IOT & CYBERSECURITY

CYBERSECURITY

ACADÉMIE MILITAIRE
SAINT-CYR COËTQUIDAN

COURSE OBJECTIVE

- Understand the pillars of Cybersecurity
- Aware of the different methods to secure equipment and communications
- Be aware of how to secure our own internet presence

PLAN

1. Areas and pillars of Cybersecurity
2. Vulnerabilities and attacks
3. General protection methods
4. Cyber awareness

I. AREAS AND PILLARS OF CYBERSECURITY

THE CYBER SPACE

- "Virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. [It] typically involves a large computer network made up of many worldwide computer subnetworks that employ TCP/IP protocol to aid in communication and data exchange activities" – Techopedia
- Term coined in 1984 by William Gibson in *Neuromancer*.

- Digital IT world
- Worldwide covering all connected devices from IoT to Servers

MODERN WAR GROUND

- The cyberspace is recognised as the fifth domain of warfare
  - Equally critical to land, sea, air and space
- Possesses additional horizontal dimension
  - Military action in other domains → increasingly dependent on cyberspace

THE AREAS OF THE CYBERSPACE

Cyber Defence

Cyber Security

Cyber Awareness

CYBER DEFENCE

- "All technical and non-technical measures allowing a state to defend all information systems deemed essential in the cyberspace" – ANSSI
- Regroups all physical and virtual methods utilised in the "Cyber war" in the cyberspace
- Concerns the resistance against a security incident
- Can also be proactive against a target
  - US attacked suspected Iranian spy ship – February 2024

CYBER SECURITY

- "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" – ITU
- Contrast with Cyber defence
  - Defence responds to threat
  - Security prevents it
- Multiple areas linked to IT specialities
  - Cloud security, network security, application, Internet, IoT security …

CYBER AWARENESS

- "The level of awareness and understanding end users have about cybersecurity best practices and the cyber threats that their networks or organizations face every day" – Mimecast
- Not limited to security personnel → Everyone is concerned

- In 2023 → approximately 95% of attacks came from human error
  - Research by IBM Security
  - Concerns both loss as well as social-engineering

PILLARS OF CYBERSECURITY – CIA TRIAD

Confidentiality

Integrity

Availability

CONFIDENTIALITY

- Large quantities of personal data
- Must be secure
  - No unauthorised access
- Use of methods such as encryption

- Example
  - End-to-end encryption on Whatsapp

INTEGRITY

- No unauthorised modification
  - Assure completeness and accuracy of data
- Any modifications are documented and stored correctly
- Use of signatures in files to detect modificatins

- Example
  - Message between two friends is modified in the middle

AVAILABILITY

- User must have timely and easy access to data
  - Must be available even with server / database errors
- Protection needed on servers and databases
- Use of backups and redundant servers

- Example
  - Bank access through app only and app is unavailable → cannot pay

II. VULNERABILITIES AND ATTACKS

GENERAL STATISTICS

- Worldwide cost estimated → $10.5 trillion per year by 2025
- 2023 → US has highest cost of data breach at $5.09M
  - 12th year in a row!
- Cybersecurity now part of core of 53% organisation
  - Integration of cybersecurity in strategic business initiatives
- 53% organisations require cybersecurity clearance before deploying solutions
  - Proactive approach to risk management
- 27% attacks utilised extortion → manufacturing most targeted
- Asia-Pacific region most targeted → 31% attacks
  - EU – 28% | NA – 25%
- 97% organisation saw increase in threats in 2022 at start of Russa-Ukraine war
  - 51% organisations updated business continuity / enterprise risk plans in 2023

THREAT VS ATTACK

- Used together → separate but critical issues
- Threat – Presence of persistent hazard to data integrity
  - Multiple forms: huma threat, virus, malware, other …
- Attack – Deliberate and malicious action or activity to exploit vulnerabilities
  - Aim to compromise integrity / availability of data or systems
  - Gain unauthorised access to sensitive informationd

DIFFERENCE THREAT -- ATTACK

	Threat	Attack
Intention	Intentional → human negligence Unintentional → natural disaster	Deliberate, malicious action Presence of motive and plan
Initiation	By internal system or outsider	Always by outsider (system or user)
Definition	Condition / circumstance that can cause damage to system / asset	Intended action to cause damage to a system / asset
Change of damage	Low → very high	Very high
Detection	Difficult	Easy
Prevention	Controlling vulnerabilities	Controlling vulnerabilities **AND** other measures (backup, detection, awareness, …)

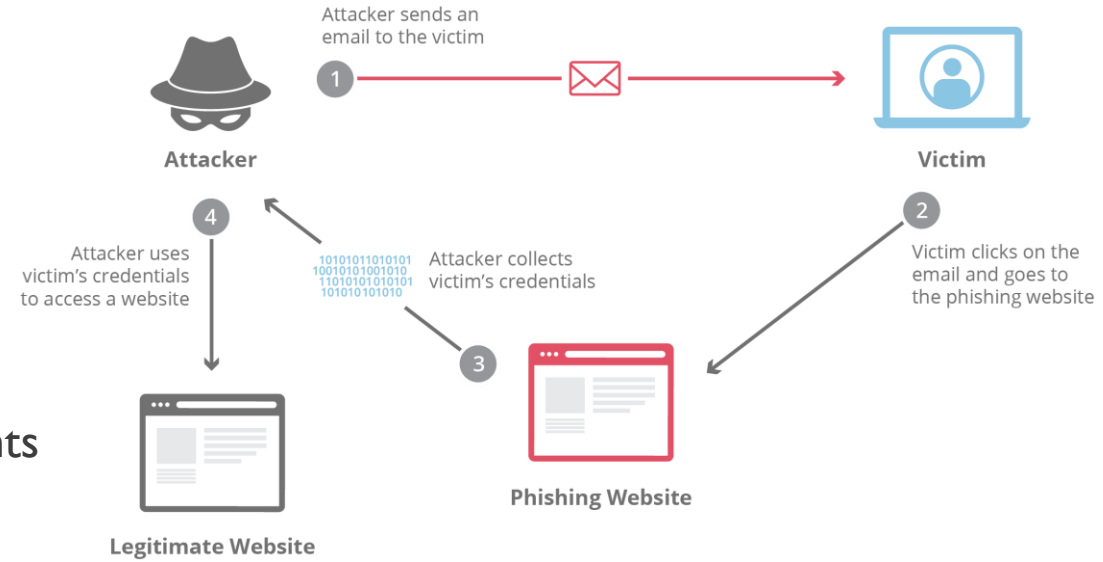
CYBER THREATS

- Significant number
  - No way of knowing how many
  - Exploiting vulnerabilities in systems and human behaviour
- Existing vulnerabilities or Zero-day exploits
- Two types of attack
  - **Passive** – Observation-based, almost invisible, no action on data / system
  - **Active** – Active participation from attacker, aim to inflict damage

Phishing
Social Engineering
Ransomware
Malware
DoS / DDoS
MitM
…

CYBER THREATS – PHISHING

- Practice of sending fraudulent emails
- Aim to trick user into interacting with the contents
  - Steal sensitive data
    - Card numbers / login information
- Most common type of attack → 39% email threats
- 94% malware delivered by email
- Identified as primary infection vector in 41% of incidents



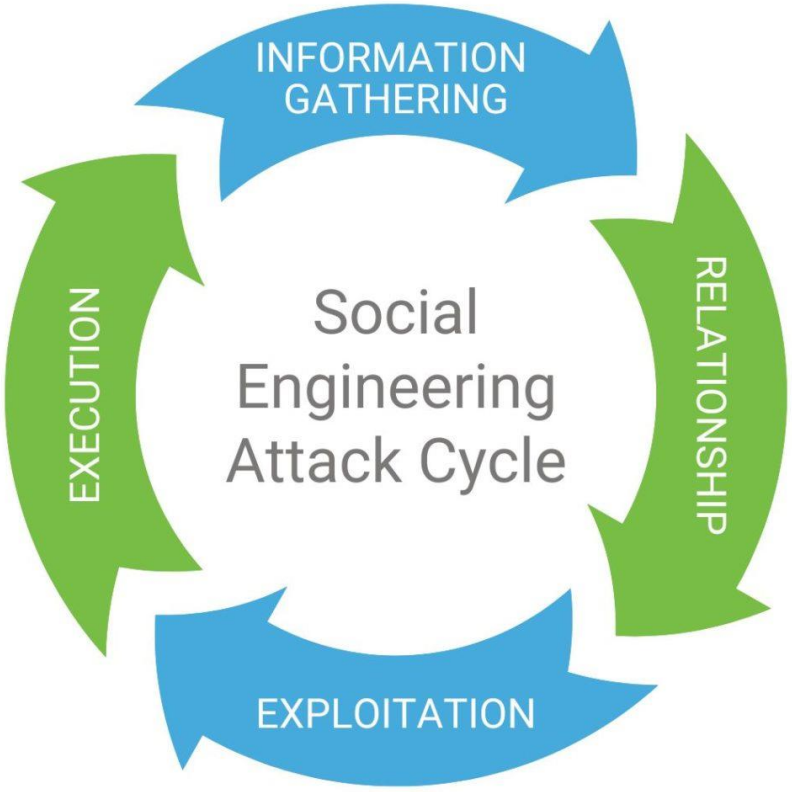
Source: Cloufflare, "*What is a phishing attack*"

- Prevention → Awareness / Email filters

CYBER THREATS – SOCIAL ENGINEERING

- Trick user to reveal sensitive information
- Solicit money or reveal sensitive information
  - Combined with any threat to influence behaviour

- Prevention → Awareness / Source verification



Source: Internos, "*The Social Engineering Attack Cycle: How Hackers Gain Your Trust in 4 Steps*", 7th October 2021

CYBER THREATS – RANSOMWARE

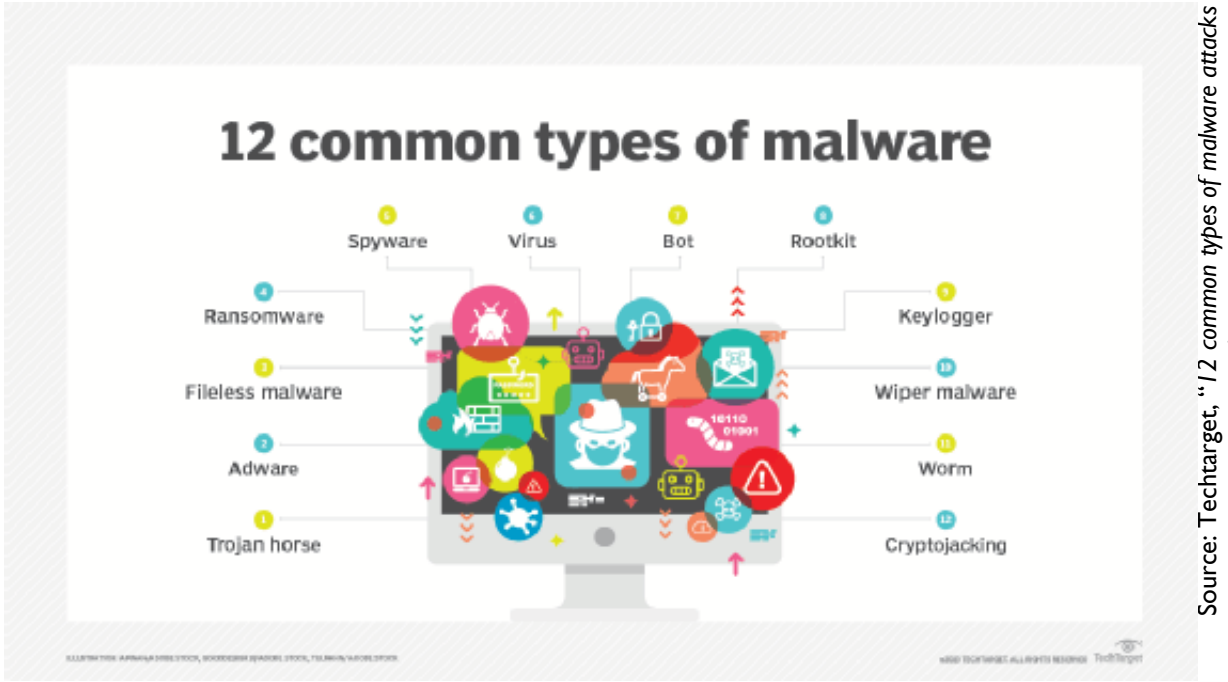
- Malicious software
- Designed to extort money from entity
  - Blocking access to files / computer system
  - Generally, encryption based
- Paying ransom does not guarantee recovery
- 71.7% global organisations impacted in 2023
  - Only 27% of incidents / decrease from 21% in 2021
- Almost half organisations pay ransom

- Prevention → Awareness / Anti-Virus / Anti-Malware

Source: Wikipedia, "*WannaCry ransomware attack*", May 2017

CYBER THREATS – MALWARE

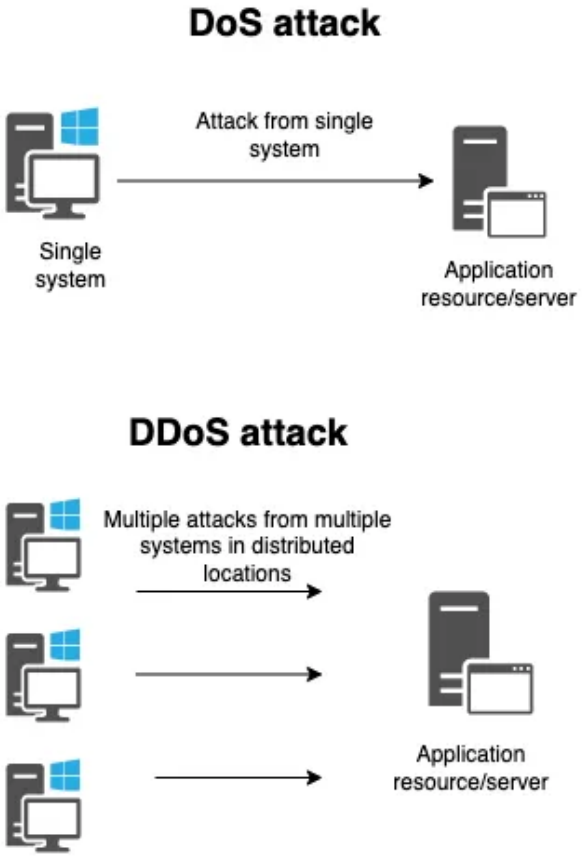
- Malicious software
  - Designed to gain unauthorised access to data
  - Cause damage to system
- Multiple types of software
  - Ransomware
- Prevention → Awareness / Anti-Virus / Anti-Malware



Source: Techtarget, "*12 common types of malware attacks and how to prevent them*", 23rd October 2023

CYBER THREATS – DOS / DDOS

- Denial of Service
- Attacks availability of a system
  - Stops users from interacting with it
- Distributed DoS more dangerous
  - Originating from multiple machines
  - Many botnet machines
    - Compromised with malware
- Very common internet-based attack
  - 2022 → 6 428 DDoS attacks reported
- Prevention → Traffic filters / DoS protection

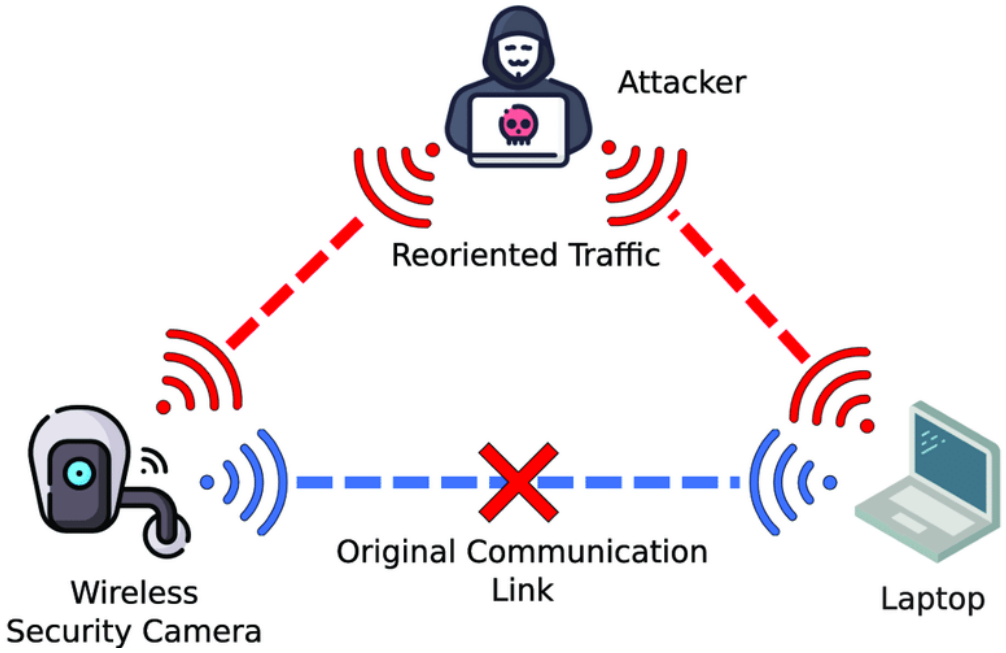


Source: Medium, "*DoS vs. DDoS attacks*", 26th October 2022

CYBER THREATS – MITM

- Man in the Middle
- Reorient traffic to pass through attacker
  - Spy on traffic, modify, send user to "fake" website
- Vary hard to identify

- Prevention → Awareness / Encrypted traffic



Source: Staddon, Edward & Loscri, V. & Mitton, Nathalie. (2021). *Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey*. Applied Sciences. 11. 7228. 10.3390/app11167228.

CYBER THREATS

Cybersecurity Threats

	Likely to Affect	Need to Understand Better
Virus	64%	41%
Spyware	62%	42%
Phishing	52%	32%
Firmware Hacking	34%	29%
IP Spoofing	32%	29%
Ransomware	31%	30%
Attacks on Virtualization	30%	30%
Social Engineering	26%	26%
Hardware-Based Attacks	26%	25%
DDoS	24%	22%
IoT-Based Attacks	23%	22%
Botnets	22%	23%
Rootkits	21%	21%
Man in the Middle Attacks	20%	23%
SQL Injection	18%	20%

Source: 6Clicks, *"What are 4 types of information security?"*

MISCELLANEOUS STATISTICS

- 55% security experts reported increased stress
  - Heightened threats and challenges
- Significant increase in global vulnerabilities
  - 23 964 in 2022 | 21 518 in 2021
- 80% organisations plan to increase security spending in 2024
- 85% hacktivist attacks in 2023 were in the EU
  - NA – 7% | Middle East – 3%
- Ransomware crypto payments reached $449.1 million in first half 2023

III. GENERAL PROTECTION METHODS

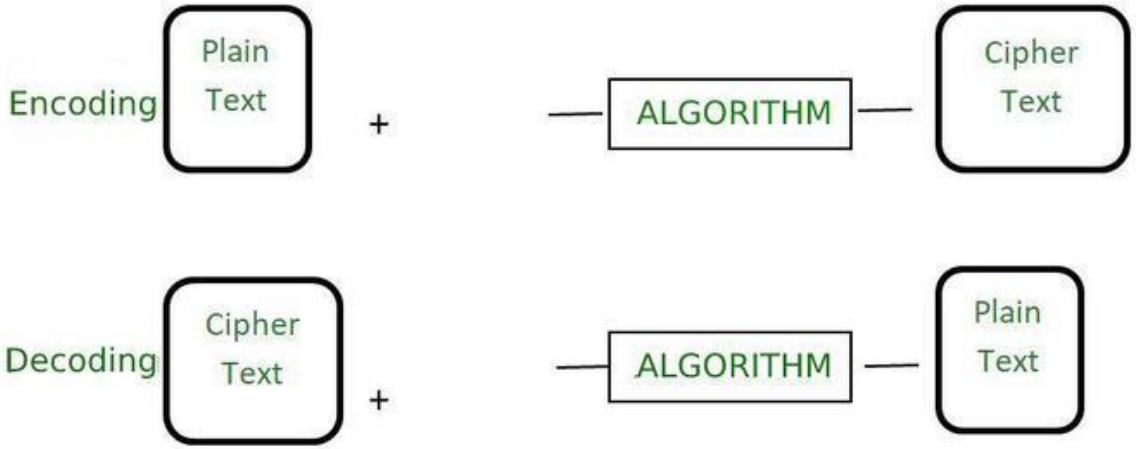
HOW TO PROTECT?

- Network traffic travelling through public domain
- No control over data once left our possession

- Secure data with various methods
  - Encryption ?
- Confirm authenticity of information
  - Signatures and certification ?
- Proactive vulnerability detection
  - Pen Testing

ENCODING VS ENCRYPTION

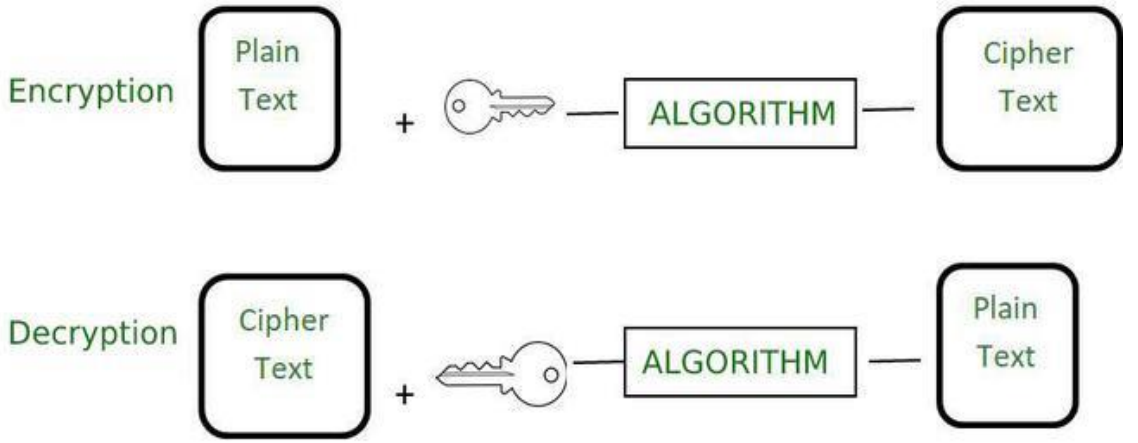
- Encoding changes contents based upon algorithm
  - Change letters with their next in line
  - Ex: Hello → lfmmp
- Difficult to understand without algorithm
- However, easy to crack
- Used in many IT systems
  - ASCII, UNICODE, URL Encoding, Base64, …



Source: Geeks for Geeks, "*Différence entre le cryotage et le codage*"

ENCODING VS ENCRYPTION

- Encryption
  - Use of personal key to modify data
  - Key is specific to person
- Without key, impossible (almost) to crack
  - Keys are long, on average 2048 bytes
- Used in many advanced
  - AES, RSA, Blowfish, SSL, …

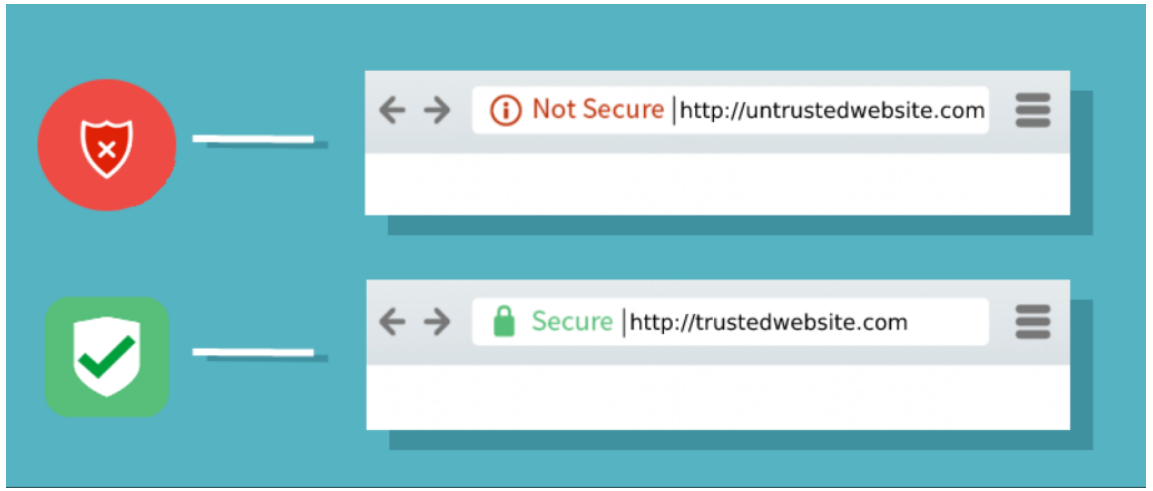


Source: Geeks for Geeks, "*Différence entre le cryotage et le codage*"

SSL

- Encryption-based method for internet security
  - HTTP → HTTPS
- Visible with padlock on browser
- Certificate based

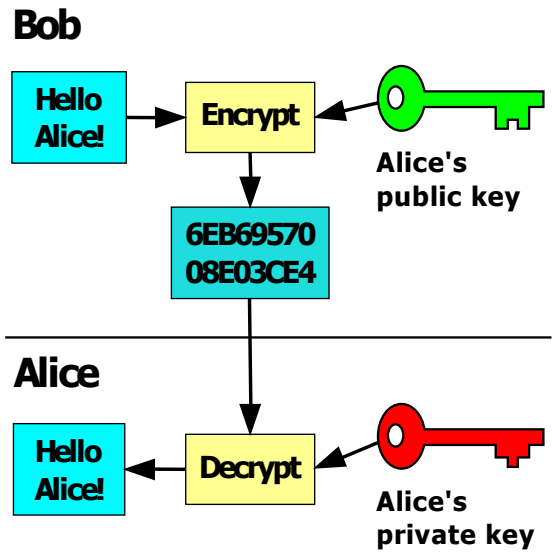
- All traffic between browser and server are encrypted

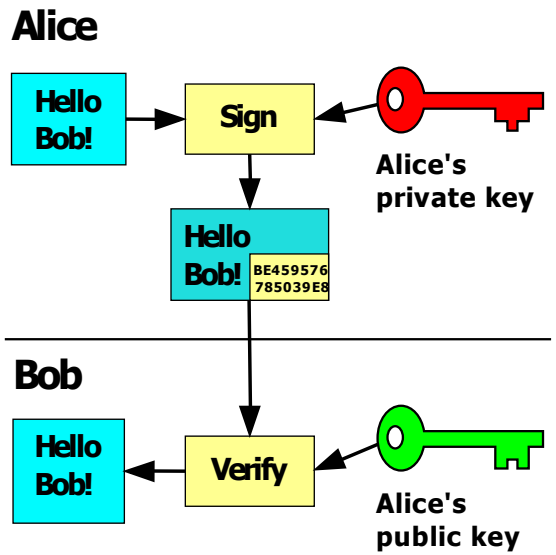


Source: Setupad, "*What is an SSL Certificate and Why Does Your Website Need It?*", 5th May 2022

PUBLIC AND PRIVATE KEY

- Use of two keys
  - Private key for user only
  - Public key for all others
- Can be used to send data
  - Public key encrypt → private key decrypt
- Can be used to sign documents and emails
  - Private key creates signature → public key verifies

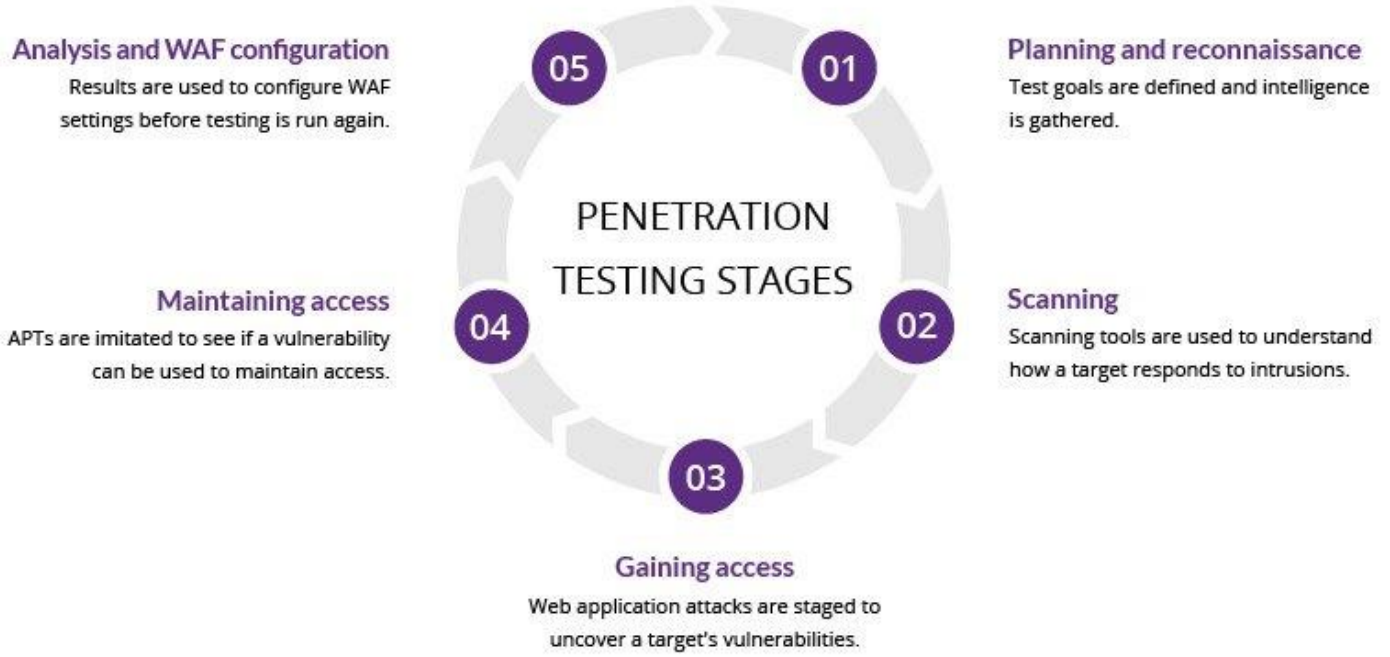




Source: Wikipedia, "*Public-key cryptography*"

PRE-EMPTIVE PROTECTION

- Pen testing – Penetration testing
- Security exercise to find and exploit vulnerabilities
  - Cybersecurity experts with authorisation
  - No prior knowledge of system
- Can be utilised for security audits
  - Check if system is secure
  - What needs to be corrected
  - "Find vulnerabilities before hackers do"



Source: Imperva, "*Penetration Testing*"

PEN TESTING TOOLS

- Multiple exist with different advantages
  - Linux is a "pen testing OS"
  - Wireshark for network observation
  - Nmap for network port checking

- Portable multi tech device → Flipper Zero
  - Sub-Zero communication, RFID, NFC, GPIO, iButton, …
  - Dangerous in wrong hands!

Source: Wikipedia, "*Public-key cryptography*"

II. CYBER AWARENESS

KNOWLEDGE

- Knowledge is powerful
  - Be aware of how system function
  - Know what threats exist

- General concept → "*Error is generally between the chair and keyboard*"
  - Goal to reduce possibility
  - Removes is impossible as mistakes can happen

PASSWORDS

- Most common authentication method
- Complexity relative to length and contents
  - Automatic brute-forcing methods
  - Dictionary based methods
- Better to have strong difficult password
  - Password managers → KeePassXC

	4 letters	8 letters	12 letters
[a-z]	456 976	208.8×10^{9}	9.5×10^{16}
[a-zA-Z]	7 311 616	7.2×10^{13}	6.1×10^{20}
[a-zA-Z0-9]	16 777 216	2.8×10^{14}	4.7×10^{21}
[a-zA-Z0-9+12 symbols]	33 362 176	1.1×10^{15}	3.7×10^{22}

PASSWORD COMPLEXITY

- Simple password → **cyber**
  - **0.1 seconds** to crack
- Longer password → **cybersecurity**
  - **54 seconds** to crack
- Adding letter variations → **CyberSecurity**
  - **3.6 minutes** to crack
- Adding numbers → **Cyb3rSecurity**
  - **7.2 minutes** to crack
- Adding symbols → **Cyb3rS3cur1ty#**
  - **11 hours** to crack
- More symbols → **Cyb3rS£cur!ty#**
  - **8 000 years** to crack

PASSWORDS

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

Source: Hive Systems. "Are your passwords in the green?", April 2018

THINGS TO REMEMBER

- Emails → Check source email
  - If not recognised → Ignore
- Links → DO NOT CLICK from unknown email
  - Check link first → If a known website AND CORRECT then ok
- Files → DO NOT DOWNLOAD suspicious files
  - Simply ignore
- Websites → Check if padlock present
  - If not present but should be → Leave immediately

- Always contact IT department
  - If done any of above → Inform and change all passwords

CONSTANT VIGILENCE

Everyone has a part to play

Do yours!