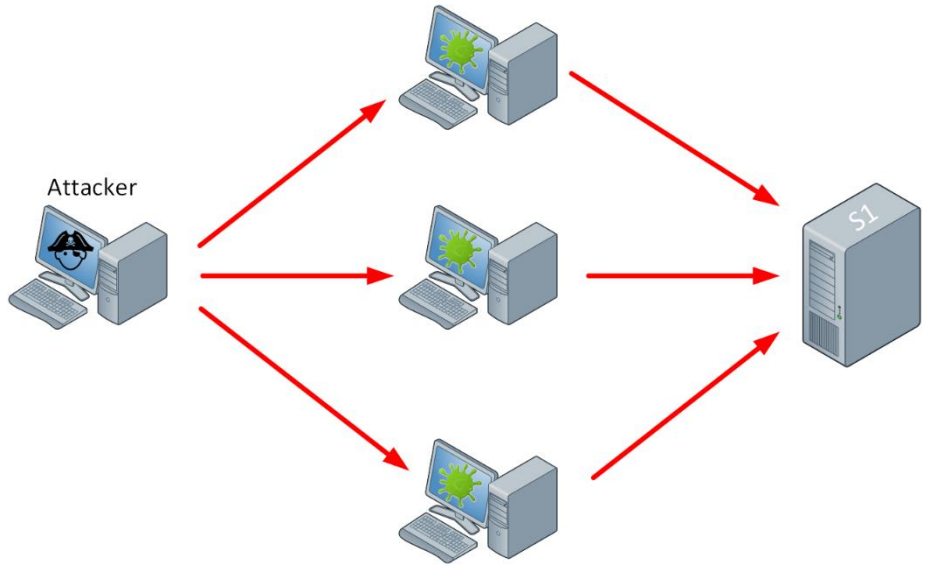
Network Attacks

- **Unauthorized Access**

An attacker gains access to the network without receiving authorization.
Causes: Weak password, Social engineering, Phishing, Insider threats

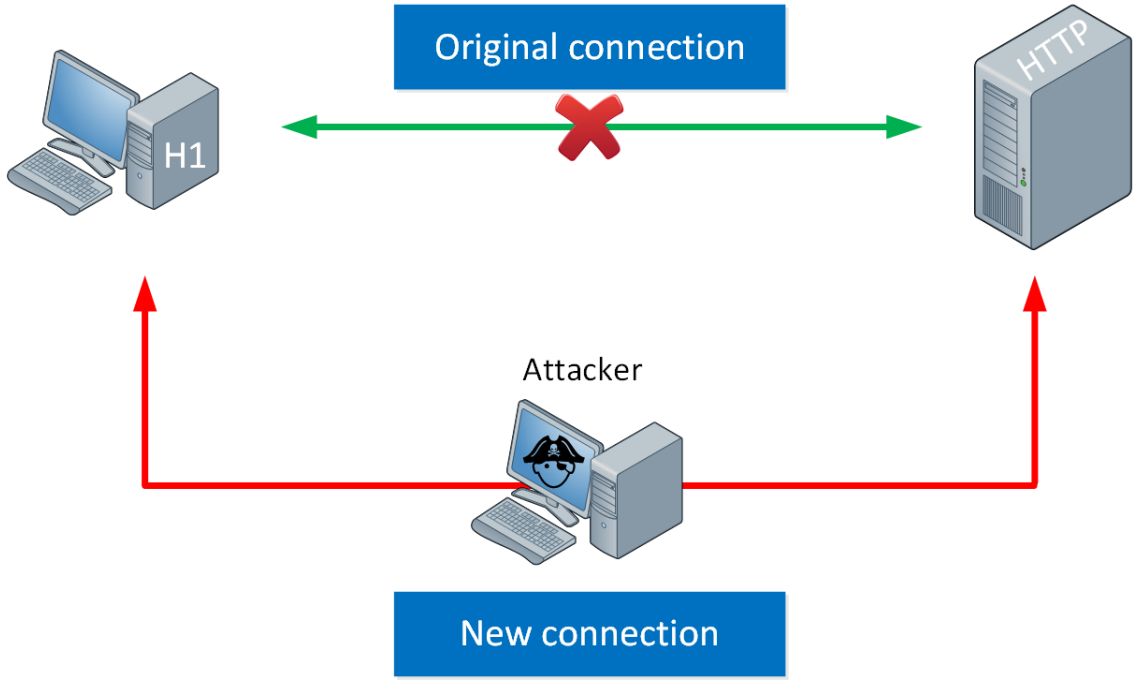
- **Distributed Denial of Service (DDoS)**

Attackers create botnets and use them to direct fake traffic to a network (or server) in order to overwhelm it.
Example: SYN/ACK packets, Complex SQL queries



Network Attacks

- **Man in the middle (MiTM)**
  - Allows an attacker to eavesdrop on communication between two devices in order to bypass security.
  - **Examples:** ARP Poisoning, Sniffing, Hijacking



Network Attacks

- **Code or SQL injection**

Attackers can exploit a form or make an API call, transmitting malicious code instead of the expected data values.

- **Reconnaissance Attacks**

Before launching an attack, the attacker gathers as much information as possible about the target network:

- Contact information
- Public IP addresses
- Open ports
- Operating system type

Tools: Network scanning (Nmap), Vulnerability scanning (OWASP ZAP)

P. Browning. Network attacks – Everything you need to know in 20 minutes. 2022 (Youtube video)

Countermeasures

- **Network Segmentation**

  Create sub-networks (VLANs)

- **Regulate Internet access via proxy**

  Monitor user behavior

- **Proper placement of security devices**

  Firewall, Antivirus

- **Use Network Address Translation (NAT)**

  Translate internal IP addresses to public IP addresses

- **Monitor network traffic**

  Use tools that provide full network visibility (SolarWinds, WhatsUP Gold, Nagios, ...)

IT SECURITY SERVICES

- **Confidentiality**

Making information unreadable to unauthorized third parties

- **Authenticity**

Identifying the author of a message

- **Data Integrity**

Protecting messages against any form of modification

- **Non-repudiation**

Guaranteeing the authenticity of the act

- **Access Control**

Limiting and controlling access to various resources

IT Security Mechanisms

- **Prevention**

  Preventing security breaches (e.g., access control)

- **Detection**

  Detecting all attempts of security breaches

- **Recovery**

  Restoring the system to its state before the breach occurred