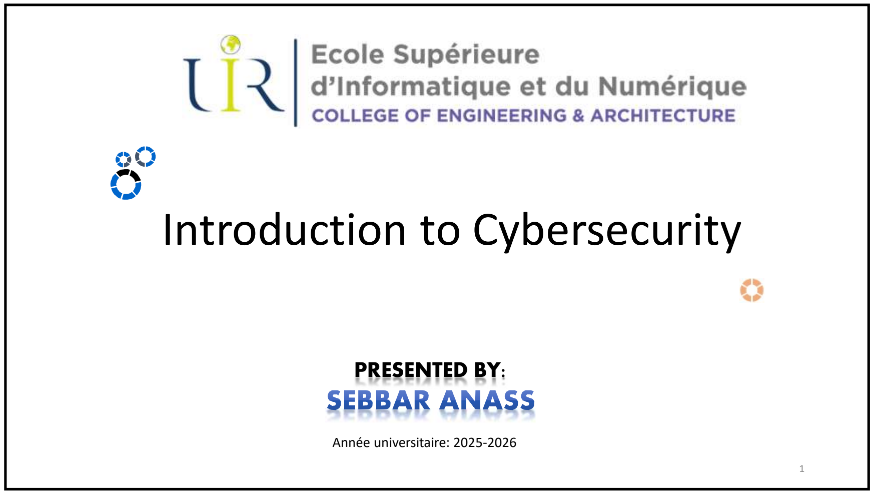
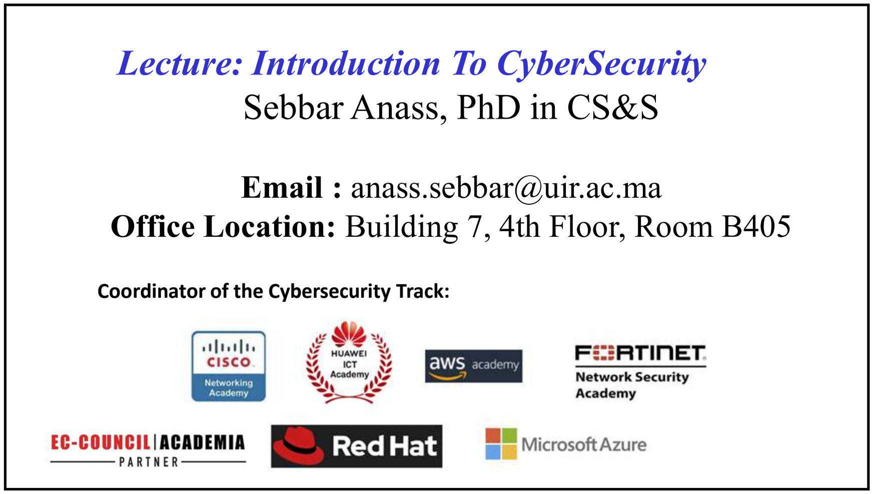


UIR | Ecole Supérieure d'Informatique et du Numérique
COLLEGE OF ENGINEERING & ARCHITECTURE

Introduction to Cybersecurity

PRESENTED BY:
SEBBAR ANASS

Année universitaire: 2025-2026

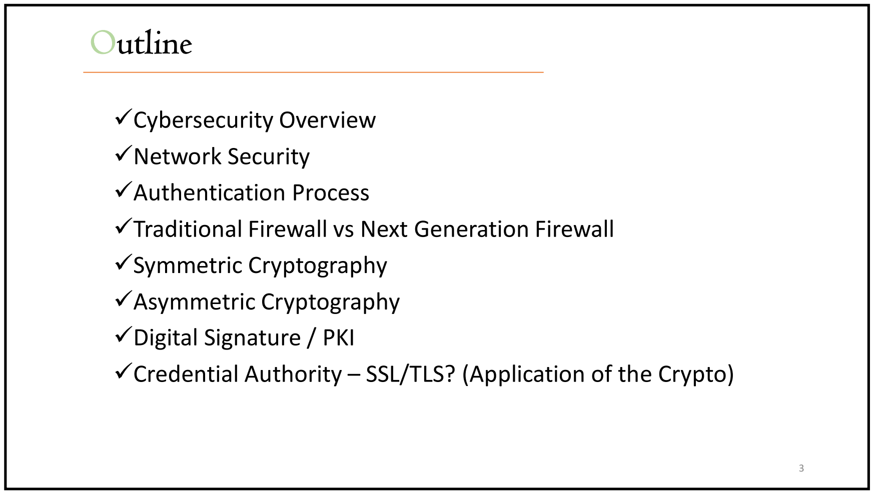


Lecture: Introduction To CyberSecurity
Sebbar Anass, PhD in CS&S

Email : anass.sebbar@uir.ac.ma
Office Location: Building 7, 4th Floor, Room B405

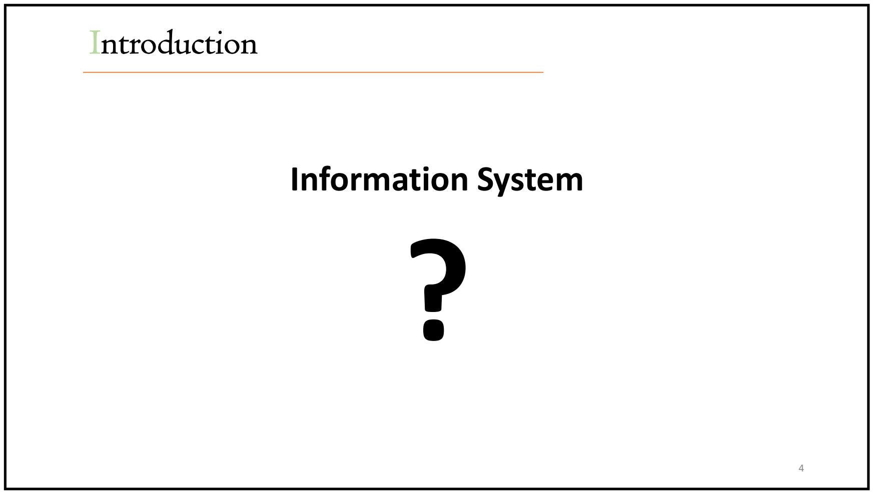
Coordinator of the Cybersecurity Track:

CISCO Networking Academy · HUAWEI ICT Academy · aws academy · FORTINET Network Security Academy · EC-COUNCIL | ACADEMIA PARTNER · Red Hat · Microsoft Azure



Outline

✓Cybersecurity Overview
✓Network Security
✓Authentication Process
✓Traditional Firewall vs Next Generation Firewall
✓Symmetric Cryptography
✓Asymmetric Cryptography
✓Digital Signature / PKI
✓Credential Authority – SSL/TLS? (Application of the Crypto)



Introduction

Information System

?

Introduction

CyberSecurity

?

5

Motivation

Cybercrime is Rising
While
Readiness Declines.*

Cybercrime **is clearly evolving, while**
Cyberdefense **measures remain far behind!!**

** 2014 U.S. State of Cybercrime Survey co-sponsored by PwC, CSO magazine, the CERT® Division of the Software Engineering Institute at Carnegie Mellon University, and the United States Secret Service.*

6

Introduction

Information

> **"Information is an asset that, like other important business assets, is valuable to an organization and, therefore, must be properly protected."**

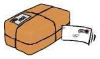
- Printed or written on paper
- Electronically stored
- Sent by mail or electronically
- communicated in conversations...

7

Introduction

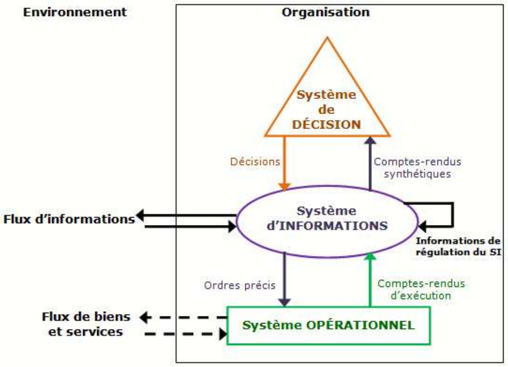
What is an information system?

Information system:
Organization of activities consisting of
to acquire, store, transform, disseminate, exploit, manage, ...
Information
One of the technical ways to operate an information system is to use a
Computer system



8

Introduction : Information system



Environnement

Organisation

Système de DÉCISION

Décisions

Comptes-rendus synthétiques

Flux d'informations

Système d'INFORMATIONS

Informations de régulation du SI

Ordres précis

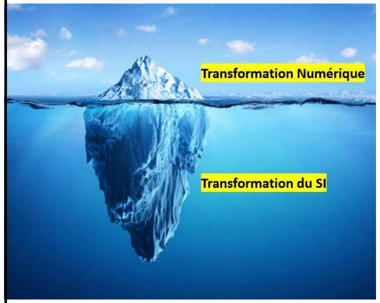
Comptes-rendus d'exécution

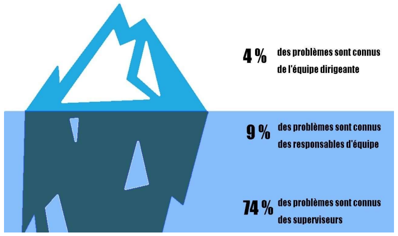
Flux de biens et services

Système OPÉRATIONNEL

9

Introduction : Information system Security





4 % des problèmes sont connus de l'équipe dirigeante

9 % des problèmes sont connus des responsables d'équipe

74 % des problèmes sont connus des superviseurs

10

10

Introduction

Evolution of Information Systems

- IS today:
  - Change dynamically:
    - Constant integration of new tools;
    - Updates, reorganizations, ...
    - Great diversity in the nature of the information (financial, technical, medical data, etc.).
  - Become more complex (heterogeneity of systems),
  - Interconnect (internally, but also externally)
- Technologies are evolving (object-oriented programming, intelligent agents, wired networks, wireless networks, ...)
  - like threats!!

11

Username : admin
Password : admin

12

Introduction

What does Cybersecurity mean:
National Security Telecommunication and Information Systems Security Committe (NSTISSC) définie la Security des réseaux comme suit:

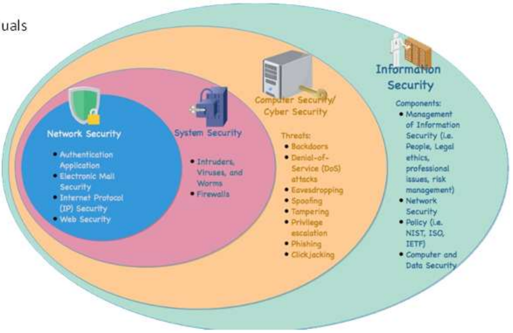
Computer Security: Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

Computer security is the protection of information and systems and hardware that use, store, and transmit that information.

Introduction

Why Cyber security?

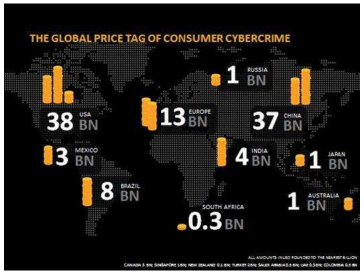
1- Internet connection 24/7
2- Increase in cybercrime
3- Impact on businesses and individuals
4- Legislation and responsibilities
5- Proliferation of threats
6- The sophistication of threats


Network Security
• Authentication Application
• Electronic Mail Security
• Internet Protocol (IP) Security
• Web Security
System Security
• Intruders, Viruses, and Worms
• Firewalls
Computer Security/ Cyber Security
Threats:
• Backdoors
• Denial-of-Service (DoS) attacks
• Eavesdropping
• Spoofing
• Tampering
• Privilege escalation
• Phishing
• Clickjacking
Information Security
Components:
• Management of Information Security (i.e. People, Legal ethics, professional issues, risk management)
• Network Security
• Policy (i.e. NIST, ISO, IETF)
• Computer and Data Security

Introduction

What is the impact of cybercrime on business:

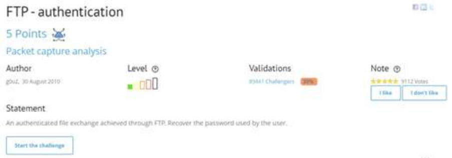
1- Decreased productivity
2- Loss of turnover
3- Release of unauthorized sensitive data
4- Threat of trade secrets of formulas
5- Compromise of reputation and trust
6- Loss of communication
7- Loss of time


THE GLOBAL PRICE TAG OF CONSUMER CYBERCRIME
38 USA BN
13 EUROPE BN
1 RUSSIA BN
37 CHINA BN
3 MEXICO BN
4 INDIA BN
1 JAPAN BN
8 BRAZIL BN
SOUTH AFRICA 0.3 BN
1 AUSTRALIA BN
ALL AMOUNTS IN USD ROUNDED TO THE NEAREST BILLION
CANADA 3 BN; SINGAPORE 1BN; NEW ZEALAND 0.1 BN; TURKEY 2BN; SAUDI ARABIA 0.5 BN; UAE 0.3BN; COLOMBIA 0.5 BN

Challenge Activity : FTP & Telnet Authentication

Objective: Explore the "FTP-authentication" challenge on Root Me.
Instructions:

- Navigate to **https://www.root-me.org/.**
- Create an account if you don't have one.
- Once logged in, follow this path: **Challenges** > **Network** > **FTP-authentication**.
- Let's find the password.



FTP - authentication

5 Points

Packet capture analysis

Author: g0uZ, 30 August 2010

Level

Validations: 89441 Challengers 30%

Note: ★★★★★ 9112 Votes

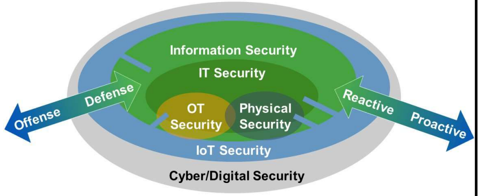
Statement

An authenticated file exchange achieved through FTP. Recover the password used by the user.

Introduction

Challenges of cybersecurity

- Application security
- Network security
- Endpoint security
- Data security
- Identity management
- Database and infrastructure security
- Cloud security
- Mobile security
- Disaster recovery/business continuity planning



Introduction

Morocco victim of a major computer attack?

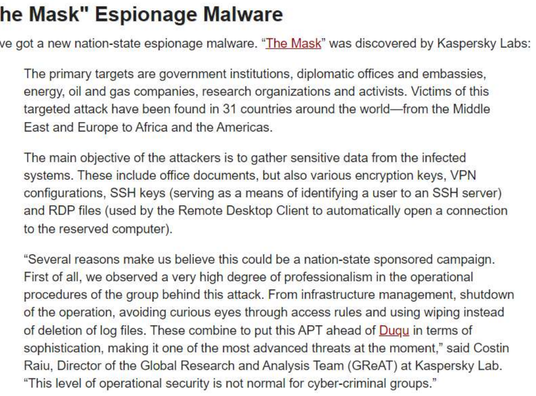
- Equifax data breach
  - Breach that may affect 500 million customers
  - Names, social security numbers, credit card numbers, addresses, etc
- Hillary Clinton Emails
- Ransomware (WannaCry, Petya)
  - Hospitals, Renault, etc
  - Power companies, airports, public transits, central bank in Ukraine

The publisher Kaspersky announces that it has discovered "The Mask", spyware that has been active since 2007. The kingdom is believed to be among the top 5 infected countries.

By Le360

Introduction

- Equifax data breach
  - Breach that may affect 143 million customers
  - Names, social security numbers, credit card numbers, addresses, etc
- Hillary Clinton Emails
- Ransomware (WannaCry, Petya)
  - Hospitals, Renault, etc
  - Power companies, airports, public transits, central bank in Ukraine



"The Mask" Espionage Malware

We've got a new nation-state espionage malware. "The Mask" was discovered by Kaspersky Labs:

> The primary targets are government institutions, diplomatic offices and embassies, energy, oil and gas companies, research organizations and activists. Victims of this targeted attack have been found in 31 countries around the world—from the Middle East and Europe to Africa and the Americas.
>
> The main objective of the attackers is to gather sensitive data from the infected systems. These include office documents, but also various encryption keys, VPN configurations, SSH keys (serving as a means of identifying a user to an SSH server) and RDP files (used by the Remote Desktop Client to automatically open a connection to the reserved computer).
>
> "Several reasons make us believe this could be a nation-state sponsored campaign. First of all, we observed a very high degree of professionalism in the operational procedures of the group behind this attack. From infrastructure management, shutdown of the operation, avoiding curious eyes through access rules and using wiping instead of deletion of log files. These combine to put this APT ahead of Duqu in terms of sophistication, making it one of the most advanced threats at the moment," said Costin Raiu, Director of the Global Research and Analysis Team (GReAT) at Kaspersky Lab. "This level of operational security is not normal for cyber-criminal groups."

Introduction

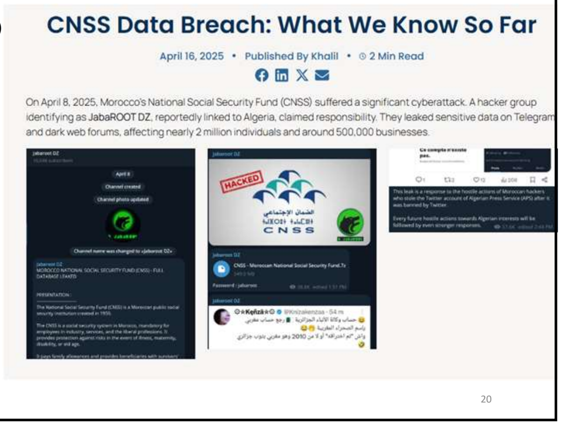
- The CNSS (National Social Security Fund) was targeted by a major cyberattack.
- The attack disrupted digital services and exposed weaknesses in information systems.
- It highlighted the growing threat to **critical public institutions**.

Impact

- Temporary unavailability of online services.
- Potential risk to sensitive personal and financial data.
- Loss of trust and operational disruption.

Likely Causes

- Credential compromise.
- Insufficient security monitoring and incident response.
- Legacy systems with limited cyber resilience.

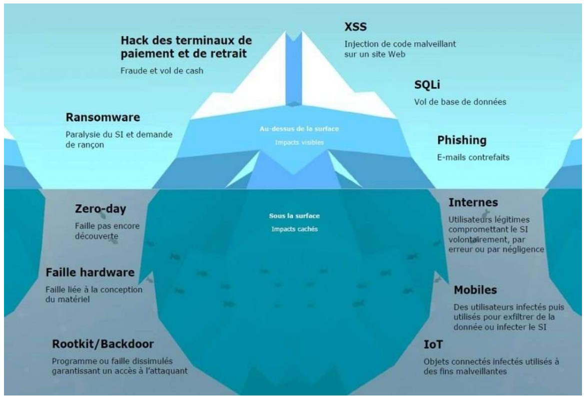


CNSS Data Breach: What We Know So Far

April 16, 2025 • Published By Khalil • 2 Min Read

On April 8, 2025, Morocco's National Social Security Fund (CNSS) suffered a significant cyberattack. A hacker group identifying as JabaROOT DZ, reportedly linked to Algeria, claimed responsibility. They leaked sensitive data on Telegram and dark web forums, affecting nearly 2 million individuals and around 500,000 businesses.

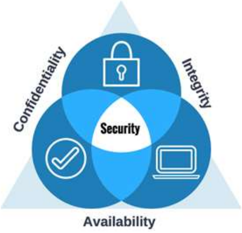
Introduction


Hack des terminaux de paiement et de retrait
Fraude et vol de cash
XSS
Injection de code malveillant sur un site Web
SQLi
Vol de base de données
Ransomware
Paralysie du SI et demande de rançon
Au-dessus de la surface
Impacts visibles
Phishing
E-mails contrefaits
Zero-day
Faille pas encore découverte
Sous la surface
Impacts cachés
Internes
Utilisateurs légitimes compromettant le SI volontairement, par erreur ou par négligence
Faille hardware
Faille liée à la conception du matériel
Mobiles
Des utilisateurs infectés puis utilisés pour exfiltrer de la donnée ou infecter le SI
Rootkit/Backdoor
Programme ou faille dissimulés garantissant un accès à l'attaquant
IoT
Objets connectés infectés utilisés à des fins malveillantes

TRIAD DE LA CIA

Confidentiality: This term covers two related concepts:

Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed



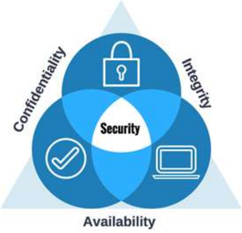
TRIAD DE LA CIA

- **Integrity:** This term covers two related concepts:

  Data integrity: Assures that information and programs are changed only in a specified and authorized manner.

  System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

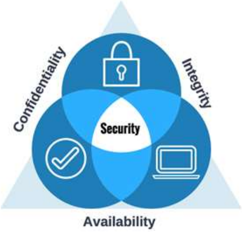
- **Availability:** Assures that systems work promptly and service is not denied to authorized users.



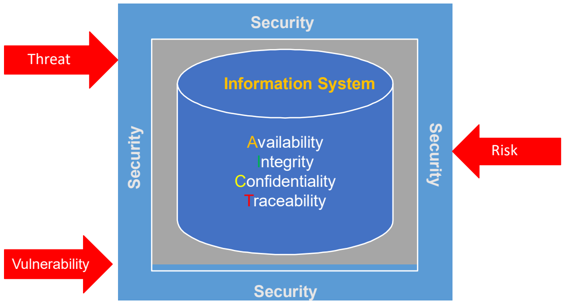
CyberSecurity goals

Goals of CyberSecurity:

- **Authenticity:** Ensure the identity of communication participants is verified.
- **Confidentiality:** Guard against unauthorized access to sensitive information.
- **Integrity:** Safeguard system information and processes from both intentional and accidental alterations.
- **Availability:** Guarantee that systems and data remain accessible to authorized users when needed.
- **Non-repudiation:** Ensure that participants in a communication cannot deny their involvement.
- **Traceability:** Ability to track and verify the history or location of an item through documented records. In cybersecurity, this means ensuring actions on a system can be linked to a specific entity or process.

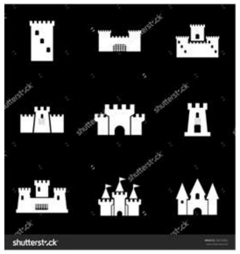


CyberSecurity goals



CyberSecurity Domains

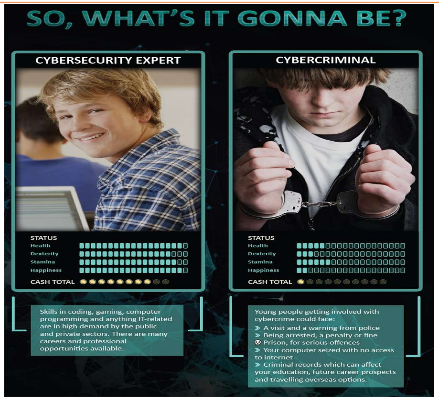
- **Websites and Power of Data**
  - ✓ Great businesses have been created by collecting and harnessing the power of data and data analytics
  - ✓ These businesses have the responsibility to protect this data from misuse and unauthorized access
  - ✓ The growth of data has created great opportunities for cybersecurity specialists
- **Domains**
  - ✓ Business large and small have recognized the power of big data and data analytics
  - ✓ Organizations like Google, LinkedIn, Amazon provide important services and opportunity for their customers
  - ✓ The growth in data collection and analytics poses great risks to individuals and modern life if precautions are not taken to protect sensitive data from criminals or others who have intent to harm



CyberSecurity Domains

- ✓ Cyber experts now have the technology to track worldwide weather trends, monitor the oceans, and track the movement and behavior of people, animals and objects in real time.
- ✓ New technologies, such as Geospatial Information Systems (GIS) and the Internet of Everything (IoE), have emerged. Each depends on collecting and analyzing tremendous amounts of data.
- ✓ This growing collection of data can help people save energy, improve efficiencies, and reduce safety risks.

Cybersecurity Criminals versus Cybersecurity Specialists



Skills in coding, gaming, computer programming and anything IT-related are in high demand by the public and private sectors. There are many careers and professional opportunities available.

Young people getting involved with cybercrime could face:

- A visit and a warning from police
- Being arrested, a penalty or fine
- Prison, for serious offences
- Your computer seized with no access to internet
- Criminal records which can affect your education, future career prospects and travelling overseas options.

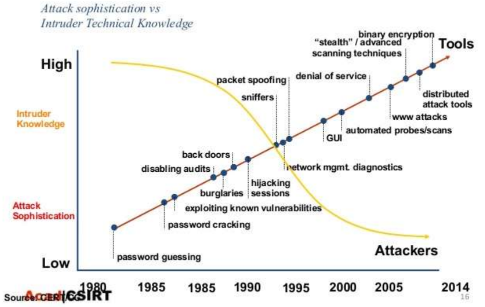
Cybersecurity Criminals versus Cybersecurity Specialists

Cost of IT Security per Year

Type de crime informatique	Royaume Unis	Monde
Online banking fraud		
Phishing	$16m	$320m
Malware (consumer)	$4m	$70m
Malware (business)	$6m	$300m
Bank tech. countermeasures	$50m	$1000m
Cost of cyber criminal infrastructure		
Expenditures on antivirus	$170m	$3400m
Cost to users of clean up	$500m	$10000m
Defense costs of firms	$500m	$10000m

**Estimation de certains coûts associés à la Security informatique.
Source: Anderson et al. Measuring the cost of cybercrime. WEIS 2012:**

No need to be an Expert to Launch Attacks ☺



Source: CERT/CC

Security tools allow hackers to launch attacks with little technical knowledge

Types of hackers

- **Script kiddies**
  - beginner hackers
  - Use ready-to-use software
- **Crime informatique organized**
  - Think the mafia. Ex: Russian Business Network
  - Monetary purpose
  - Very sophisticated and specialized: Virus development, virus distribution, hosting, etc.
- **States**
  - Gouvernments e.g. USA, Russie, Chine, Ukraine etc
  - But politique: espionage, sabotage, etc
  - Sophistication sans précédant

Types de Pirates

- **Hackactivists**
  - IT activist: political goals
  - Example: Anonymous
  - Sophistication varies
- **White hats**
  - Ethical hacker
  - Goal: discover vulnerabilities before malicious hackers

33

CyberSecurity

34

CyberSecurity Terminologies

Common network security terms:

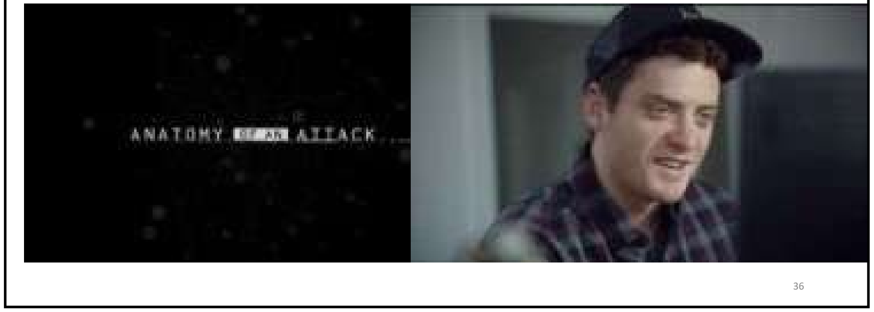
- **Attack**: Any action that compromises the security of information.
- **Security mechanisms:** a mechanism that is designed to detect, prevent and combat a security attack.
- **Security Service:** a service that increases the security of data processing and exchange of a system. A security service uses one or more security mechanisms.

35

CyberSecurity

The Steps of an attack?

- Example of a real attack Phishing vs Ransomware



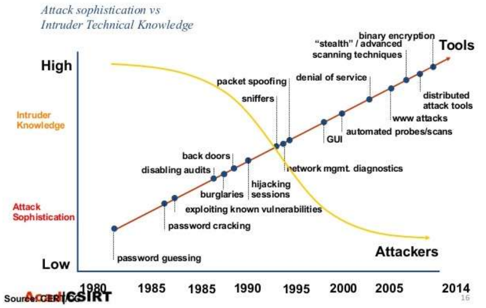
36

Cost of IT Security per Year

Type de crime informatique	Royaume Unis	Monde
Online banking fraud		
Phishing	$16m	$320m
Malware (consumer)	$4m	$70m
Malware (business)	$6m	$300m
Bank tech. countermeasures	$50m	$1000m
Cost of cyber criminal infrastructure		
Expenditures on antivirus	$170m	$3400m
Cost to users of clean up	$500m	$10000m
Defense costs of firms	$500m	$10000m

Estimation de certains coûts associés à la Security informatique.
Source: Anderson et al. Measuring the cost of cybercrime. WEIS 2012:

No need to be an Expert to Launch Attacks ☺



Security tools allow hackers to launch attacks with little technical knowledge

Types of hackers

- **Script kiddies**
  - beginner hackers
  - Use ready-to-use software
- **Crime informatique organized**
  - Think the mafia. Ex: Russian Business Network
  - Monetary purpose
  - Very sophisticated and specialized: Virus development, virus distribution, hosting, etc.
- **States**
  - Gouvernments e.g. USA, Russie, Chine, Ukraine etc
  - But politique: espionage, sabotage, etc
  - Sophistication sans précédant

Types de Pirates

- **Hackactivists**
  - IT activist: political goals
  - Example: Anonymous
  - Sophistication varies
- **White hats**
  - Ethical hacker
  - Goal: discover vulnerabilities before malicious hackers

CyberSecurity

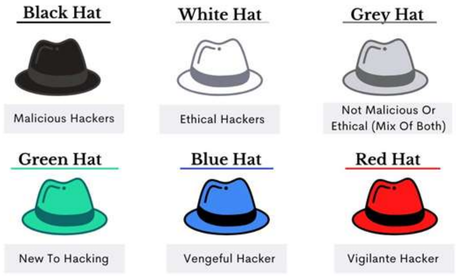
CyberSecurity Terminologies

Common network security terms:

- **Attack**: Any action that compromises the security of information.
- **Security mechanisms:** a mechanism that is designed to detect, prevent and combat a security attack.
- **Security Service:** a service that increases the security of data processing and exchange of a system. A security service uses one or more security mechanisms.

Types de Pirates

- **Hackers** – This group of criminals breaks into computers or networks to gain access for various reasons.
  - ***White hat*** attackers break into networks or computer systems to discover weaknesses in order to improve the security of these systems.
  - ***Gray hat*** attackers are somewhere between white and black hat attackers. The gray hat attackers may find a vulnerability and report it to the owners of the system if that action coincides with their agenda.
  - ***Black hat*** attackers are unethical criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks.

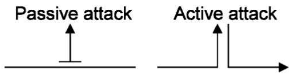


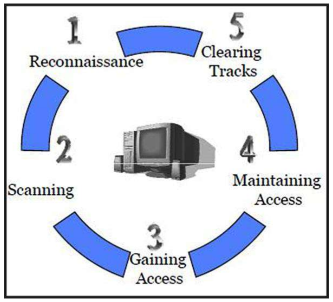
CyberSecurity

The Steps of an attack

1. Reconnaissance
2. Scanne (adresses, port, vulnérabilités)
3. Gagner access
4. Maintaing access
5. Clearing Tracks

Passive Attacks and Active Attacks





Passive and Active Attacks

Passive Attack

- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping on, or monitoring of, transmissions
- Goal of attacker is to obtain information that is being transmitted
- Two types:
  - Release of message contents
  - Traffic analysis

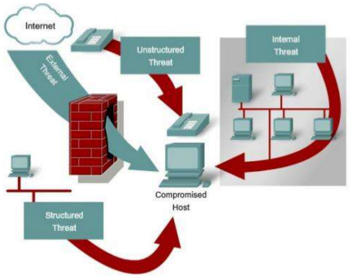
Active Attack

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream
- Four categories:
  - Replay
  - Masquerade
  - Modification of messages
  - Denial of service

CyberSecurity

Vecteurs d'attaques de réseau

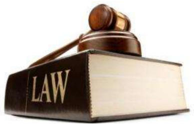
- Attaques externes
- Attaques internes
- Attaques structurées
- Attaques non structurées



The laws of CyberSecurity

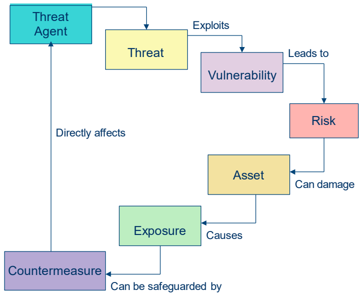
Legislation:
Several laws are established by the federal and government to protect users from the threats of cybercrime:
1- The healt Insurance Portability and Accountability 1996
2- The sarbanes-Oxley Act of 2002
3- The Gramm-Leach-Blilely Act
4- US PATRIOT ACT 2001

In Morocco we have:
1- Law 53-05 on the electronic exchange of legal data
2- Law 09-08 on the automated processing of personal data



CyberSecurity

Common network security terms:



Threat Agent
Threat
Exploits
Vulnerability
Leads to
Risk
Directly affects
Asset
Can damage
Exposure
Causes
Countermeasure
Can be safeguarded by

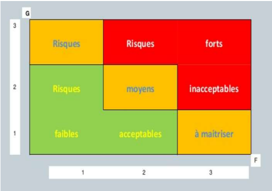
CyberSecurity Risk

Risk Management
Definition:
The assessment and quantification process and the establishment of an acceptable level of risk to the organization

Risk = Probability * Impact

Stages of risk management:

- **Risk analysis**
- **Assessed and identified threats**
- **Assessed and identified vulnerabilities**
- **Establish a Security Policy (countermeasure)**



CyberSecurity Risk

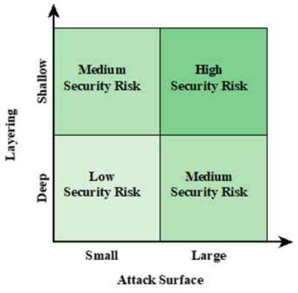
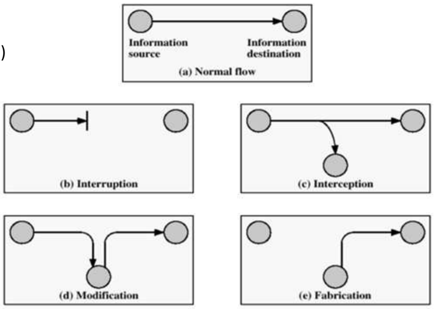


Figure 1.4 Defense in Depth and Attack Surface

CyberSecurity

Attackers' tools

- Port/address scan (nmap, Nessus)
- Vulnerability Scanner (MetaSploit, Core Impact, ISS)
- Sniffers (Wire shark, tcpdump, Snort)
- Cracking tools (Cain, wepCrack, jhon the ripper)
- Malware (viruses, worms, trojon)
- Hijackin tools (Netcat, MetaSploit)



(a) Normal flow

(b) Interruption

(c) Interception

(d) Modification

(e) Fabrication

Aims of attacks

- **Interruption**: aims at the availability of information
- **Interception**: aims at the confidentiality of information
- **Modification**: aims at the integrity of information
- **Manufacturing**: aims at the authenticity of the information