Ministry of Higher Education and Scientific Research
M'sila University
Faculty of Mathematics and Computer Science
Department of Computer Science

Specialty: Master in Networks

Introduction to Network Security

Presented by:
SAOUDI Lalia

2021/2022

Introduction

computer security is classified into two categories:

- those concerning the security of the computer itself, server or workstation.
- those arising from the rise of networks: Network security then defines the means employed to protect data during its transmission

Rapport sécurité

Internet Security Threat Report 2017

- Cybercriminals have carried out attacks with disastrous political repercussions. manifest attempts to disrupt the American electoral process.
- BEC (Business Email Compromise): one in 131 messages contained malware, the highest proportion in five years. BEC (Business Email Compromise) frauds based on phishing messages targeted more than 400 companies per day.
- In 2016, the most effective bank robbers equipped themselves with computers, rather than weapons. Billions of dollars were stolen during virtual attacks.
- **Ransomware has turned into an international profit centre for criminals.**

Rapport sécurité

Internet Security Threat Report 2017

- Cloud infrastructures foster cybercrime: Increasing reliance on cloud services undermines companies. In 2016, tens of thousands of MongoDB (cloud) databases were hacked.
- Internet Of Things:Software embedded in connected devices can contain vulnerabilities or misconfigurations that allow them to be hacked.
  - 2016 saw the first major incident with the emergence of Mirai malware, a botnet made up of IoT devices such as routers and security cameras.

Internet Security Threat Report 2018

Coin mining attacks :

Cyber criminals are using coin miners to steal computer processing power and cloud CPU usage from consumers and enterprises to mine cryptocurrency. While the immediate impact of coin mining is typically performance-related—slowing down devices, overheating batteries, and in some cases, rendering devices unusable,

Internet Security Threat Report 2018

Software supply chain attacks:

Hijacking software updates provides attackers with an entry point for compromising well-protected targets, or to target a specific region or sector. The Petya/NotPetya (Ransom.Petya) outbreak was the most notable example

- On June 27, 2017, a destructive payload dubbed “NotPetya” by researchers was deployed covertly using a legitimate software package employed by organisations operating in Ukraine. The attack was perpetrated using a mechanism to provide updates distributed by that vendor to their customers.

Rapport sécurité

Internet Security Threat Report 2018

- Ransomware business experiences market correction: Last year, the average ransom demand dropped to $522, less than half the average of the year prior. And while the number of ransomware variants increased by 46 per cent, indicating the established criminal groups are still quite productive
- Mobile malware continues to surge:
  - The number of new mobile malware variants increased by 54 per cent in 2017, as compared to 2016. And last year, an average of 24,000 malicious mobile applications were blocked each day.

Rapport sécurité

Internet Security Threat Report 2019

- Formjacking:
  - Cyber criminals are loading malicious code onto retailers' websites to steal buyers' credit card information. More than 4,800 websites are compromised on average each month.
- Cryptojacking Down But Not Out: Symantec blocked four times more crypto-jacking in 2018 compared to 2017.
- Ransomware Drops, But Still Challenges Organisations: Infections from enterprise and mobile ransomware have increased while terminals have experienced a decline.

Internet Security Threat Report 2019

- **Supply Chain and Living Off the Land Attacks Are the New Staple.**
  - supply chain attacks surged by 78% in 2018.
- 'Land Attacks' techniques allow attackers to hide within legitimate processes. For example, the use of malicious PowerShell scripts increased by 1000% last year.

Rapport sécurité

Internet Security Threat Report 2019

- **Cloud Security Challenges Emerge on Multiple Fronts.**
- 70 million records were stolen or leaked from improperly configured S3 buckets in 2018.
- **IoT in the Crosshairs of Attacks.**
- Routers and connected cameras are the most infected devices.

Kaspersky Security Report 2020

- **mobile banking and eCommerce**: banks may become victims of targeted ransomware attacks, as financial organisations are more likely to pay a ransom than accept a loss of data.
- **Financial institutions**: black market for digital fingerprints – and the birth of ATM malware. New cryptocurrencies are growing in popularity.
- **Healthcare**: Growing interest in medical records on the dark web and access to private patient information.
- Corporate security: focus on cloud incidents.
- **5G security**: increase the risk that someone could collect and track large data sets sent by user devices.

Highlights of the Check Point Research 2021 Security Report

- **Remote working is targeted: Hackers ramped up 'thread hijacking'** attacks on remote workers to steal data or infiltrate networks.
- **Cloud adoption races ahead of security**: Public cloud security is still a major concern for 75% of enterprises. Cloud security problems will continue into 2021.
- **Double-extortion ransomware attacks rise**: On average, a new organisation becomes a victim of ransomware every 10 seconds worldwide.
- **Attacks on the healthcare sector** have become an epidemic: in Q4 2020, CPR reported that cyber-attacks on hospitals had increased by 45% worldwide.
- **Mobiles are moving targets**: 46% of organisations had at least one employee download a malicious mobile application.

The 5 main developments in the threat landscape in 2023

- **1. Speed of ransomware attacks**
- **2. Evolution of data monetisation methods**
  - The payment of ransoms
  - Espionage and data theft
- **3. Increasingly frequent misuse of legitimate tools**
- **4. Use of AI for offensive purposes**
  - Generation of attack processes, identity theft, etc.
- **5. Targeting Cloud infrastructure**

- **Ref: https://media.advens.com/securite-operationnelle/rapport-etat-de-la-menace-2023-2024/**

Top 10 cybersecurity threats in 2024

- Human risks
- Phishing
- Ransomware
- AI-powered threats
- The dark web
- Business Email Compromise (BEC)
- Remote work
- Supply chain vulnerabilities
- Cloud Security
- Quantum computing

Definitions

Vulnerability
Weakness/Flaw: accidental or intentional fault introduced into the specification, design, or configuration of the system

Attack
Malicious action that attempts to exploit a weakness in the system and violates one or more security requirements

Intrusion
Partial or total takeover of a remote system.

Threat
Potential violation of a security property

Risk
The probability that a threat will exploit a vulnerability in the system.
Pair (threat, vulnerability)

Definitions

Security Mechanisms: a mechanism designed to detect, prevent, and combat a security attack (Encryption, Signature, Notarisation, Access Control, etc.)
Security Service: a service that enhances the security of data processing and exchange in a system. A security service uses one or more security mechanisms.

What's security of a system

- The security of a system (IT or information) is a set of technical, organisational, legal, and human measures required and implemented to reduce the vulnerability of a system against accidental or intentional threats in order to ensure security services.

1. Availability

- Availability: For a user, the availability of a resource is the probability of being able to successfully complete a work session.
- The availability of a resource is inseparable from its accessibility: it is not enough for it to be available; it must be usable with acceptable response times.

➨2 Integrity

- The integrity criterion relates to the fact that resources, data, processing, transactions, or services have not been altered, modified, or destroyed either intentionally or accidentally

.3.Confidentiality

- Confidentiality can be viewed as the 'protection of data against unauthorised disclosure.'
- There are two actions to ensure data confidentiality:

– limiting their access through a control mechanism

- Confidentiality between a sender and a receiver. Requires the encryption of the data by the sender and its decryption by the receiver

.4 Identification and authentication

- identification and authentication procedures can be implemented to aid in access control procedures and security measures.

5 Non-repudiation

- Non-repudiation is the ability to neither deny nor reject that an event (action, transaction) has taken place. This security criterion is associated with the concepts of accountability, traceability, and potentially auditability.
- Accountability is defined by the attribution of an action (an event) to a specific entity (resource, person). Accountability is related to the notion of responsibility.
- It can be achieved through a set of measures ensuring the reliable recording of pertinent information concerning an entity and an event.

Domain of application of security

- Physical and environmental security
- Operational security
- Logical and application security
- Telecommunications infrastructure security

Physical and environmental security

- control of systems and the environment:
- Protection of energy and air conditioning sources
- Environmental protection: flooding or even earthquake…
- Physical access controls to premises, equipment, and infrastructure: traceability and rigorous management of access keys to premises
- Physical redundancy of infrastructure and energy sources.
- The marking of materials
- The preventive and corrective maintenance plan for equipment

operational security

- Management of the IT park.
- Management of configurations and updates
- Incident management
- Backup plan
- Testing plan

Logical and application security

- **Logical security:**
  - implementation of security mechanisms through software that contribute to the proper functioning of programmes and services offered
  - Adequate implementation of cryptography, logical access control procedures, authentication, malware detection, and intrusion and incident detection

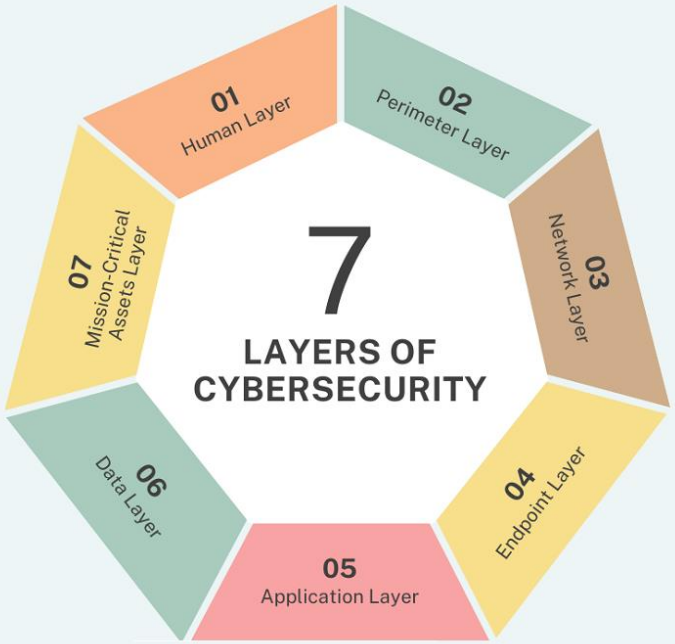
Telecommunications infrastructure security

- Providing reliable end-to-end connectivity

 implementation of a secure network infrastructure at the network access level and information transport

- the responsibility of the main actors in fraud involving the company's IT resources.
- Compliance with digital technology laws and legal conformity of their information system

Seven Layers of cybersecurity



Course questions3

- Q1: List the targets of cyber attacks in the last three years,
- Q2: What is the difference between an attack and an intrusion.
- Q3: list the different layers of cybersecurity,
- Q4: What are the origins of security problems?