Chapitre 2

Les principales attaques sécuritaires

Rappel sur la sécurité informatique

- La sécurité informatique est un concept qui englobe la protection/sécurité globale:
  - des systèmes informatiques
  - Réseaux
  - Applications
  - Données
  - matériels
  - infrastructures contre toute forme de menace, qu'elle soit numérique, physique, humaine ou organisationnelle.

Domaines de la sécurité informatique

Sécurité des données

Sécurité des systèmes embarqués

Sécurité des SE

Sécurité réseau et infrastructure

Types de sécurité informatique

des endpoints (terminaux)

Sécurité physique

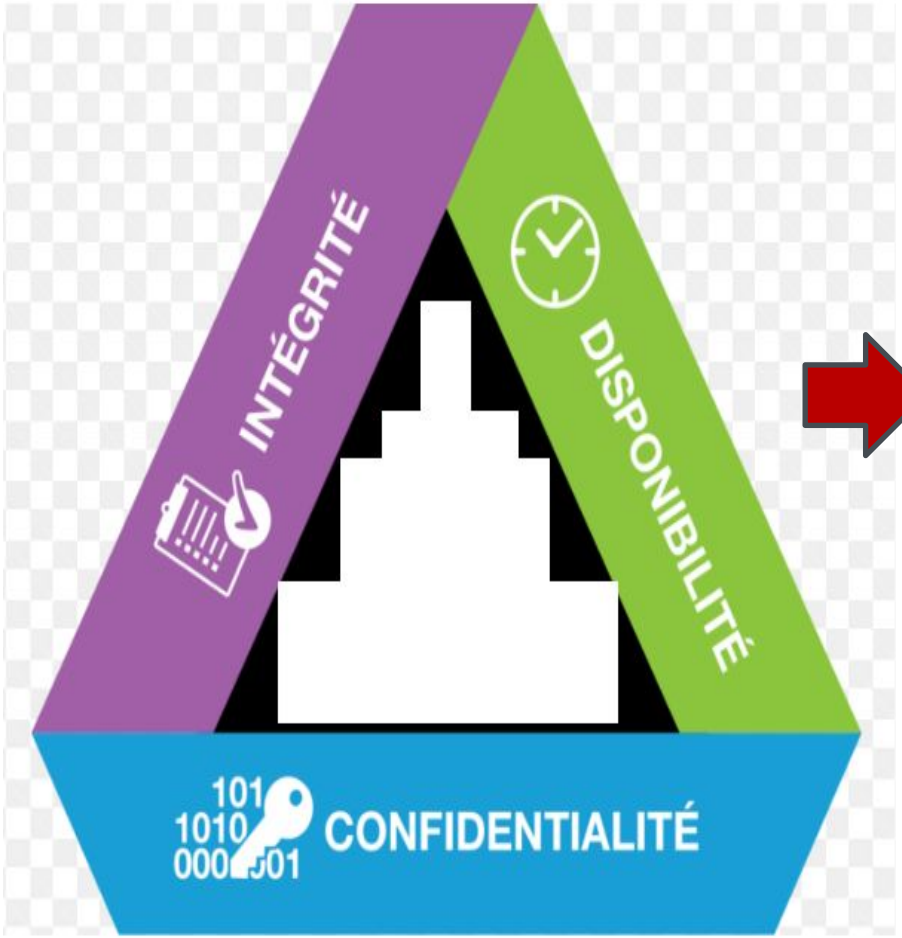
Sécurité d'application

Sécurité opérationnelle

Sécurité opérationnelle

cybersécurité

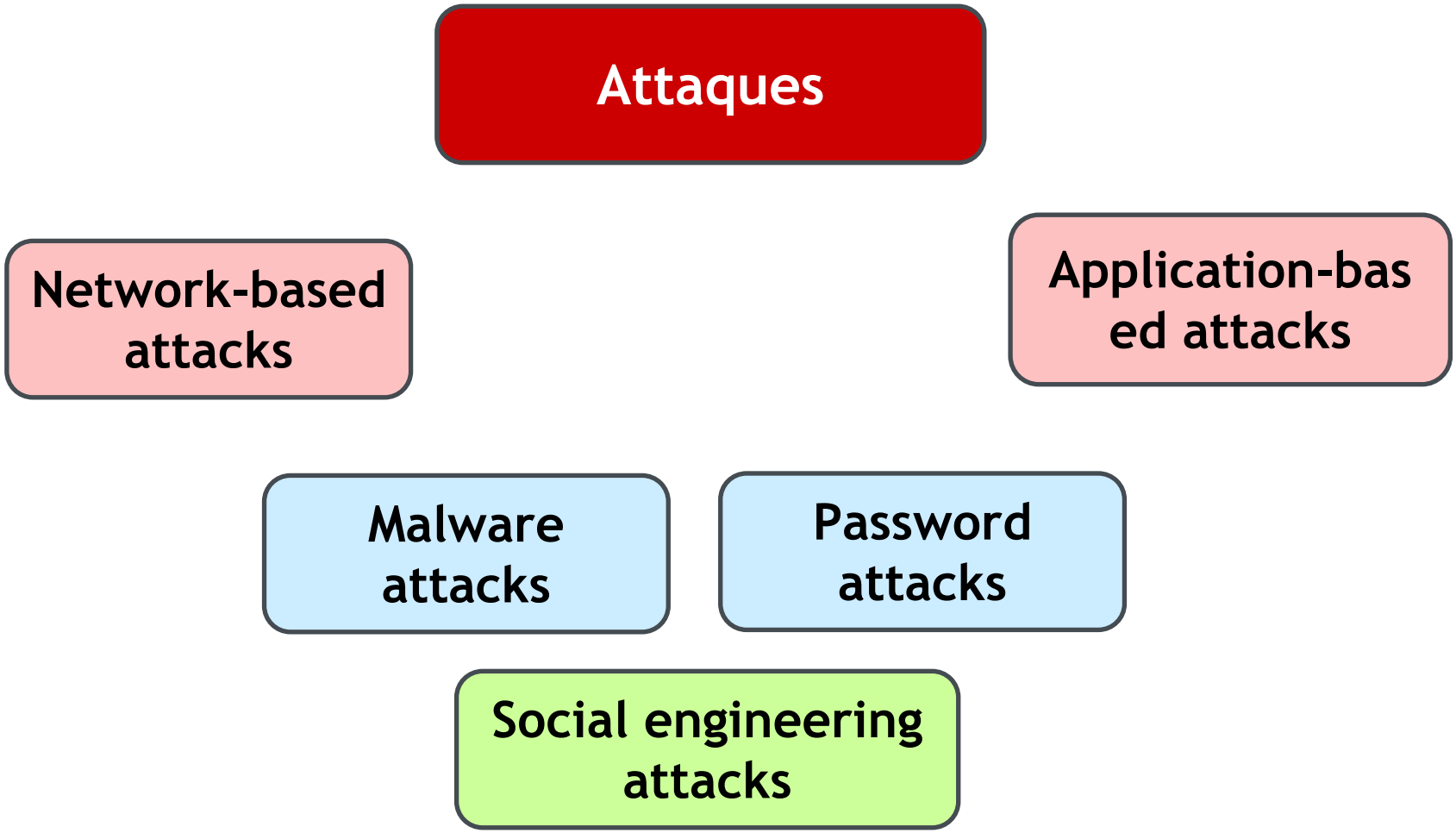
Rappel: Principes fondamentaux de la sécurité informatique



- Authentification
- Non-répudiation
- Gestion des risques

Figure 1

Attaques sécuritaires



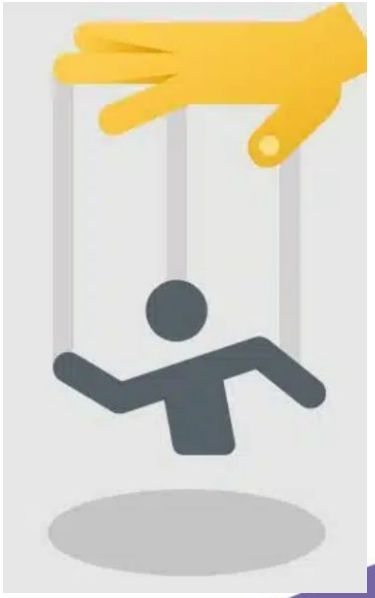
Social engineering attacks: What is social engineering?

- Social engineering is the use of psychological manipulation and deception to influence individuals or groups to divulge sensitive information or to perform actions that may not be in their organization's best interest

- It is **one of the most common** tactic used by cybercriminals **to gain access to sensitive information**, such as login credentials or financial information and was responsible for 255 million attacks in the first six months of 2022 alone

Social Engineering

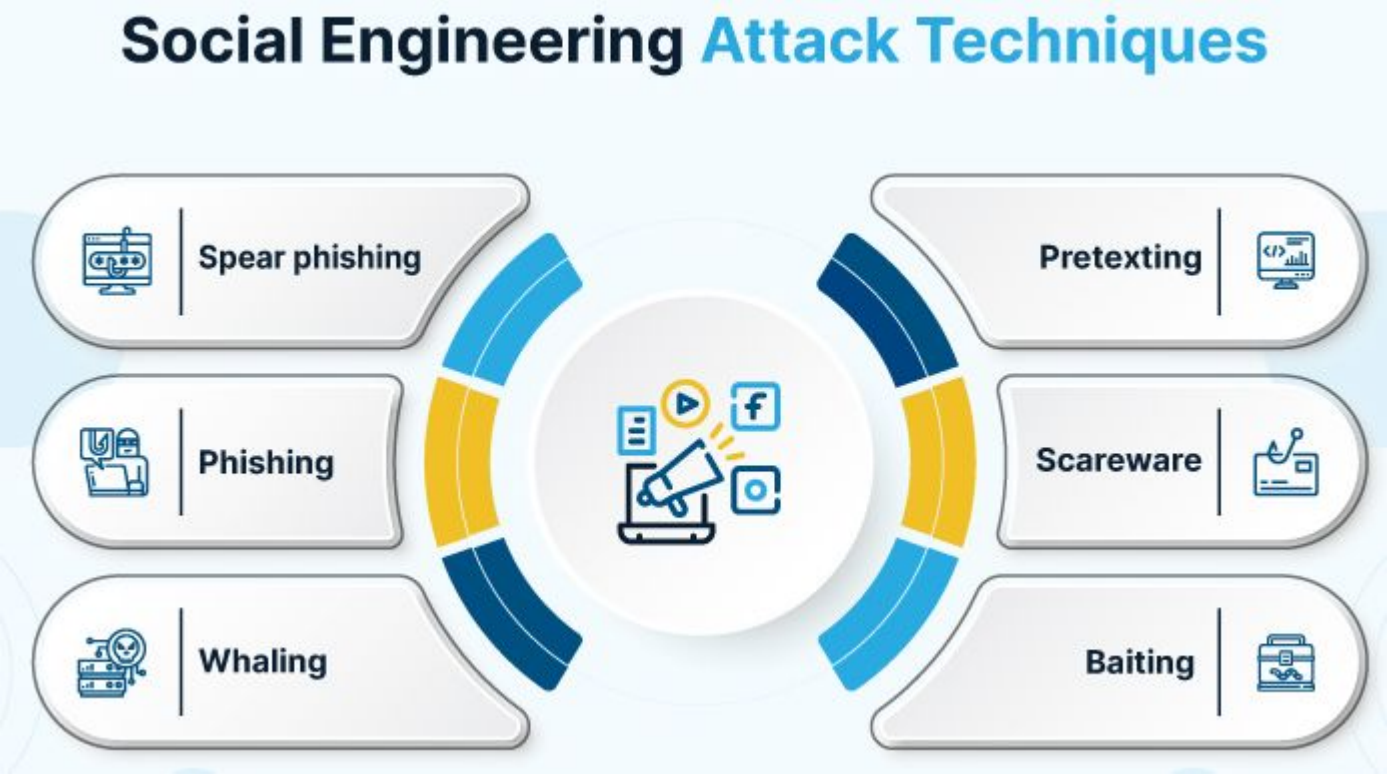
The Art of Human Manipulation



Social engineering attacks

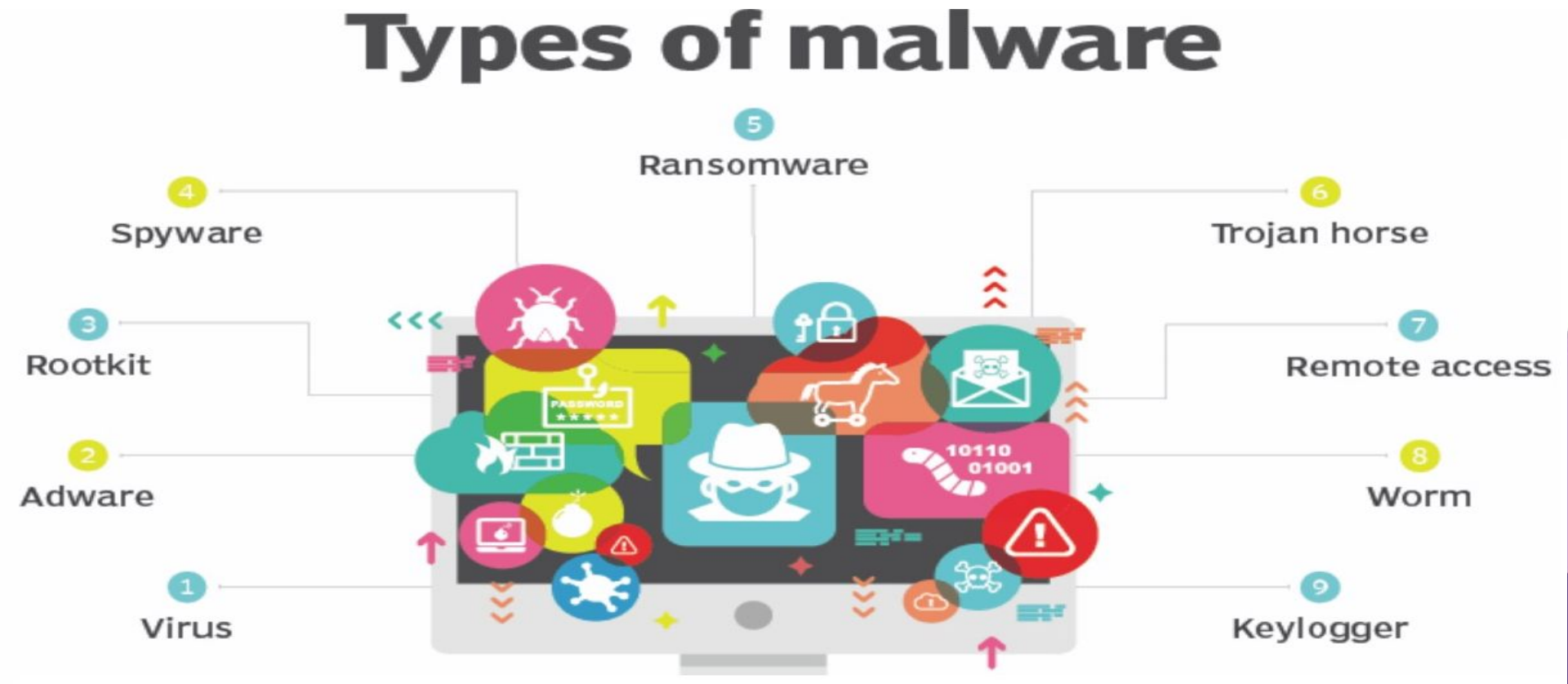
- Cyber threats and attacks are becoming more common than anything else as hackers are becoming more advanced and skilled. These attacks are based on two approaches: technical expertise and human psychology. Social engineering utilizes the latter. Responsible for endless hassle and nuisance, it is more about a human-error process than technical expertise

The most frequent



Malware attacks (1)

- **Malicious software, or malware** is one of the most significant categories of threats to computer systems
- A malware is defined as *"a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim."*



Malware attacks (2)

- **Viruses:** it is a malicious code that replicates itself (or an evolved copy of itself) without any human intervention. A virus cannot be spread without a human action (such as running an infected file or program

File extension	Description
.DOCX, .XLSX	Microsoft Office user documents
.EXE	Executable program file
.MSI	Microsoft installer file
.MSP	Windows installer patch file
.SCR	Windows screen saver
.CPL	Windows Control Panel file
.MSC	Microsoft Management Console file
.WSF	Windows script file
.REG	Windows registry file
.PS1	Windows PowerShell script

Windows file types that can be infected

Malware attacks (3)

- **A worm** is designed to take **advantage of vulnerability** in an application or an operating system on the host computer. Once the worm has exploited the vulnerability on one system, it immediately searches for another computer on the network that has the same vulnerability
- **Note:** The main difference between a virus and a worm: A virus will self-replicate on the host computer but not to other computers. A worm will self-replicate between computers (from one computer to another)

- **Trojan horse** (or just Trojan) is an executable program that masquerades as performing a benign activity but also does something malicious. For example, a user may download what is advertised as a calendar program, yet when it is installed, in addition to installing the calendar it also installs malware that scans the system for credit card numbers and passwords, connects through the network to a remote system, and then transmits that information to the attacker

Malware attacks (4)

Action	Virus	Worm	Trojan
What does it do?	Inserts malicious code into a program or data file	Exploits a vulnerability in an application or operating system	Masquerades as performing a benign action but also does something malicious
How does it spread to other computers?	User transfers infected files to other devices	Uses a network to travel from one computer to another	User transfers Trojan file to other computers
Does it infect a file?	Yes	No	It can
Does there need to be user action for it to spread?	Yes	No	Yes

Difference between viruses, worms, and Trojans

- **Adware:** delivers advertising content in a manner that is unexpected and unwanted by the user. Once the adware malware becomes installed, it typically displays advertising banners, popup ads, or opens new web browser windows at random intervals
- Adware may display objectionable content, such as gambling sites or not respectable content.
- Frequent popup ads can interfere with a user's productivity. Popup ads can slow a computer or even cause crashes and the loss of data. Unwanted advertisements can be a nuisance

Malware attacks (5)

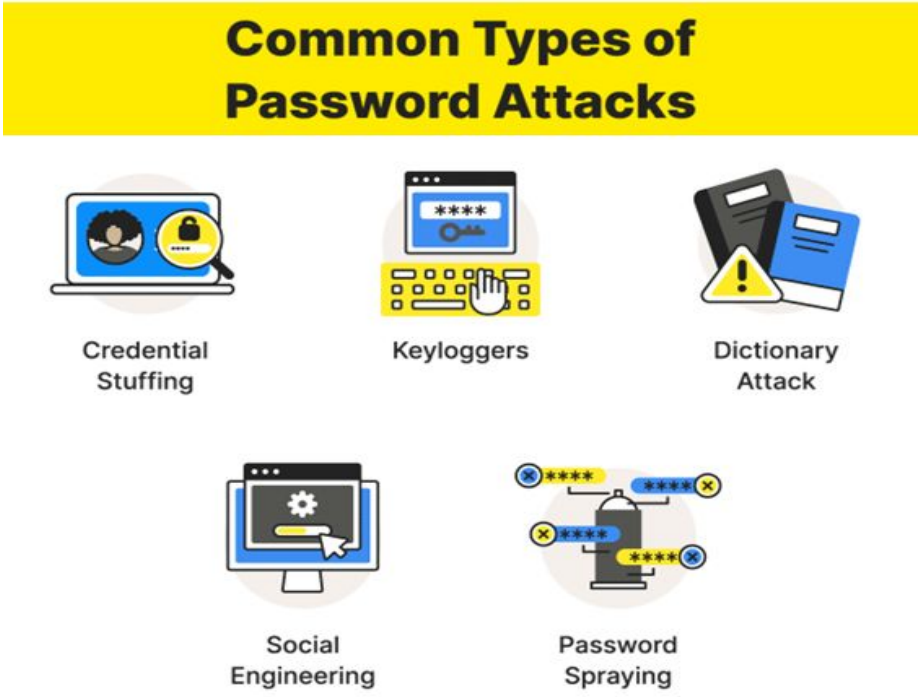
- **Spyware** is a general term used to describe software that secretly spies on users by collecting information without their consent
  - The Anti-Spyware Coalition defines spyware as tracking software that is deployed without adequate notice, consent, or control by the user
  - This software uses the computer's resources, including programs already installed on the computer, for the purpose of collecting and distributing personal or sensitive information.

Malware attacks (6)

- **Ransomware** One of the newest and fastest-growing types of malware is ransomware. Ransomware prevents a user's device from properly operating until a fee is paid. One type of ransomware locks up a user's computer and then displays a message that purports to come from a law enforcement agency

Password attacks (1)

- Password based attacks are among the most common types of cyberattacks
- **An attacker** uses one of several methods to try to steal or crack passwords to access your personal or organization's data.



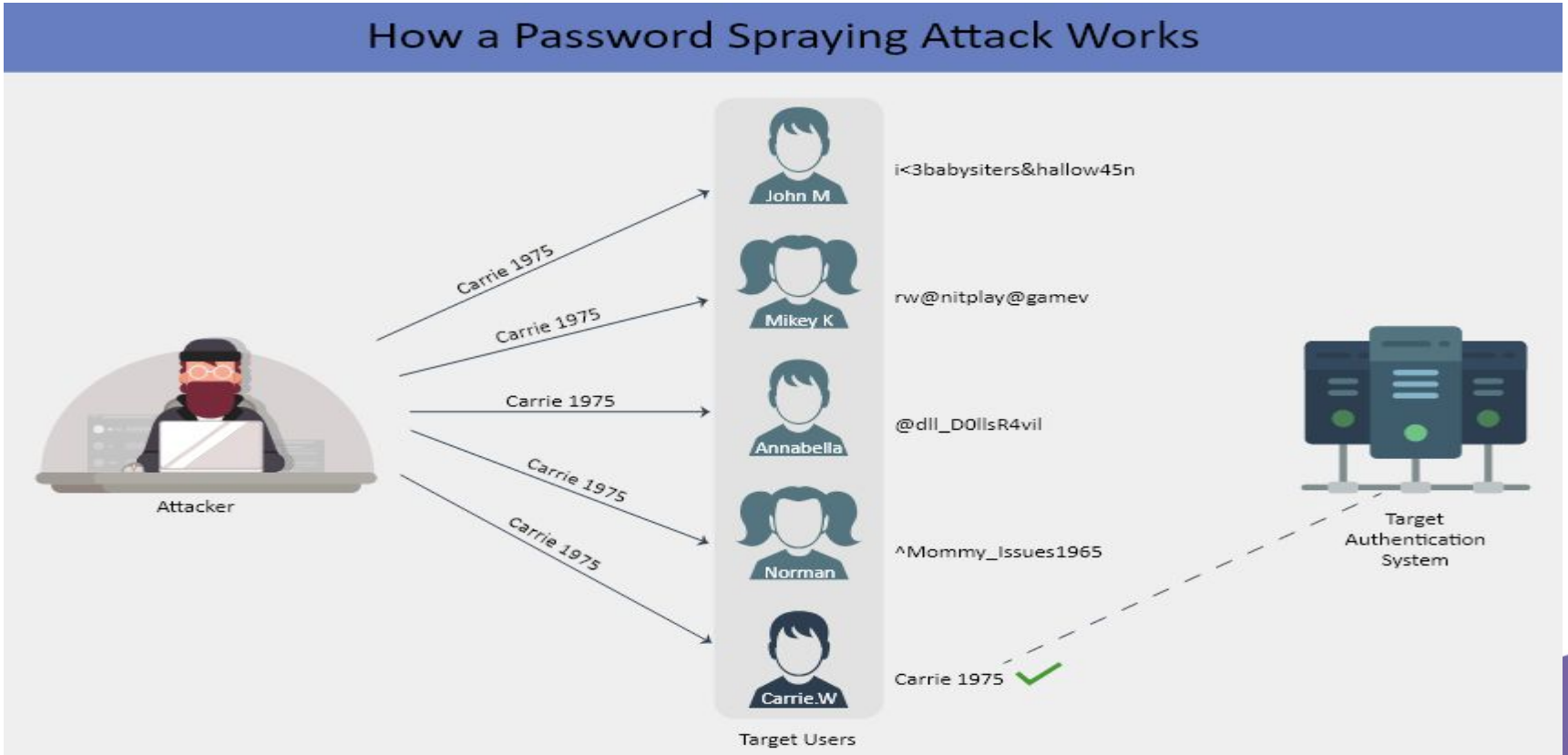
Password attacks (2)

- **Phishing attacks:** are among the most common types of password attacks. Hackers typically send an email pretending to be someone else to get users to download malicious attachments or click on malicious links that take them to fake login pages
- Cybercriminals can also use this login spoofing to get victims to unintentionally give up their access credentials

- **Brute Force Attack:** Brute force attacks are one of the easiest and most commonly seen login attack methods. Attackers use this trial-and-error tactic to guess login credentials, encryption keys or to find hidden web pages. Put simply, hackers try all the possible combinations in the hope of finding the correct solution. Depending on the complexity and length of the password, it can take from a few seconds to years to crack the password

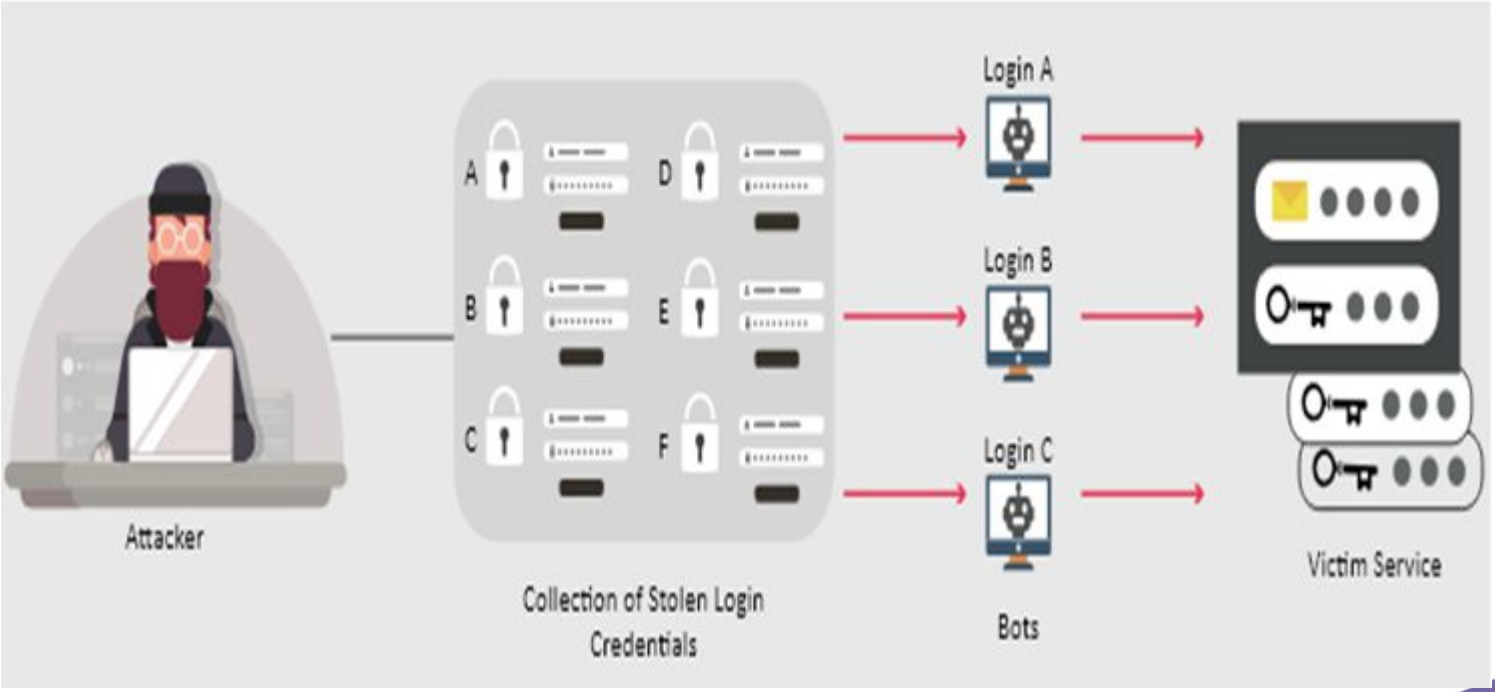
Password attacks (3)

- **Password Spraying Attacks:** the attacker uses a single commonly used password, like 12345 or Password123, to attempt to gain access to all the accounts on their list. They try it against a list of usernames to see if any match. After trying the password with all the usernames, they move on to the second password, then the third, and so on, repeating the process as they go.



Password attacks (4)

- **Credential Stuffing Attacks:** Credential stuffing is a login attack where hackers use the organization's stolen login credentials, often purchased from the dark web or shared on another online forum, and try to access other accounts within the organization
- Likewise, attackers use a combination of different passwords and usernames they've gained through data breaches that they've carried out themselves



Password attacks (5)

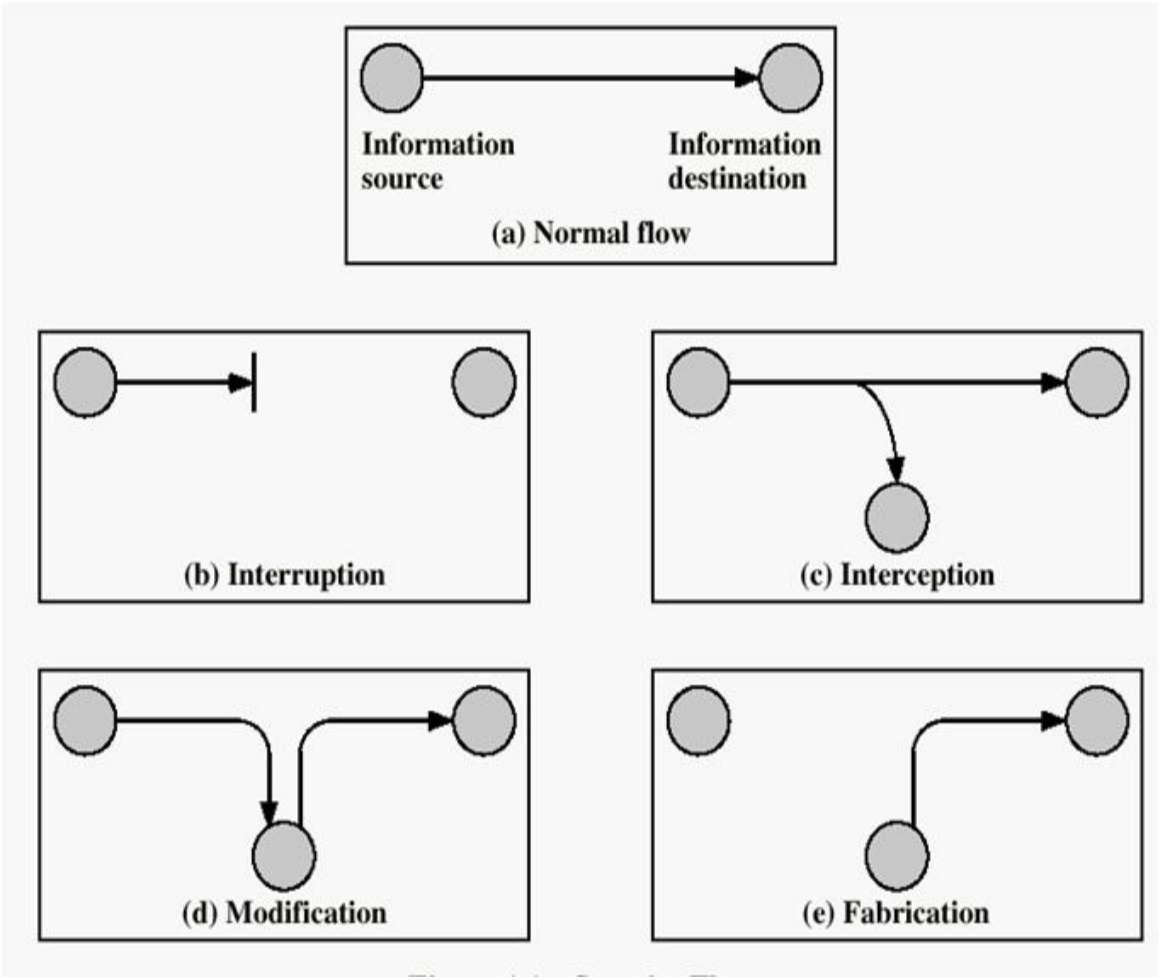
- **Keylogger Attacks** As the name implies, a keylogger attack is an attack where an attacker logs the user's keystrokes
  - **it records all the input that comes from a keyboard without the user's knowledge**
  - An attacker can utilize software or hardware to perform a keylogger attack. Software keyloggers are often installed by hackers getting users to click on malicious links or open attachments.

Network-based attacks

Les attaques basées sur le réseau sont des attaques qui exploitent:

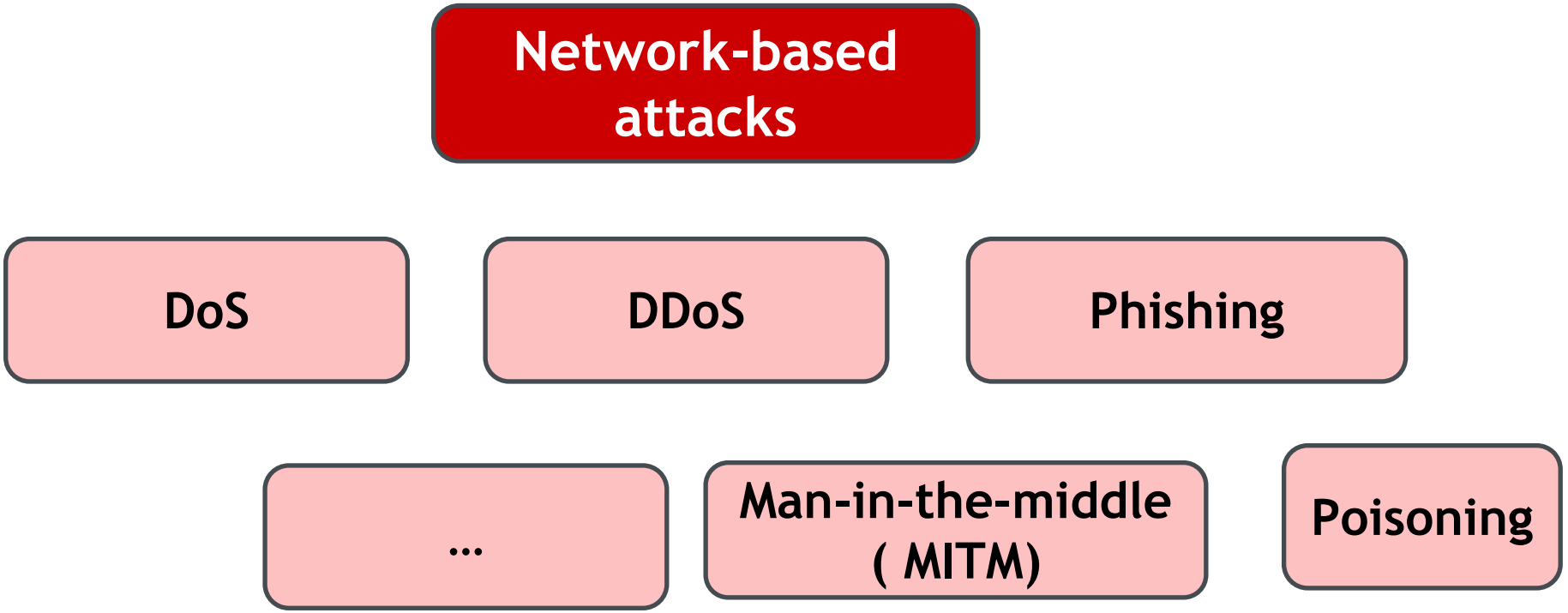
- les failles des infrastructures de communication
- des protocoles réseau pour perturber les services, intercepter des données ou manipuler les échanges entre systèmes

Network-based attacks & CIA principles



- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

Main network-based attacks

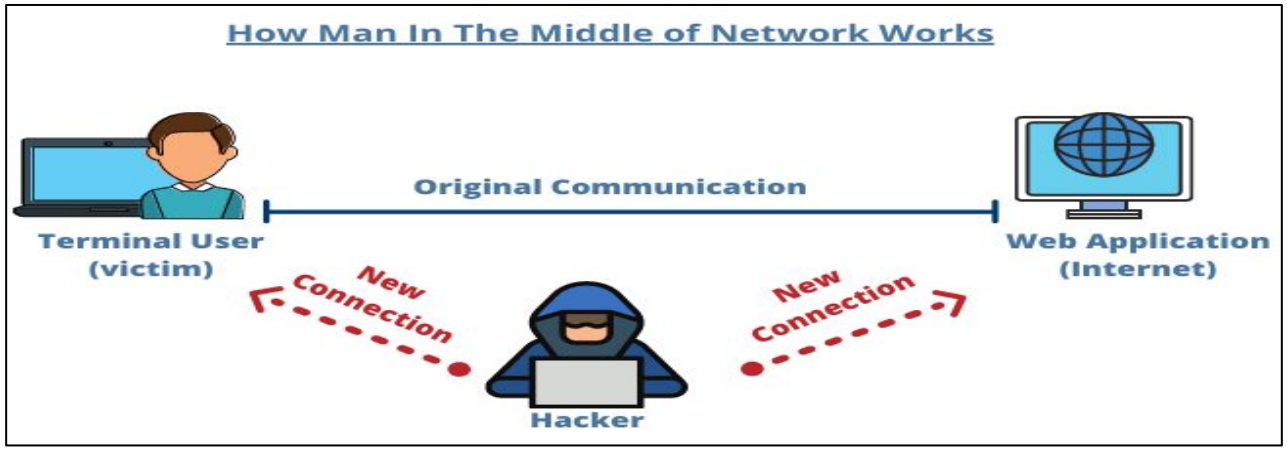


Phishing/Hameçonnage

- Le phishing prend souvent la forme d'un e-mail ou d'un message qui semble provenir d'une source fiable (banque, administration, entreprise reconnue). L'objectif est de pousser la victime à cliquer sur un lien frauduleux, à ouvrir une pièce jointe malveillante, ou à fournir volontairement des informations personnelles (identifiants de connexion, mots de passe, coordonnées bancaires, ou autres données confidentielles,..) sur un faux site web qui imite un site légitime

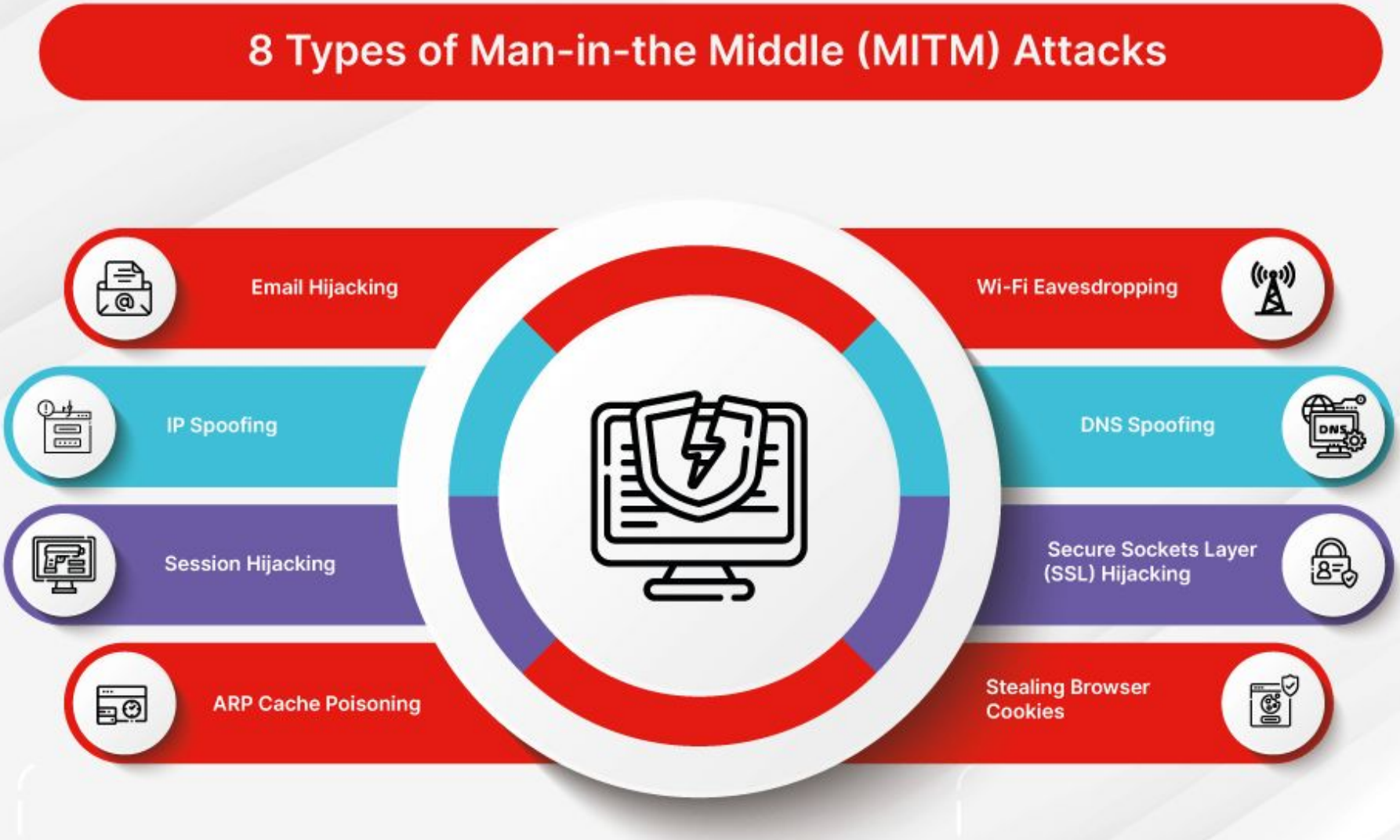
Man-in-the-middle attack (MITM) (1)

- Une attaque MITM est une cyberattaque au cours de laquelle un pirate informatique vole des informations sensibles en écoutant les communications entre deux cibles **en ligne**



- Comment fonctionne une attaque de type MITM?
  - Les vulnérabilités des réseaux, des navigateurs web, des comptes de messagerie, du comportement des utilisateurs et des protocoles de sécurité sont le point de départ des attaques de type MITM
  - Le **phishing** est une voie d'entrée courante pour les attaquants MITM

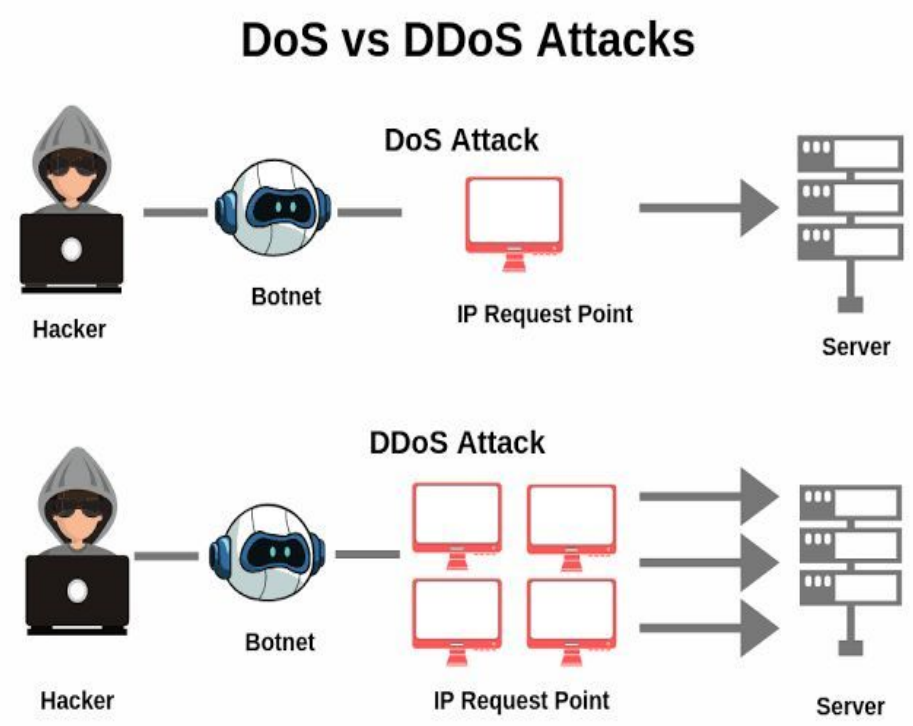
Man-in-the-middle attack (MITM) (2)



Denial-of-Service (DoS) & DDoS attacks (1)

- Les attaques par déni de service (DoS) ou déni de service distribué (DDoS) consistent à **inonder** une ressource en ligne (un site Web, un service cloud …) de demandes de connexion frauduleuses ou d'autres types de trafic malveillant
- Incapable de gérer ce trafic, la cible **ralentit** ou **tombe en panne**, ce qui la rend inaccessible pour les utilisateurs légitimes

- **Différence entre attaques DoS & DDoS**
  - La principale différence est que pour le premier l'attaque vient d'un **seul** système, tandis que pour le second implique **plusieurs** systèmes simultanément



Denial-of-Service (DoS) & DDoS attacks (2)

- **Types d'attaques DoS et DDoS**
  - **Attaque Teardrop:** Une attaque Teardrop est une attaque DoS qui envoie d'innombrables fragments de données de protocole Internet (Internet Protocol, IP) à un réseau. Lorsque le réseau tente de recompiler les fragments dans leurs paquets d'origine, il n'y parvient pas
  - **Attaque par saturation:** elle consiste à envoyer plusieurs demandes de connexion à un serveur, mais ensuite ne répond pas pour établir la liaison
  - **Attaque volumétrique:** elle consiste à consommer la bande passante en vain. Par exemple, l'attaquant utilise un réseau zombie pour envoyer un volume élevé de paquets de requêtes à un réseau, submergeant sa largeur de bande de requêtes d'écho d'Internet Control Message Protocol (ICMP). Cela entraîne un ralentissement ou même l'arrêt total des services.

Denial-of-Service (DoS) & DDoS attacks (3)

- **Comment améliorer la protection contre les attaques DDoS & DoS**
  - Surveiller le réseau en permanence pour identifier les modèles de trafic normaux et anormaux
  - Effectuer des tests pour simuler des attaques DoS : cela permettra d'évaluer les risques, d'exposer les vulnérabilités et de former les employés à la cybersécurité.
  - Créer un plan de protection
  - Identifier les systèmes critiques et les modèles de trafic normaux: les premiers permettent de planifier la protection et les seconds permettent la détection précoce des menaces.
  - Prévoir une largeur de bande supplémentaire : elle n'arrêtera peut-être pas l'attaque, mais elle aidera le réseau à faire face aux pics de trafic et à réduire l'impact de toute attaque.

Attaque par empoisonnement ARP (1)

- Une attaque de "poisoning" désigne diverses actions malveillantes qui visent à corrompre ou à manipuler des données ou des systèmes

- **Objectif**
  - Perturber les systèmes, détourner le trafic réseau, voler des informations ou de rediriger des utilisateurs vers des sites frauduleux, …

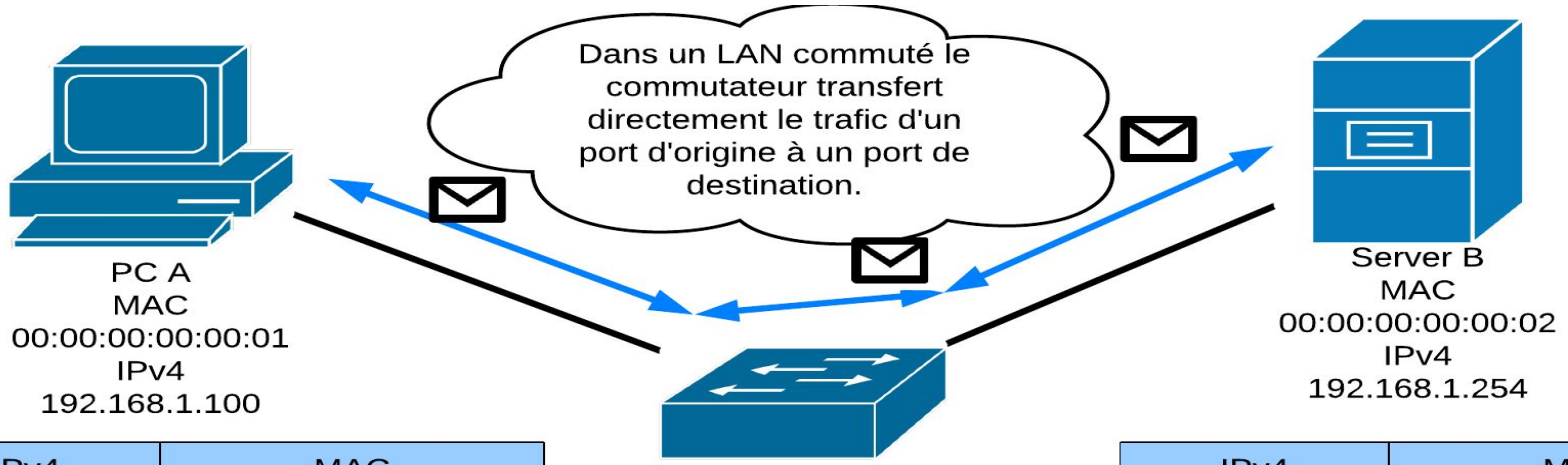
- **Types d'attaques par empoisonnement**
  - **empoisonnement de données :** introduisant des informations fausses et nuisibles
  - **Empoisonnement ARP** : exploitant des faiblesses dans des protocoles de communication
  - **Empoisonnement de cache :** injectant des contenus malveillants dans des caches

Attaque par empoisonnement ARP (2)

- **Empoisonnement ARP (ARP Poisoning) :** c'est une attaque qui exploite les faiblesses du protocole ARP
  - **Objectif :** Modifier le tableau des correspondances d'adresses IP et MAC d'un réseau local (LAN)
  - **Exemple :** L'attaquant envoie de faux messages ARP à la passerelle réseau, ce qui lui permet **d'intercepter** et **de modifier** tout le trafic réseau passant par lui pour un utilisateur ciblé.

Attaque par empoisonnement ARP (3)

- Fonctionnement normal de ARP



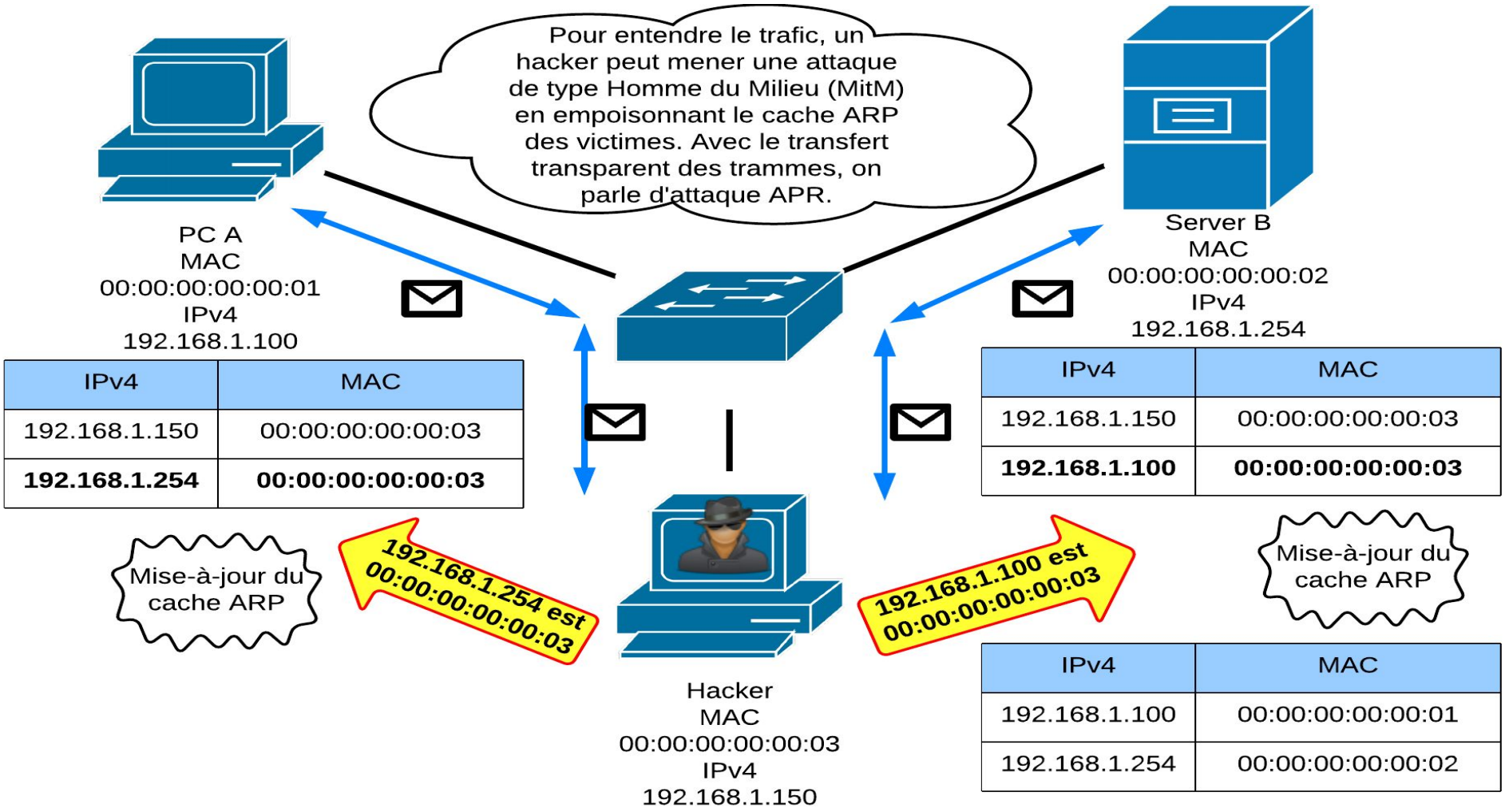
IPv4	MAC
192.168.1.254	00:00:00:00:00:02
192.168.1.150	00:00:00:00:00:03

IPv4	MAC
192.168.1.100	00:00:00:00:00:01
192.168.1.150	00:00:00:00:00:03

IPv4	MAC
192.168.1.100	00:00:00:00:00:01
192.168.1.254	00:00:00:00:00:02

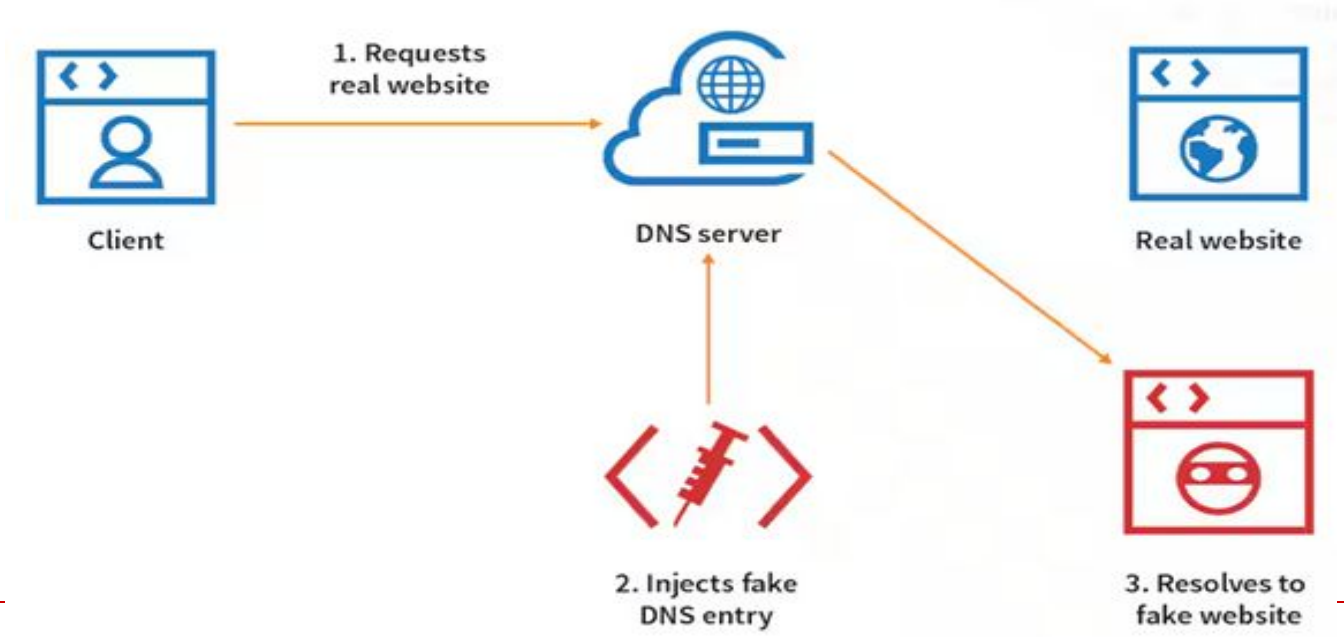
Attaque par empoisonnement ARP (4)

Attaque par empoisonnement ARP



Attaque par empoisonnement du cache DNS (DNS Cache Poisoning)

- Dans une attaque par empoisonnement du cache DNS, les auteurs de la menace utilisent différentes techniques pour remplacer les adresses légitimes dans un cache DNS par de fausses adresses DNS.
- Lorsque les utilisateurs tentent de consulter un site légitime, le résolveur DNS renvoie **la fausse adresse** dans son cache, détournant la session du navigateur et envoyant l'utilisateur vers un **faux site Web** ou un **site Web malveillant**.



Application-based attacks

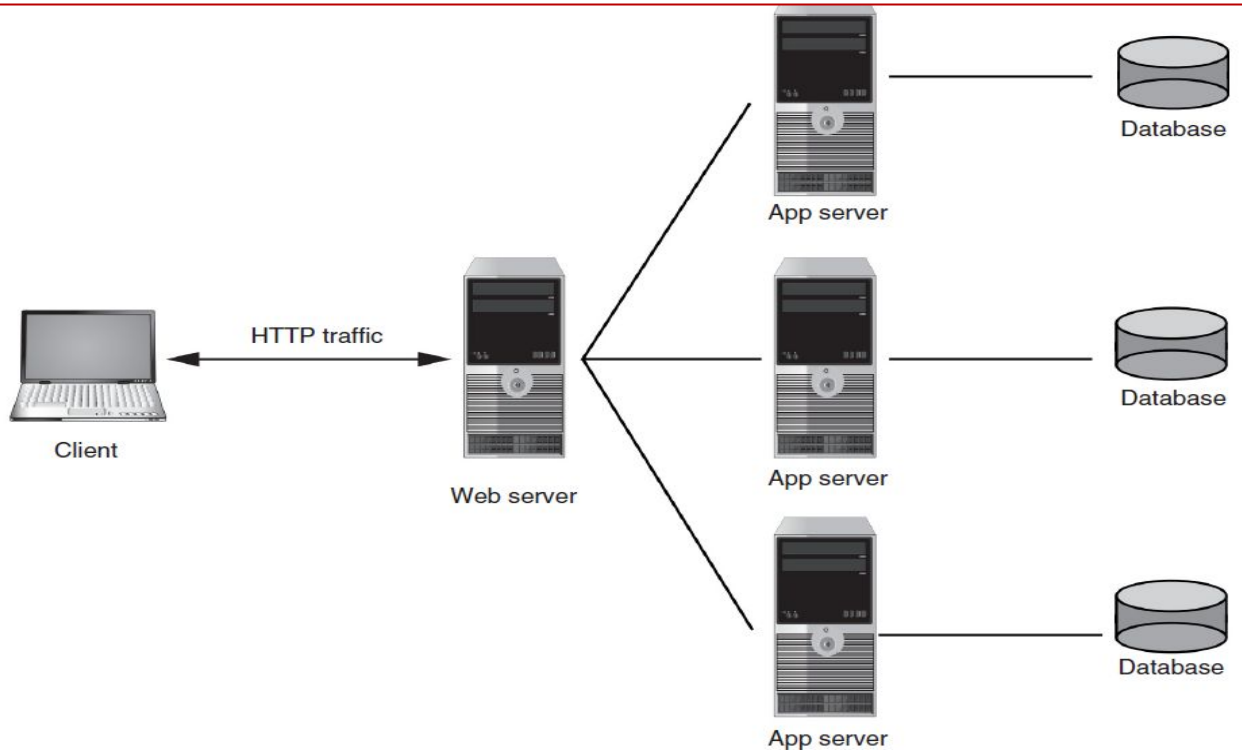
A typical Server-side Web application infrastructure

An important characteristic of server-side web applications is that they create dynamic content based on inputs from the user. For example, a webpage might ask a user to enter her zip code in order to receive the latest weather forecast for that area. Thus the dynamic operations of a web application depend heavily upon inputs provided by users.

Securing server-side web applications is often considered more difficult than protecting other systems. First, although traditional network security devices can block traditional network attacks, they cannot always block web application attacks. This is because many traditional network security devices ignore the *content* of HTTP traffic, which is the vehicle of web application attacks. Second, many web application attacks (as well as other application attacks) exploit previously unknown vulnerabilities. Known as **zero-day attacks**, these attacks give victims no time—zero days—to defend against the attacks. Finally, by design the dynamic server-side web applications accept user input, such as the zip code of the region for which a weather forecast is needed. Most other systems would categorically reject any user input as potentially dangerous, not knowing if the user is a friend or foe.

A typical Server-side Web application infrastructure

A typical dynamic web application infrastructure is shown in Figure 2. The client's web browser makes a request using the Hypertext Transport Protocol (HTTP) to a web server, which may be connected to one or more web application servers. These application servers run the specific "web apps," which in turn are directly connected to databases on the internal network. Information from these databases is retrieved and returned to the web server so that the dynamic information can be sent back to the user's web browser.



Attaques sécuritaires

Many server-side web application attacks target the input that the applications accept from users. Such common web application attacks are cross-site scripting, SQL injection, XML injection, and command injection/directory traversal.

Application-based attacks

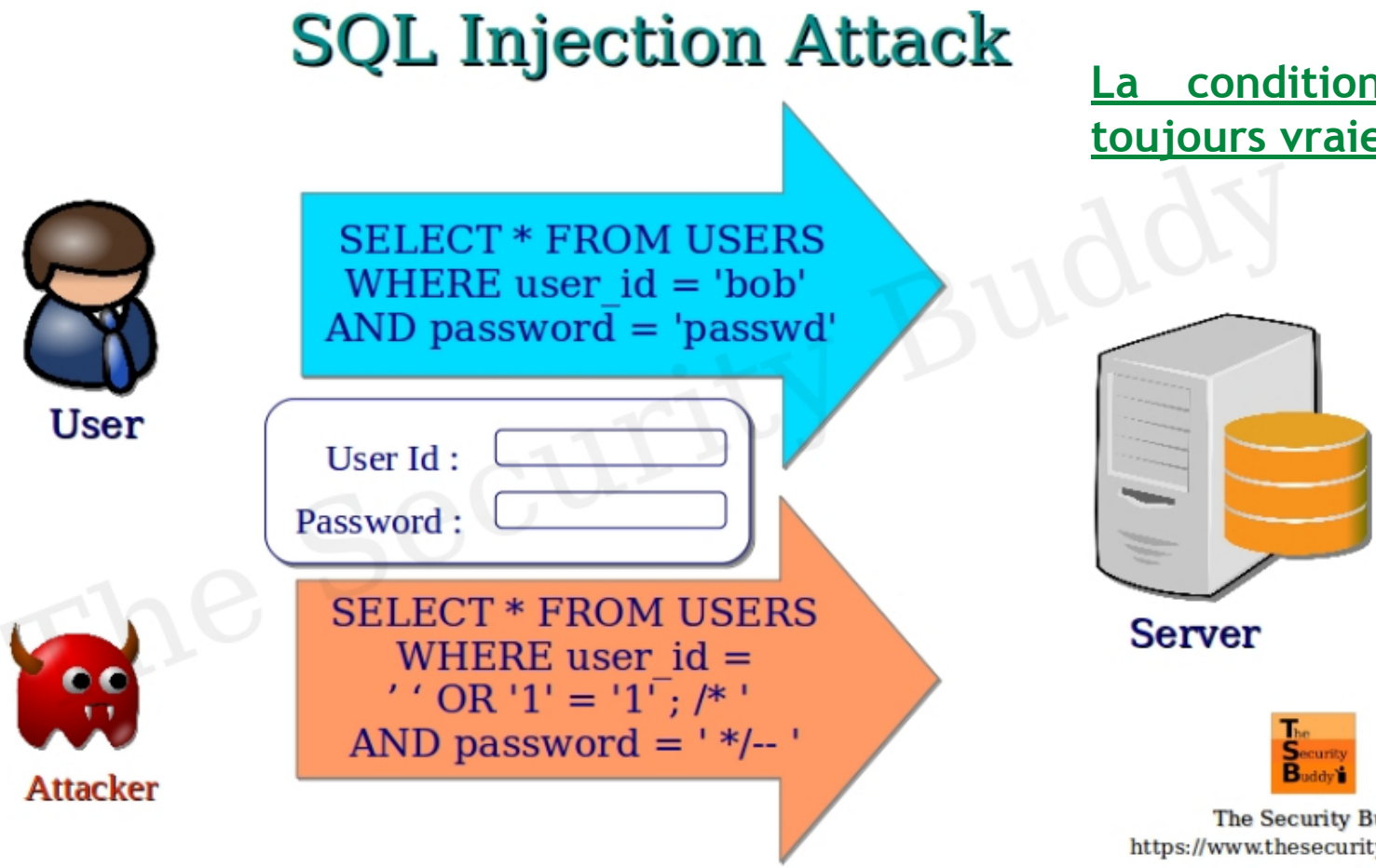
- SQL Injection
- Cross-Site Scripting (XSS)
- Spear phishing/ Phishing ciblé
- Session hijacking
- ...

Injection SQL (1)

- **Injection SQL** (ou attaques par injection de commandes SQL)
  - exploitent les failles de sécurité d'une application qui interagit avec des bases de données.
  - elle consiste à insérer du code SQL malveillant dans les champs de saisie d'une application ou dans les paramètres de requête qui interagissent avec une base de données
  - le hacker peut ainsi accéder à la base de données, mais aussi modifier le contenu et donc compromettre la sécurité du système
  - Cette vulnérabilité exploite un traitement insuffisant ou absent de la validation des entrées utilisateurs, permettant à l'attaquant de manipuler les requêtes SQL exécutées par l'application.

Injection SQL (2)

- Exemple



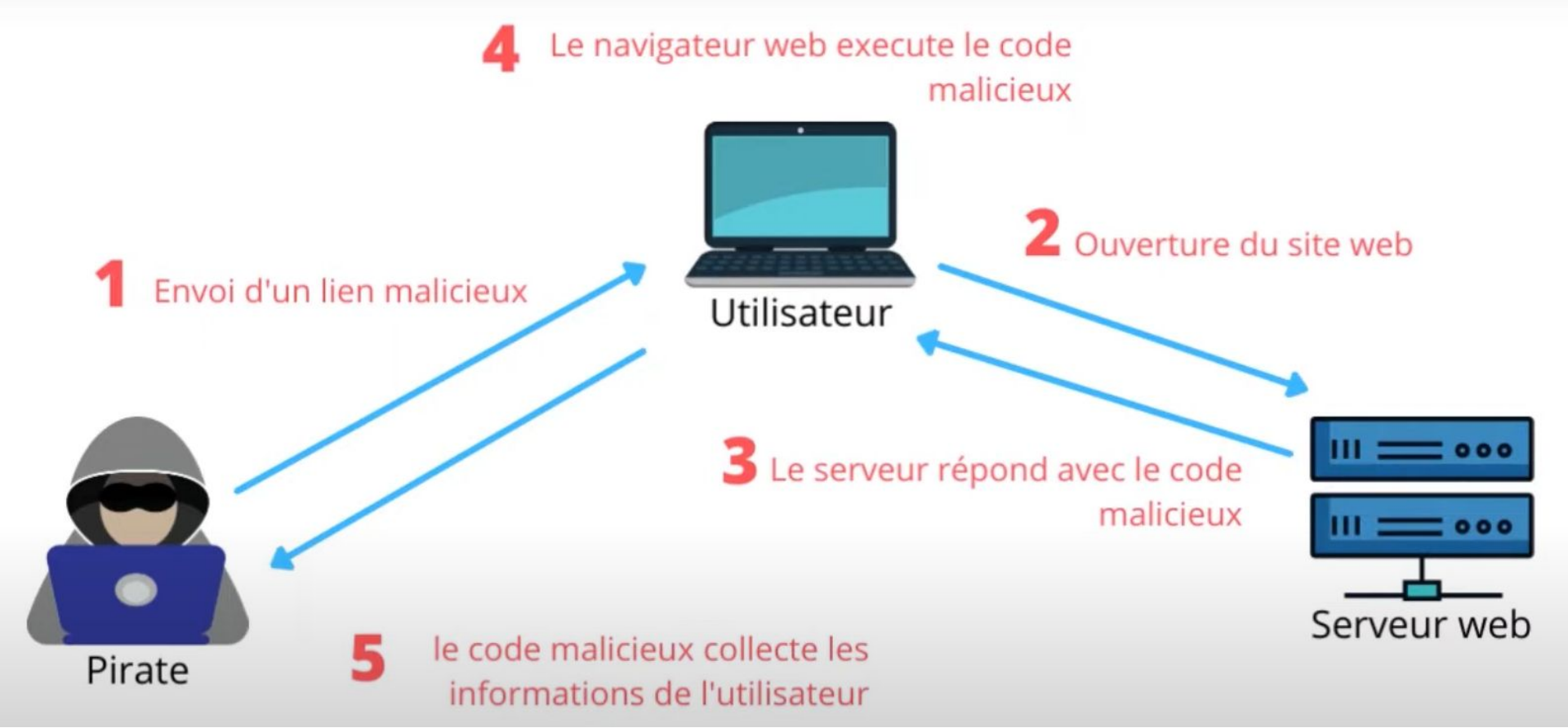
Injection SQL (3)

- **Dégâts possibles**
  - Accès non autorisé aux données sensibles (identifiants, informations personnelles, financières),
  - Modification, suppression, ou ajout de données dans la base,
  - Exécution de commandes d'administration sur la base (suppression de tables, modification des tables, ..),
  - Compromission totale du système si le serveur de base de données est mal sécurisé.

Cross-Site Scripting (XSS) (1)

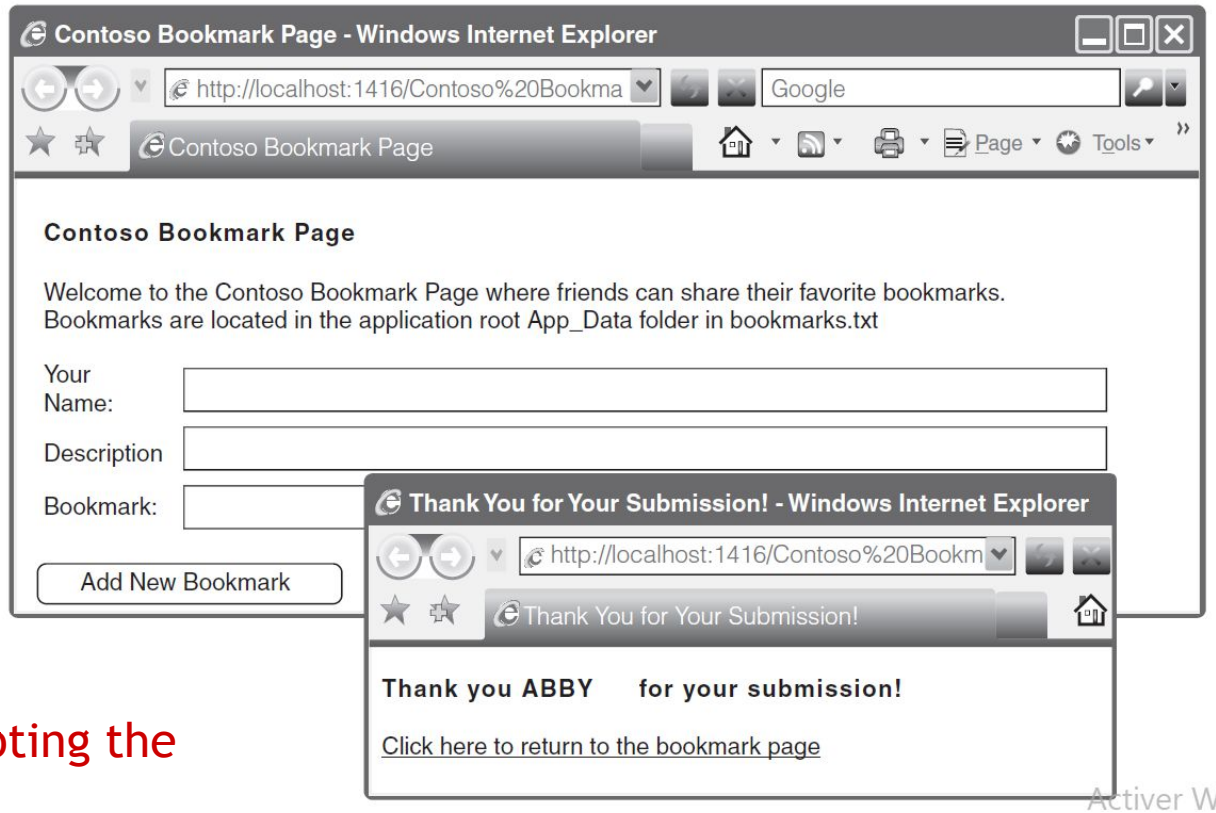
- Une attaque XSS consiste à injecter des scripts malveillants dans un site web légitime pour qu'ils soient exécutés par le navigateur de la victime
- Les conséquences peuvent inclure le vol de données sensibles (cookies, jetons de session), le détournement de sessions utilisateurs, l'installation de malwares ou la défiguration de sites web,..
- Les attaques XSS exploitent des vulnérabilités de validation des entrées utilisateur, et il existe trois principaux types : XSS réfléchi, XSS stocké et XSS basé sur DOM

Cross-Site Scripting (XSS) (2)



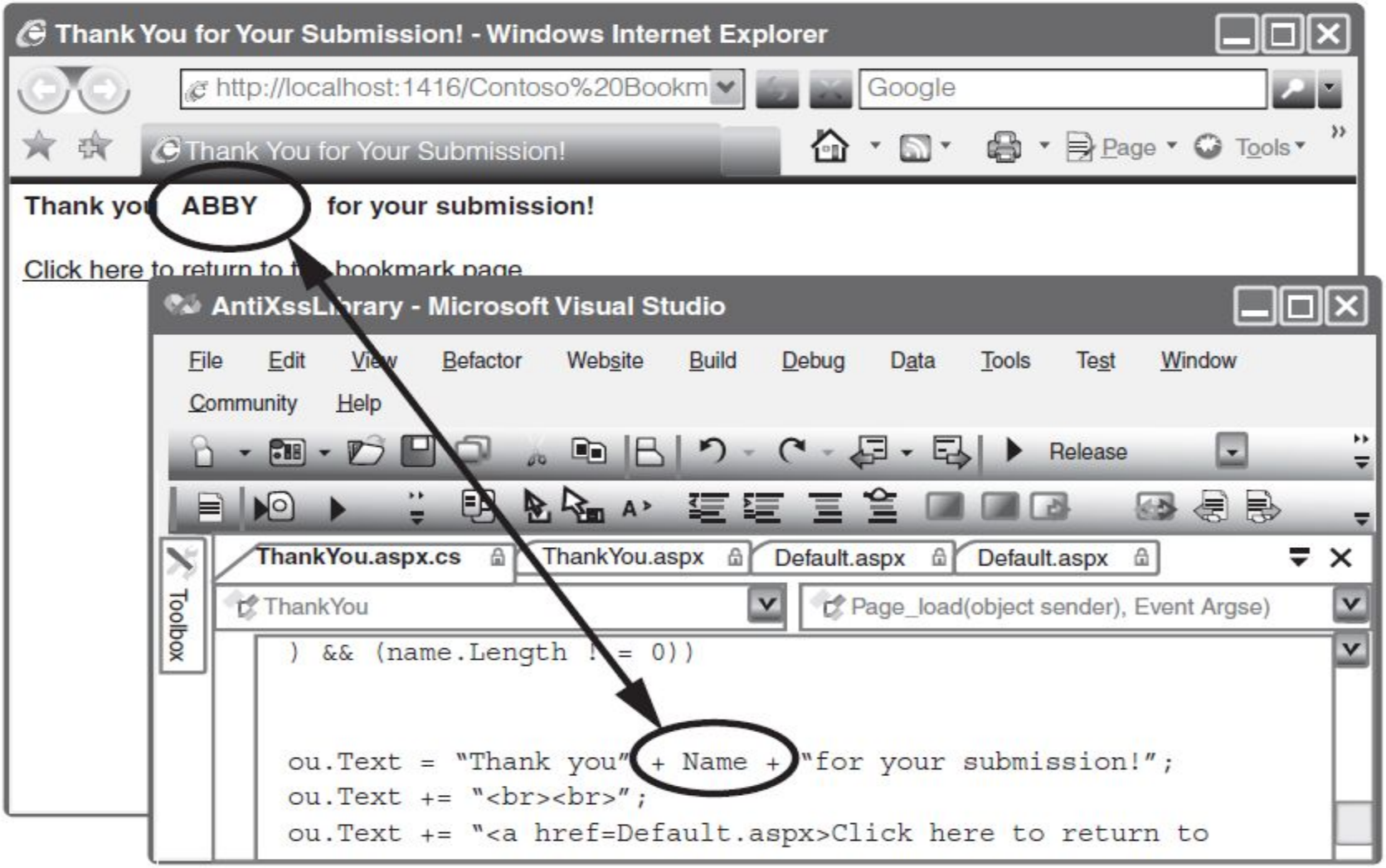
Cross-Site Scripting (XSS) (3)

- Une attaque XSS réquiert que le site web satisfait deux critères: **(1)** il accepte la saisie de données par un utilisateur et **(2)** il utilise ces données dans une réponse
- Exemple de site web acceptant user data input



Bookmark page accepting the user input

Cross-Site Scripting (XSS) (4)



user input used in response

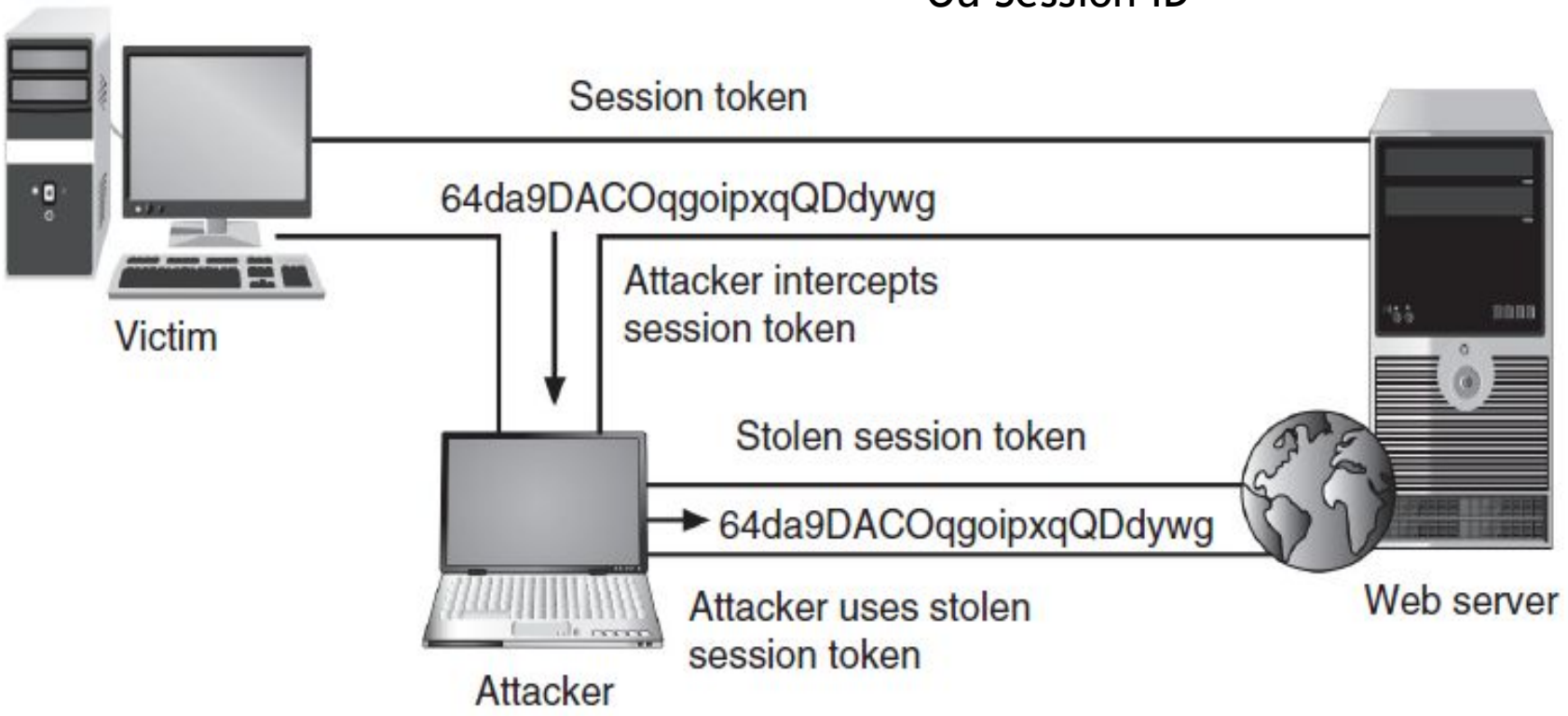
Attaque par Détournement de session/ Session hijacking attack (1)

- Le détournement de session consiste **à détourner** un accès à une plateforme, sans avoir besoin de collecter l'identifiant et le mot de passe associé au compte ▫ **principe de Session ID**
- **Principe de session ID**
  - Lorsqu'un utilisateur se connecte à une plateforme, il reste authentifié pendant **un certain temps** sans qu'il soit nécessaire de saisir ou de retransmettre systématiquement ses identifiants de connexion. Cela est possible, car le serveur maintient une **session active** pour l'utilisateur
  - Pour faire référence à cette session, le serveur décerne à l'utilisateur un identifiant unique appelé **session ID**, le plus souvent un cookie de session
  - Lorsque l'utilisateur va réaliser des actions sur la plateforme, ce session ID, stocké dans son navigateur, va **systématiquement** être transmis au serveur afin qu'il puisse **identifier la session correspondante** ▫ Session ID est crucial car il authentifie l'utilisateur sans que ce dernier ait besoin de fournir ses identifiants

Attaque par Détournement de session/ Session hijacking attack (2)

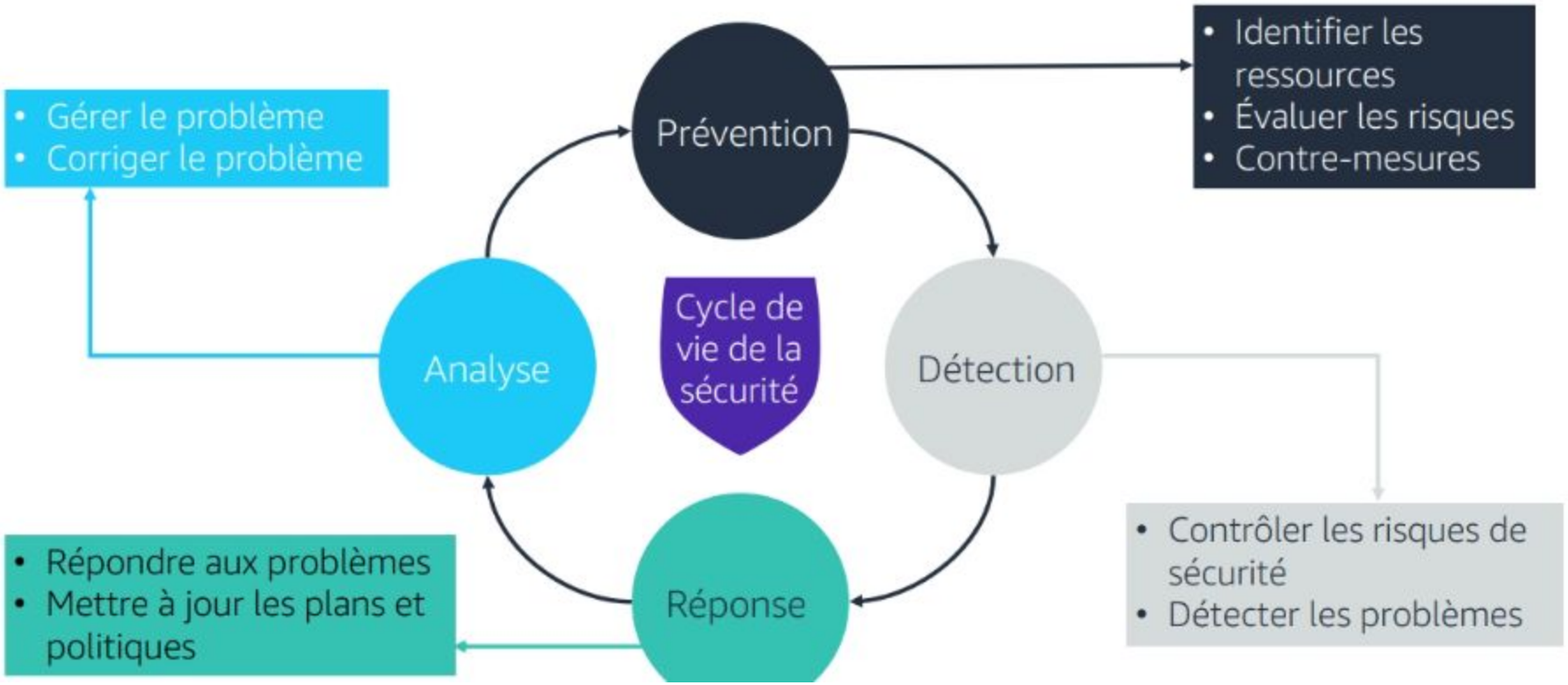
Le détournement de session consiste donc à dérober ce session ID, de manière à prendre possession de la session active.

Ou Session ID



Chapitre 3

Cryptologie:
Introduction & Notions de base


Prévention
• Identifier les ressources
• Évaluer les risques
• Contre-mesures
Détection
• Contrôler les risques de sécurité
• Détecter les problèmes
Réponse
• Répondre aux problèmes
• Mettre à jour les plans et politiques
Analyse
• Gérer le problème
• Corriger le problème
Cycle de vie de la sécurité