Université de Guelma
Département Informatique

Chapitre 1 : Introduction à la Sécurité Informatique

Cours - Sécurité Informatique

3 année LMD Système d'Information

Par : Dr. M. A. Ferrag

Syllabus

- **Chapitre 1 : Introduction à la sécurité : objectifs et critères de sécurité, menaces informatique, logiciels malveillants, criminalité informatique.**

- **Chapitre 2 : Principaux outils utilisés pour analyser et attaquer un réseau : (whireshark, nmap, nessus, metasptoit, etc).**

- **Chapitre 3 : Les protocoles de sécurité (IPSec, AAA, RADIUS, Diameter, EAP…)**

- **Chapitre 4 : Les Pare-feux (Translation, Filtrage, Mandataires et Détection d'Intrusions)**

- **Chapitre 5 : Autres aspects de la sécurité informatique abordée par les exposés des étudiants, par exemple, SSH, TLS, SSL, l'attaque du trou de ver, l'attaque du trou noir…etc.**

MODE D'EVALUATION

- **Examen final + Exposé**

- $Note\ Finale = \frac{(Note\ TD * 50) + (Note\ Examen * 50)}{100}$

Plan

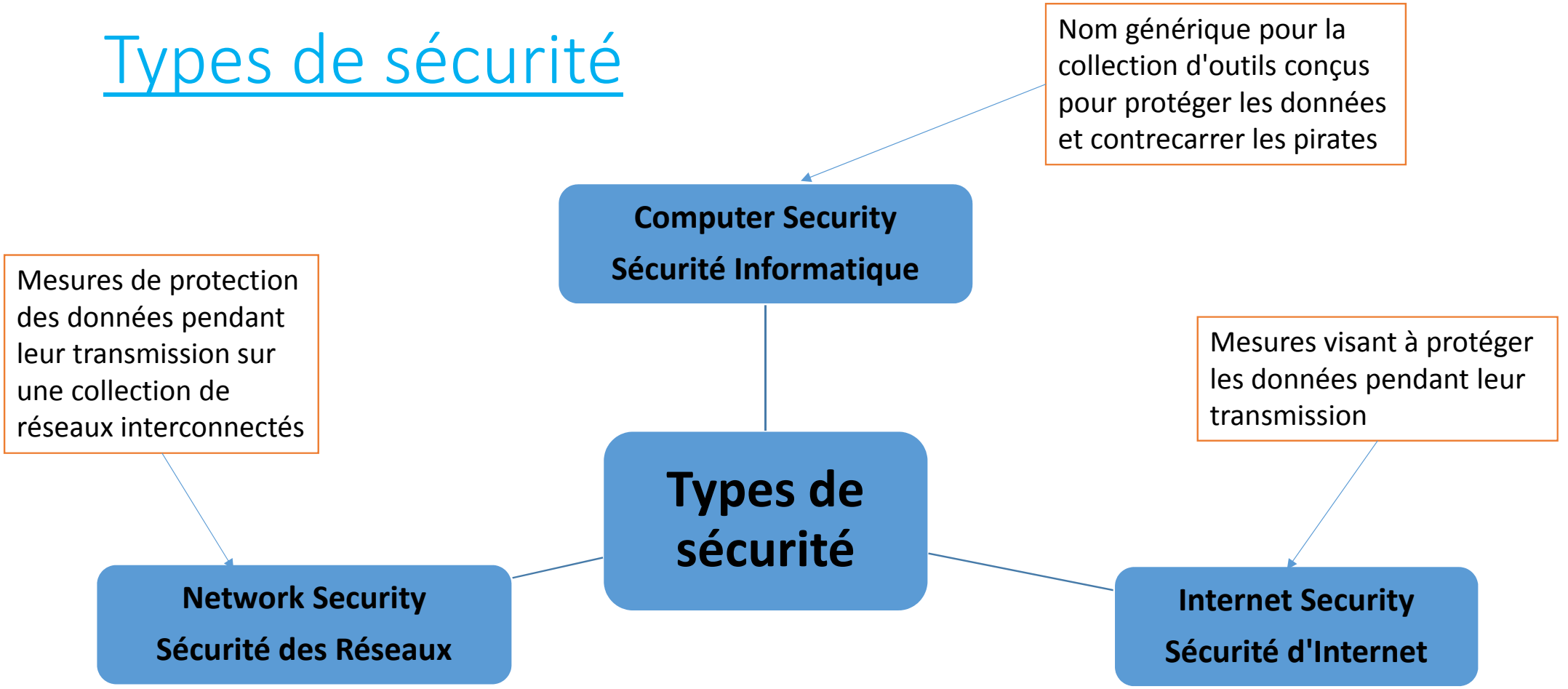
Partie 1

- Types de sécurité
- Terminologie essentielle
- Exigences fondamentales
- Contrôle d'accès
- Types de contrôle d'accès
- Authentification
- Authentification forte
- Autorisation
- Authentification vs. Autorisation
- Intégrité

Partie 2

- Les attaques : en temps réel
- Type des attaquants : par compétence
- Type des attaquants : par objectif
- Motivation des attaques
- Les attaques réseaux (Les plus fréquentes)
- L'attaque par rebond

Types de sécurité



Terminologie essentielle

- **Malware :** désigne tout programme informatique conçu pour infecter et endommager l'ordinateur d'un utilisateur légitime de multiples façons
- **Botnet:** groupe d'ordinateurs infectés et contrôlés par un pirate à distance
- **Vulnérabilité**: représente le niveau d'exposition face à la menace dans un contexte particulier: n'importe quel défaut matériel ou logiciel qui laisse le réseau ouvert pour une potentielle exploitation.
- **Menace :** action susceptible de nuire dans l'absolu. Il s'agit de toute intention ou méthodes utilisées pour exploiter une vulnérabilité (ou faiblesse) dans un système. Une menace peut être accidentelle ou intentionnelle.
- **Attaque :** toute action qui exploite une ou plusieurs vulnérabilités (failles) pour réaliser une menace avec l'intention de nuire.
- **Contre-mesure :** est l'ensemble des actions mises en œuvre en prévention de la menace.

Exemple

Dans le cas d'une authentification d'un utilisateur pour accéder à son compte mail :

- Vulnérabilité : envoie de mot de passe non chiffré à travers le réseau
- Menace : détournement du mot de passe
- Attaque : interception du mot de passe par un pirate qui écoute la communication (man-in-the-middle)
- Contre-mesure : chiffré le mot de passe avant de l'envoyer

Objectifs de la sécurité

- **Disponibilité :** *Demande que l'information sur le système soit disponible aux personnes autorisées.*
- **Confidentialité :** *Demande que l'information sur le système ne puisse être lue que par les personnes autorisées.*
- **Intégrité :** *Demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées.*
- **Non répudiation:** *Permettant de garantir qu'une transaction ne peut être niée.*
- **Authentification:** *Consistant à assurer que seules les personnes autorisées aient accès aux ressources.*

Contrôle d'accès

Il offre 3 services essentiels:

- **Authentification (qui peut se connecter)**
- **Autorisation (ce que les utilisateurs autorisés peuvent faire)**
- **Responsabilisation (identifie ce qu'un utilisateur a fait)**

Types de contrôle d'accès

- Contrôle d'accès centralisé

- Contrôle d'accès décentralisé

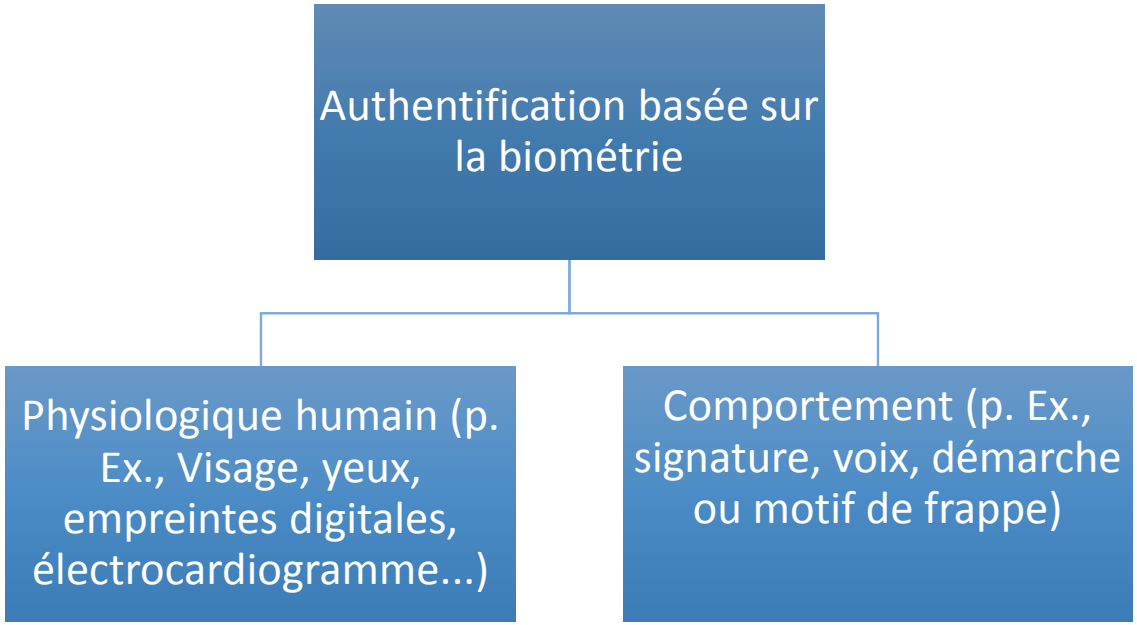
Authentification

Un moyen de vérifier ou de prouver l'identité d'un utilisateur

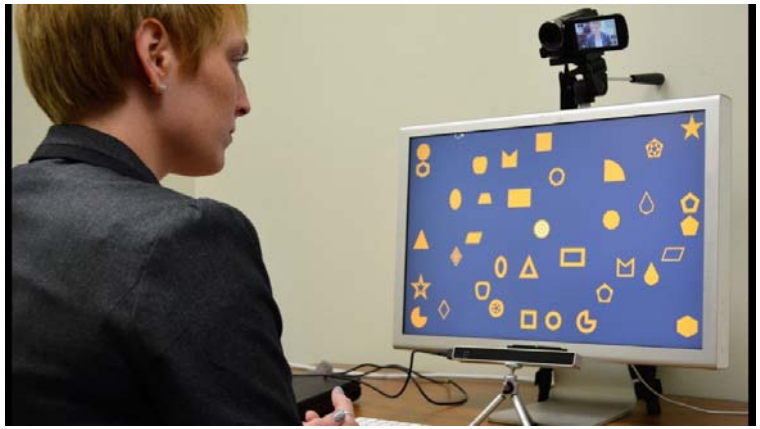
- Le terme «utilisateur» peut désigner:
  - Une personne
  - Application ou processus
  - Machine ou appareil
- Identification avant l'authentification
  - Fournir un nom d'utilisateur pour établir l'identité de l'utilisateur
- Pour prouver l'identité, l'utilisateur doit présenter l'une des informations suivantes:
  - Ce que vous savez (Mots de passe, PIN (Personal Identification Number))
  - Ce que vous avez (Jeton, cartes à puce, codes de passage, RFID)
  - Qui êtes-vous (biométrie comme les empreintes digitales et l'iris scan, signature ou Voix)

Authentification basée sur la biométrie

- **Gestes de regard**
- **Electrocardiogramme**
- **Reconnaissance vocale**
- **Reconnaissance de signature**
- **Reconnaissance de la marche**
- **Reconnaissance de visage**
- **Reconnaissance de l'iris**
- **Profilage de comportement**
- **Dynamique Keystroke**
- **Dynamique tactile**
- **Empreinte digitale**
- **Carte à puce**
- **Interfaces multi-touch**
- **Mot de passe graphique**
- **Rythme**
- **Écran tactile capacitif**

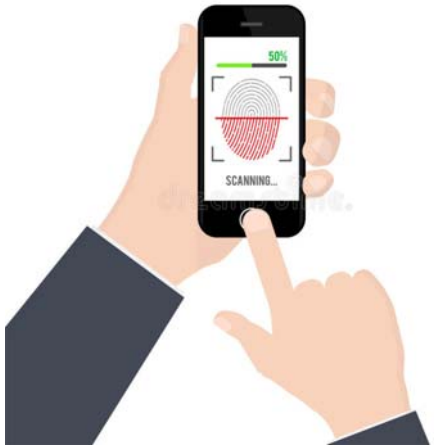


Gestes de regard

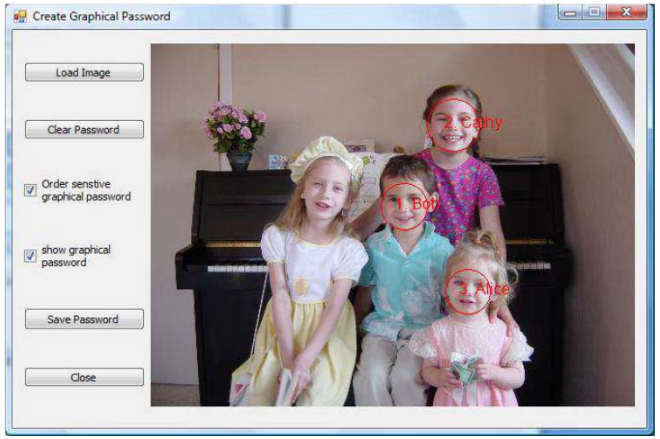


Le rythme cardiaque

Empreinte digitale

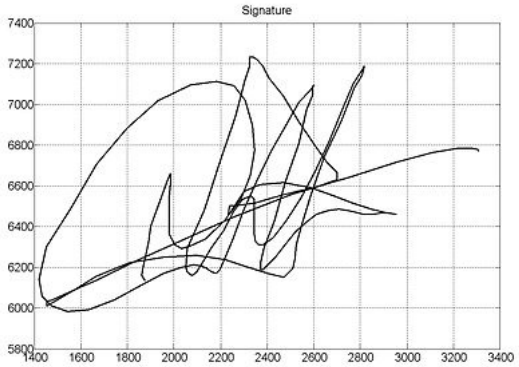


Mot de passe graphique

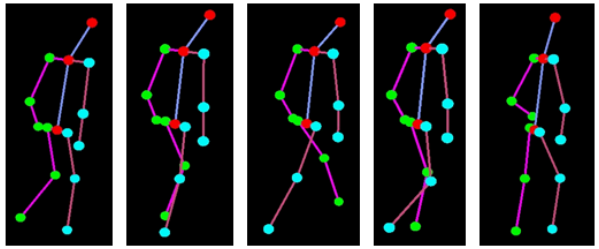


Reconnaissance vocale

Reconnaissance de signature



Reconnaissance de la marche



Reconnaissance de visage

Reconnaissance de l'iris

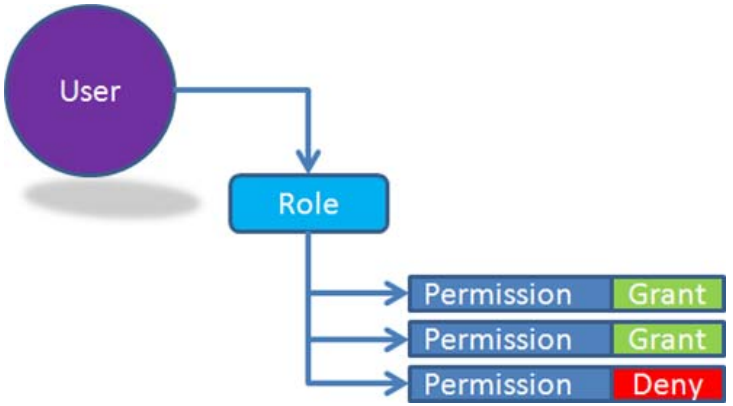
Authentification forte (Strong Authentication)

- **Authentification à deux facteurs (Two-factor authentication)**
- **Authentification à trois facteurs (Three-factor authentication)**
- **Authentification à multi facteurs (Multi-factor authentication)**

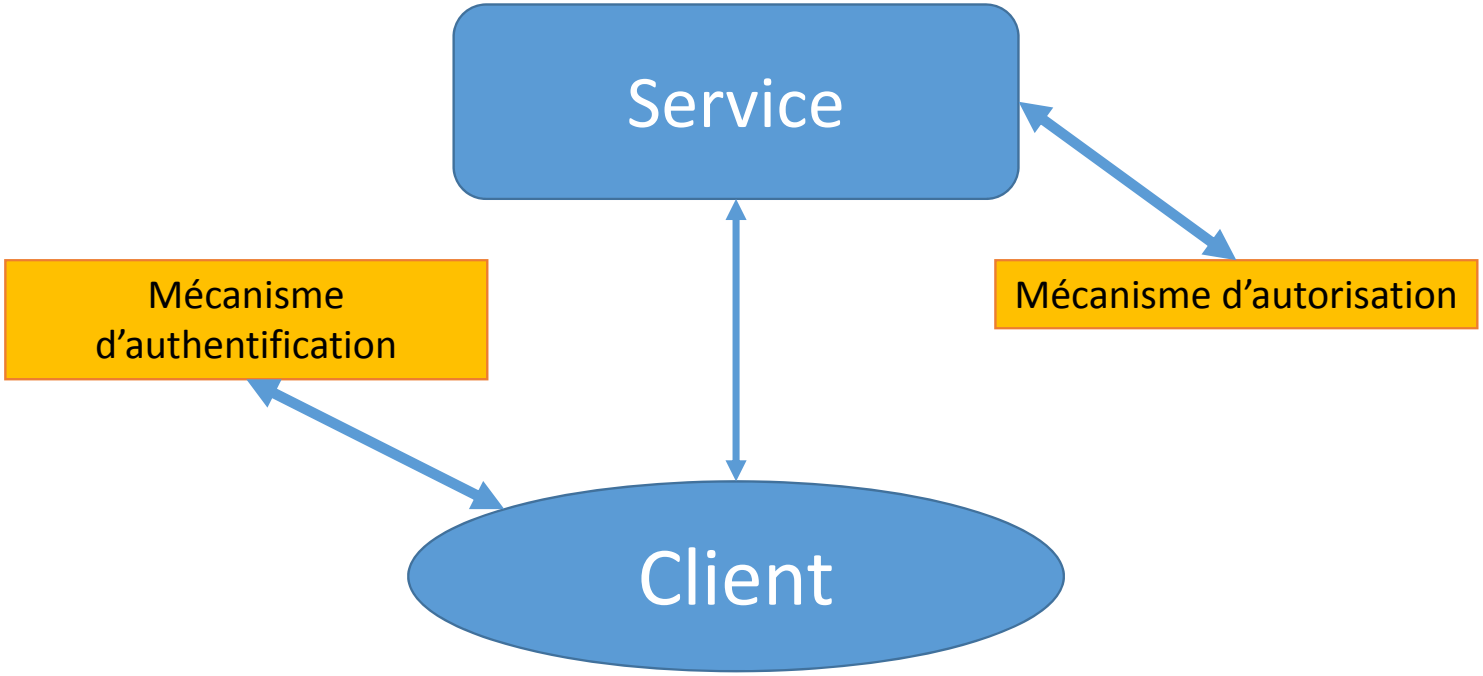
Autorisation

Définit les droits et autorisations de l'utilisateur sur un système

- Généralement effectué après l'authentification de l'utilisateur
- Permet à un utilisateur d'accéder à une ressource particulière et aux actions qu'il est autorisé à effectuer sur cette ressource
- Critères d'accès basés sur le niveau de confiance:
  - Les rôles
  - Groupes
  - Emplacement
  - Temps
  - Type de transaction



Authentification vs. Autorisation



- "Authentification identifie simplement une partie, l'autorisation définit si elles peuvent effectuer une certaine action" - RFC 3552 https://datatracker.ietf.org/doc/rfc3552/

Intégrité

- **Intégrité des données** : La propriété que les données n'ont pas été modifiée d'une manière non autorisée

- **Intégrité du système**: La qualité d'un système lorsqu'il exécute sa fonction prévue de manière intacte, sans manipulation non autorisée

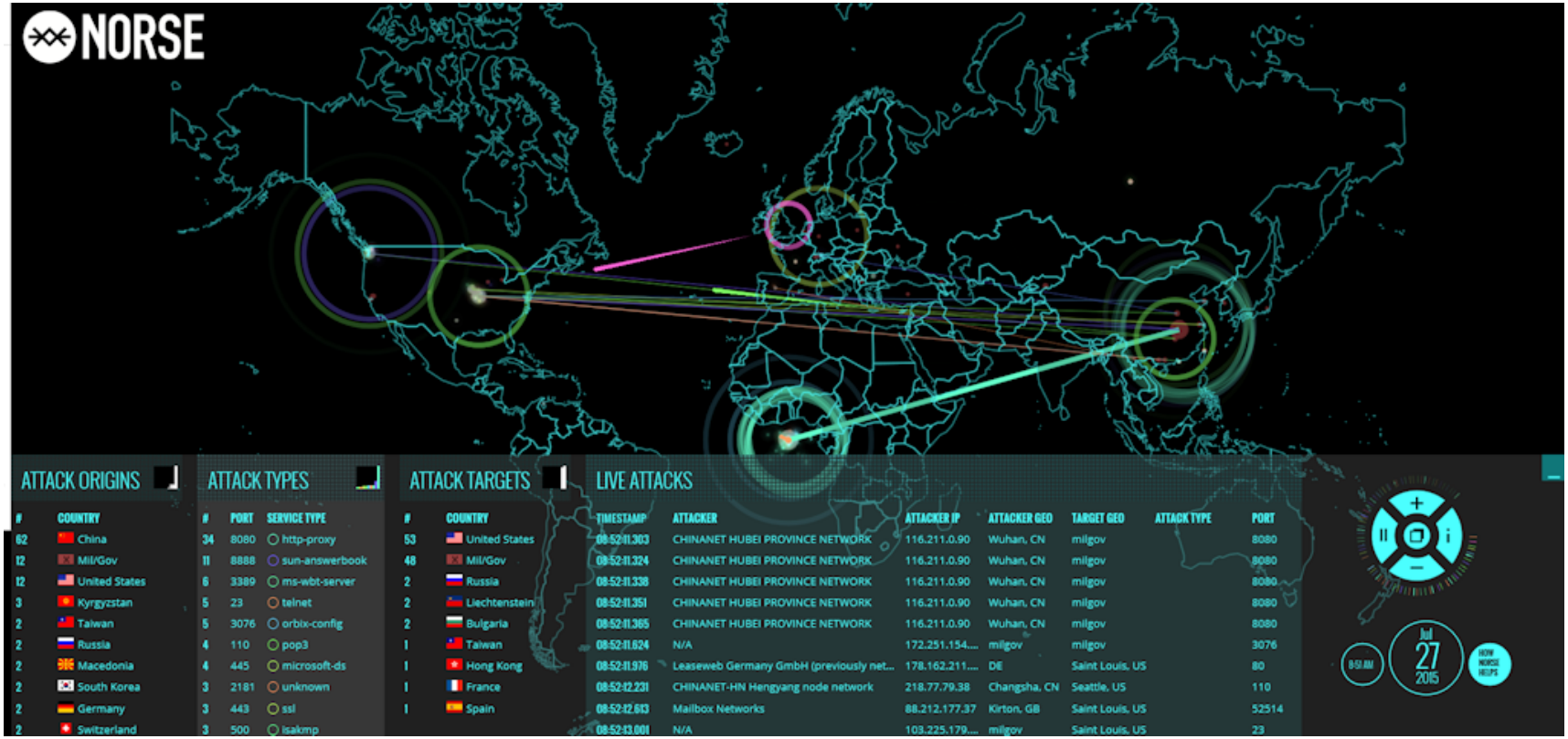
Les menaces informatiques

- Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.
- Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

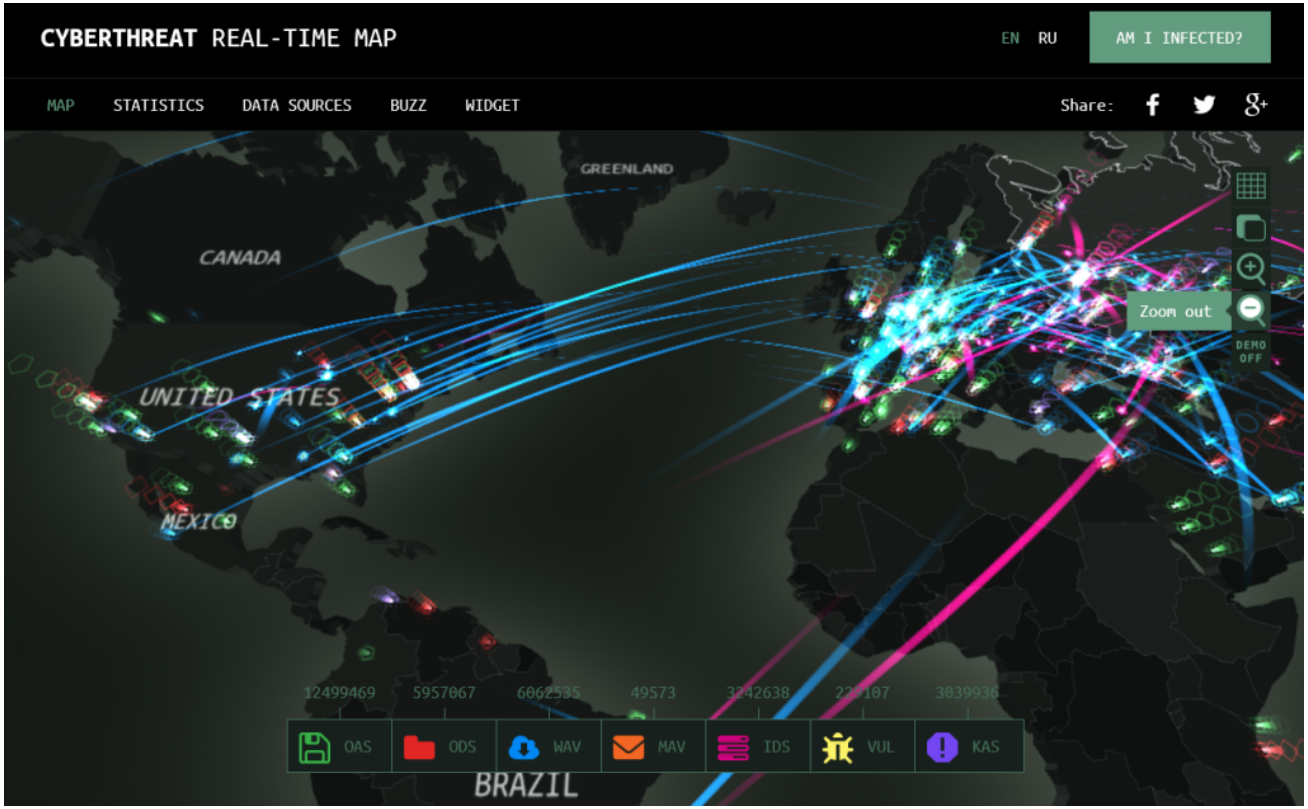
- Afin de détecter ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

Les attaques : en temps réel

http://map.norsecorp.com/



https://cybermap.kaspersky.com/



http://threatmap.fortiguard.com/

Type des attaquants : par compétence

- **Script Kiddy**
  - 90% playstation 9% clickomane 1% intelligence
  - utilise ce que font les autres
- **Amateur**
  - Failles connues
  - Failles web
- **Professionnel**
  - En equipe
  - Avec beaucoup de moyens (financiers, techniques, parfois préparatoires)
  - 0days possibles

Type des attaquants : par objectif

- **L'argent**
  - piratage volumétrique
  - cryptolocker "killer application"
- **Hacktiviste**
  - "Terroriste"
  - Anonymous
- **Espions**
  - Etatique
  - Industriel
- **"Petit con"**

Motivation des attaques

Les motivations des attaques peuvent être de différentes sortes :

- Obtenir un accès au système
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles
- Glaner des informations personnelles sur un utilisateur
- Récupérer des données bancaires ;
- S'informer sur l'organisation (entreprise de l'utilisateur, etc.)
- troubler le bon fonctionnement d'un service
- utiliser le système de l'utilisateur comme « rebond » pour une attaque
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée

Définitions – Les attaques

- En informatique et les réseaux informatiques, une attaque est une tentative d'exposer, de modifier, de désactiver, de détruire, de voler ou d'obtenir un accès non autorisé. Cependant, nous avons les deux définitions populaires suivantes,

- **Internet Engineering Task Force** définit l'attaque dans RFC 2828 comme :

« Un assaut sur la sécurité du système qui découle d'une menace intelligente, c'est-à-dire d'un acte intelligent qui est une tentative délibérée (en particulier dans le sens d'une méthode ou d'une technique) pour échapper aux services de sécurité et violer la politique de sécurité d'un système. »

- **Gouvernement des États-Unis,** l'instruction CNSS n°4009 du 26 avril 2010 par le Comité des systèmes de sécurité nationale des États-Unis d'Amérique définit une attaque comme suit :

« Toute activité malveillante qui tente de collecter, perturber, nier, dégrader ou détruire les ressources du système d'information ou l'information elle-même. »

Types d’attaques

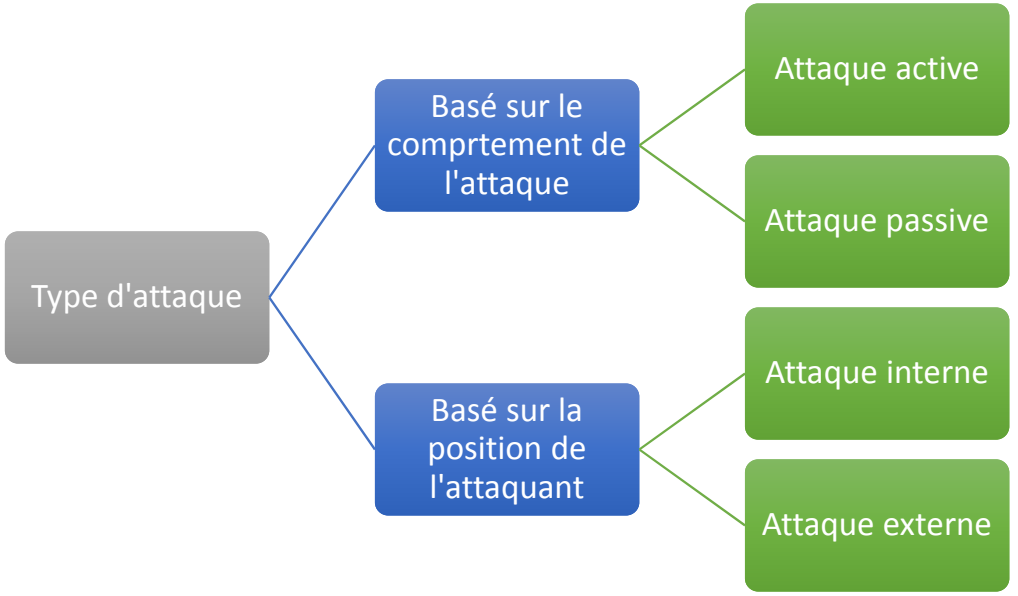
Comme présenté dans la Figure, une attaque peut être classée par son comportement ou par la position de l’attaquant.

Une attaque peut être active ou passive.

- Une **«attaque active»** tente de modifier les ressources du système ou d'affecter leur fonctionnement.
- Une **«attaque passive»** tente d'apprendre ou d'utiliser des informations du système mais n'affecte pas les ressources du système. (P. Ex., Écoutes téléphoniques).

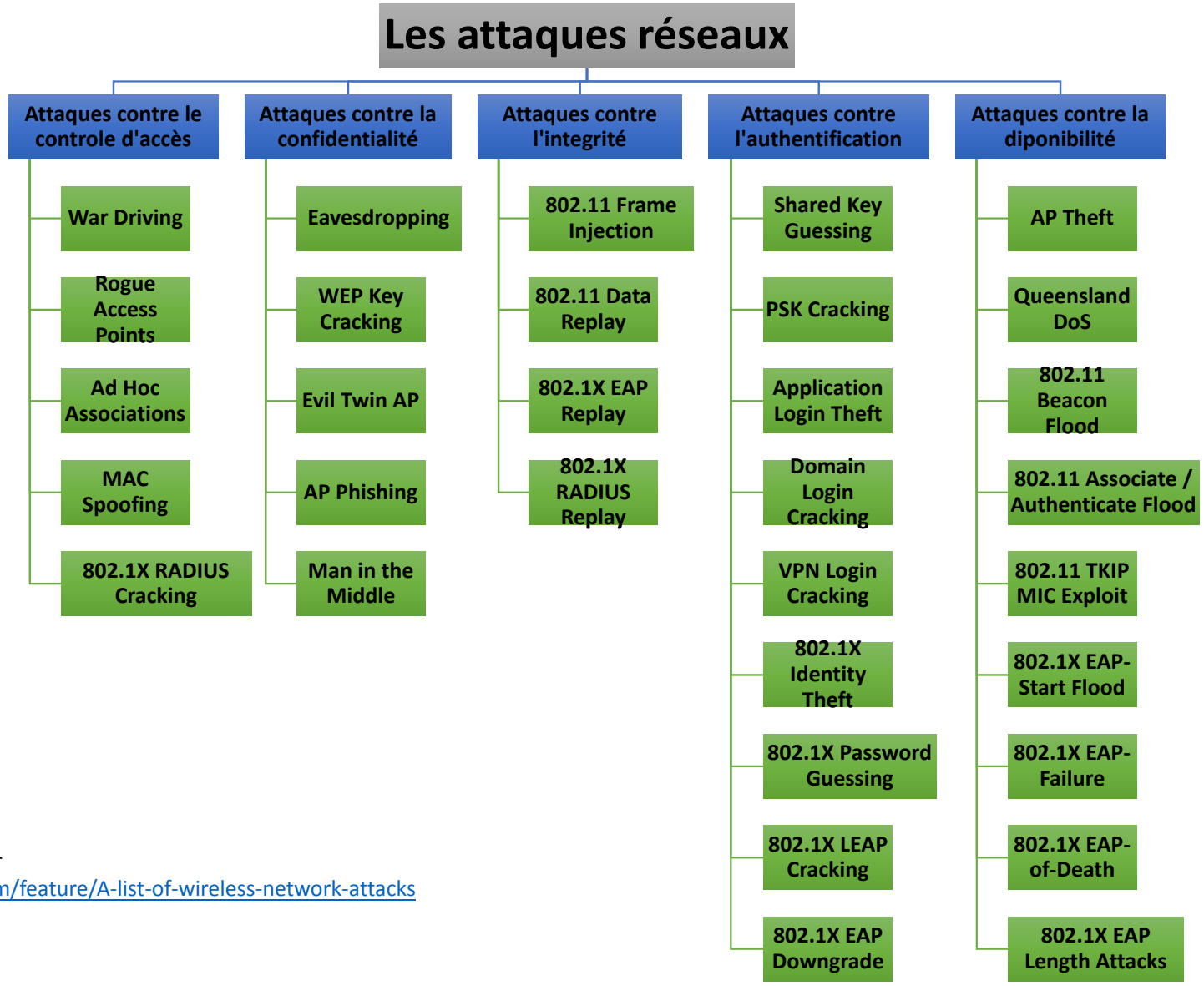
Une attaque peut être perpétrée par l’intérieur ou de l'extérieur de l’organisation.

- Une **«attaque interne»** est une attaque initiée par une entité dans le périmètre de sécurité, c'est-à-dire une entité autorisée à accéder aux ressources du système mais qui les utilise d'une manière non approuvée par ceux qui ont accordé l'autorisation.
- Une **«attaque extérieure»** est initiée depuis l'extérieur du périmètre, par un utilisateur non autorisé ou illégitime du système.



Classification des attaques

- Les attaques réseaux contre 802.11 et 802.1X, peuvent être classées selon le type de menace, et mises en correspondance avec des méthodes et des outils de piratage associés, à savoir,
- les attaques contre le contrôle d'accès,
- les attaques contre la confidentialité,
- les attaques contre l'intégrité, les attaques contre l'authentification,
- et les attaques contre la disponibilité.



Classification donnée par Lisa Phifer
http://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks

Attaques contre le contrôle d'accès

- Ces attaques tentent de pénétrer dans un réseau en utilisant des mesures de contrôle d'accès WLAN sans fil, comme les filtres AP MAC et les contrôles d'accès au port 802.1X.

Type d'attaque	Description	Méthodes et outils
War Driving	Découvrir les réseaux locaux sans fil en écoutant des balises ou en envoyant des requêtes de sonde, fournissant ainsi un point de lancement pour d'autres attaques.	Airmon-ng, DStumbler, KisMAC, MacStumbler, NetStumbler, Wellenreiter, WiFiFoFum
Rogue Access Points	Installation d'un point d'accès non sécurisé dans un pare-feu, création d'une porte dérobée ouverte dans un réseau de confiance.	Tout point d'accès matériel ou logiciel
Ad Hoc Associations	Connexion directe à une station non sécurisée pour contourner la sécurité de l'AP ou la station d'attaque.	Toute carte sans fil ou adaptateur USB
MAC Spoofing	Reconfiguration de l'adresse MAC d'un attaquant pour se présenter comme un AP ou une station autorisée.	MacChanger, SirMACsAlot, SMAC, Wellenreiter, wicontrol
802.1X RADIUS Cracking	Récupération du secret RADIUS par la force brute à partir de la demande d'accès 802.1X.	Outil de capture de paquets sur LAN ou chemin réseau entre le serveur AP et RADIUS

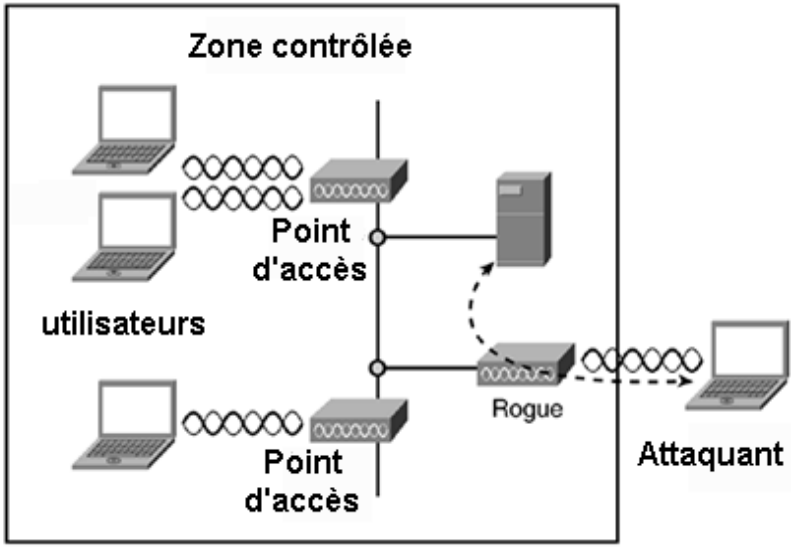
Attaques contre le contrôle d'accès
L'attaque « War Driving»

- **L'attaque « War Driving» :** La conduite de guerre, également appelée cartographie des points d'accès, consiste à localiser et éventuellement exploiter des connexions aux réseaux locaux sans fil tout en conduisant autour d'une ville ou ailleurs, comme présenté dans la Figure. Pour faire une conduite de guerre, vous avez besoin d'un véhicule, d'un ordinateur (qui peut être un ordinateur portable), d'une carte Ethernet sans fil configurée en mode promiscuous et d'une sorte d'antenne qui peut être montée au-dessus ou positionnée à l'intérieur de la voiture. Étant donné qu'un réseau local sans fil peut avoir une portée qui s'étend au-delà d'un immeuble de bureaux, un utilisateur extérieur peut se pénétrer dans le réseau, obtenir une connexion Internet gratuite et accéder éventuellement aux enregistrements de l'entreprise et à d'autres ressources.

- Avec une antenne omnidirectionnelle et un système de positionnement géophysique (GPS), le conducteur de guerre peut systématiquement localiser les emplacements des points d'accès sans fil 802.11b. Les entreprises qui ont un réseau local sans fil sont entrain d'ajouter des garanties de sécurité qui assureront uniquement les utilisateurs visés. Les garanties comprennent l'utilisation de la norme de chiffrement WEP (Wired Equivalent Privacy), IPsec ou Wi-Fi Protected Access (WPA), avec un pare-feu ou DMZ.

Attaques contre le contrôle d'accès
L’attaque « Rogue Access Points »

- **L’attaque « Rogue Access Points » :** Cette attaque se base sur l'installation d'un point d’accès non sécurisé dans un pare-feu, puis la création d'une porte dérobée ouverte dans un réseau de confiance, comme présenté dans la Figure. Les grandes entreprises investissent souvent dans des systèmes de prévention des intrusions sans fil (WIPS) qui utilisent des capteurs distribués pour surveiller à plein temps le trafic sans fil.

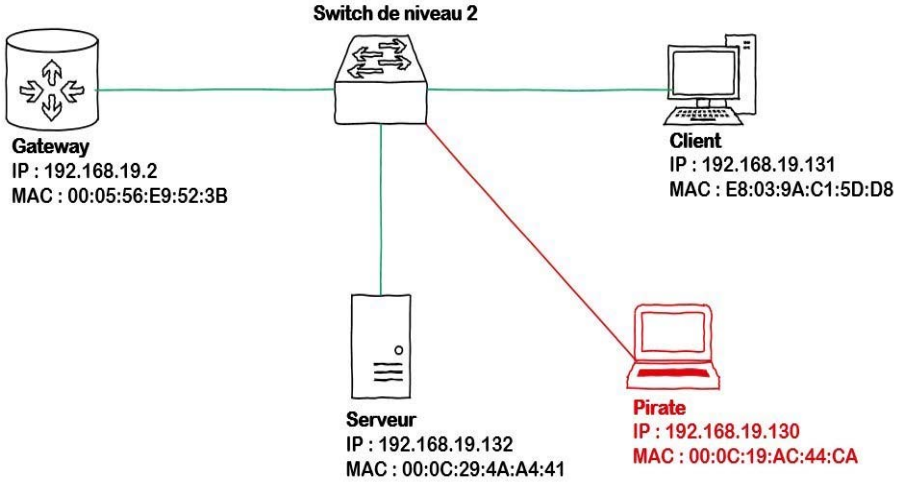


Attaques contre le contrôle d'accès
L’attaque « Ad Hoc Associations »

- L’attaque « Ad Hoc Associations » : Les réseaux ad hoc ne sont pas sans risques. Probablement le plus grand risque associé à la mise en réseau ad hoc a toujours été l'écoute électronique. Traditionnellement, les connexions ad hoc ont manqué les différents mécanismes de cryptage qui sont habituellement utilisés avec des points d'accès sans fil tels que WEP et WPA.

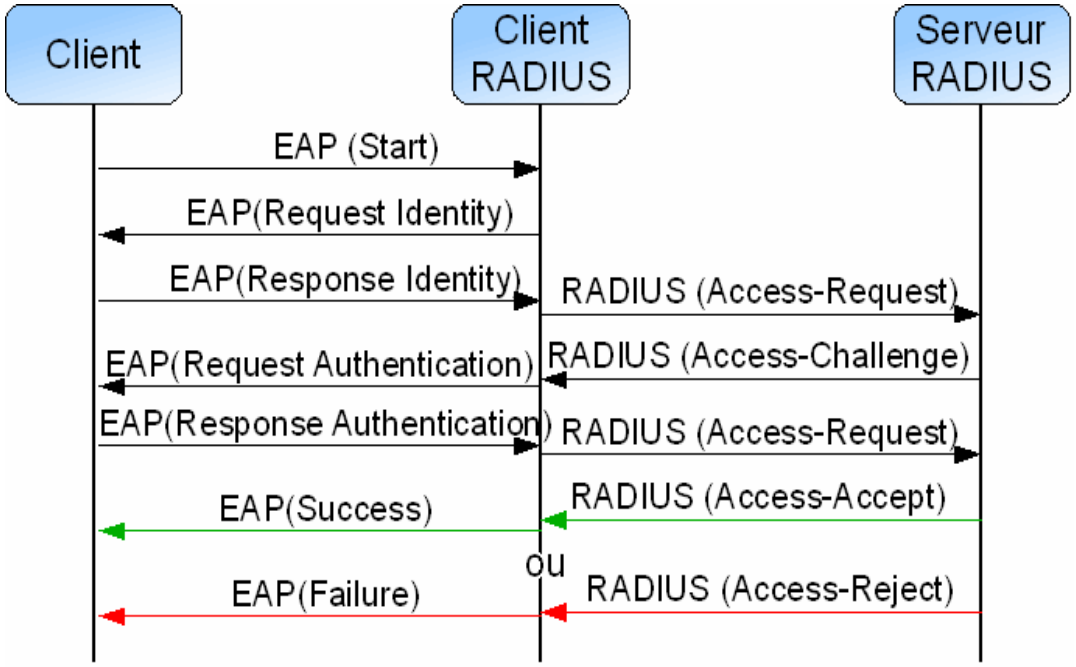
Attaques contre le contrôle d'accès
L’attaque « MAC Spoofing »

- **L’attaque « MAC Spoofing »:** La falsification MAC est une technique permettant de modifier une adresse de contrôle d'accès aux médias (MAC) attribuée à une interface réseau sur un périphérique en réseau. L'adresse MAC codée sur un contrôleur d'interface réseau ne peut pas être modifiée. Cependant, de nombreux pilotes permettent de modifier l'adresse MAC. De plus, il existe des outils qui permettent à un système d'exploitation de croire que la NIC a l'adresse MAC du choix d'un utilisateur. Le processus de masquage d'une adresse MAC est connu sous le nom de spoofing MAC. Essentiellement, la spoofing MAC implique de changer l'identité d'un ordinateur, pour quelque raison que ce soit, et c'est relativement facile.
- Comme présenté dans la Figure, le changement de l'adresse MAC assignée peut permettre de contourner les listes de contrôle d'accès sur les serveurs ou les routeurs, soit en cachant un ordinateur sur un réseau, soit en la permettant d'imiter un autre périphérique réseau. La falsification MAC est effectuée à des fins légitimes et illicites.



Attaques contre le contrôle d'accès
L'attaque « 802.1X RADIUS Cracking »

- **L'attaque « 802.1X RADIUS Cracking » :** Cette attaque se base sur la récupération du secret RADIUS par la force brute à partir de la demande d'accès 802.1X. De plus, cette attaque peut être lancée par un Outil de capture de paquets sur LAN ou chemin réseau entre le serveur AP et RADIUS



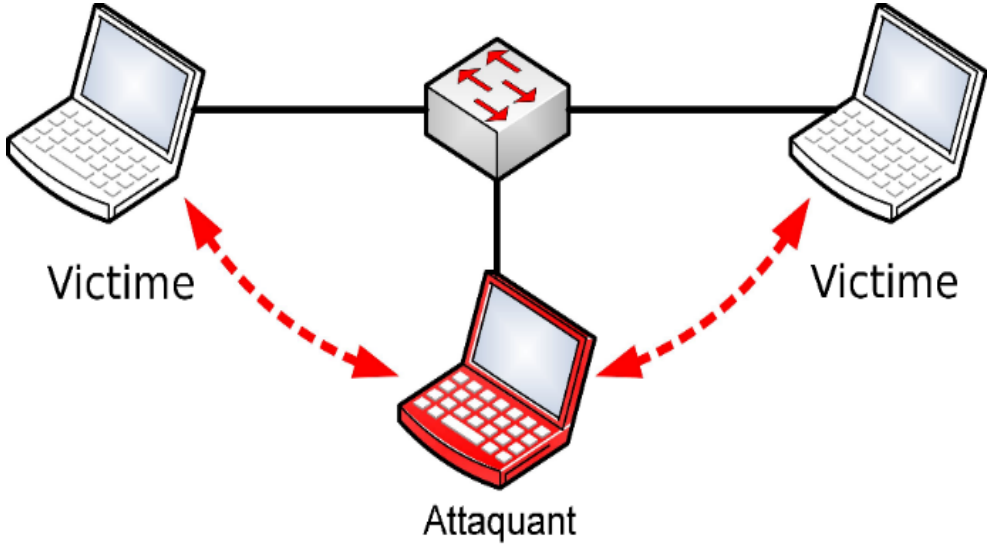
Attaques contre la confidentialité

- Ces attaques tentent d'intercepter des informations privées envoyées sur des associations sans fil, soit envoyé en clair ou chiffré par 802.11 ou des protocoles de couche supérieure.

Type d'attaque	Description	Méthodes et outils
Eavesdropping (Ecoute)	Capture et décodage du trafic d'application non protégé pour obtenir des informations potentiellement sensibles.	bsd-airtools, Ettercap, Kismet, Wireshark
WEP Key Cracking	Capture de données pour récupérer une clé WEP en utilisant des méthodes passives ou actives.	Aircrack-ng, airoway, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab, wesside
Evil Twin AP	Masquage en tant qu'appareil autorisé en balayant l'identificateur du WLAN (SSID) pour attirer les utilisateurs.	cqureAP, D-Link G200, HermesAP, Rogue Squadron, WifiBSD
AP Phishing	Exécution d'un faux portail ou d'un serveur Web sur un AP double mal à "phish" pour les connexions d'utilisateurs, les numéros de carte de crédit.	Airpwn, Airsnarf, Hotspotter, Karma, RGlueAP
Man in the Middle (d'attaque de l'homme dans le milieu)	Exécuter des outils traditionnels d'attaque de l'homme dans le milieu pour intercepter des sessions TCP ou des tunnels SSL / SSH.	dsniff, Ettercap-NG, sshmitm

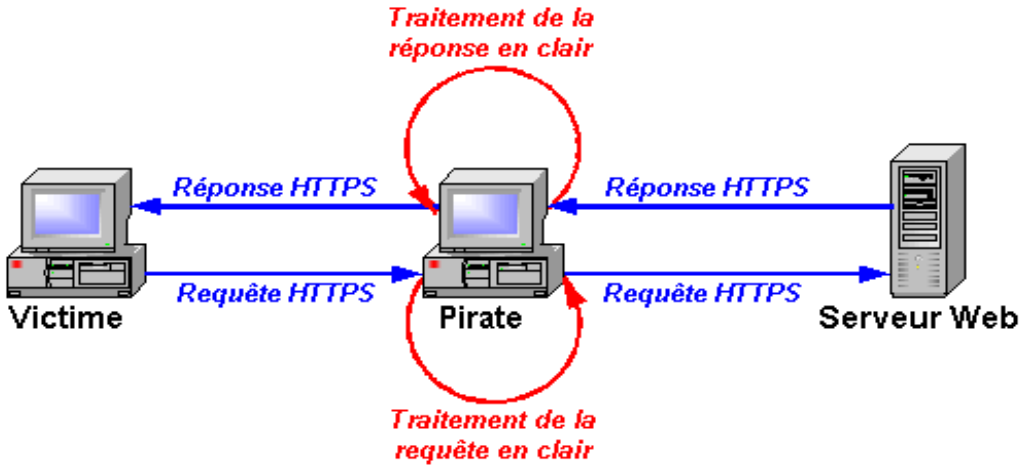
Attaques contre la confidentialité
L'attaque « Eavesdropping - Ecoute»

- **L'attaque « Eavesdropping - Ecoute» :** Comme présenté dans la Figure, cette attaque se base sur l'interception non autorisée en temps réel d'une communication privée, comme un appel téléphonique, un message instantané, une vidéoconférence ou une transmission de télécopie. Le terme «écoute» dérive de la pratique de se tenir debout sous les avant-toits d'une maison, en écoutant des conversations à l'intérieur.



Attaques contre la confidentialité
L'attaque Man in the Middle

- **L'attaque « Man in the Middle» :** est celui dans lequel l'attaquant intercepte et relève secrètement les messages entre deux parties qui croient communiquer directement entre elles, comme présenté dans la Figure.



Attaques contre l'intégrité

- les attaques contre l'intégrité se basent sur l'envoi des contrôles forgés, de la gestion ou des trames de données sur un réseau sans fil pour induire le destinataire ou faciliter un autre type d'attaque (par exemple, l'attaque DoS).

Type d'attaque	Description	Méthodes et outils
802.11 Frame Injection	Création et envoi des trames forgées 802.11.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
802.11 Data Replay	Capture des trames de données 802.11 pour une relecture ultérieure (modifiée).	Capture + Outils d'injection
802.1X EAP Replay	Capture des protocoles d'authentification extensible 802.1X pour une relecture ultérieure.	Capture sans fil + Outils d'injection entre une station et l'AP
802.1X RADIUS Replay	Capture d'accès RADIUS: accepter ou rejeter les messages pour une nouvelle version ultérieure.	Ethernet Capture + Injection Tools between AP and authentication server

Attaques contre l'authentification

- Les attaquants contre l'authentification utilisent ces attaques pour voler les identités et les informations d'identification des utilisateurs légitimes pour accéder aux réseaux et services privés.

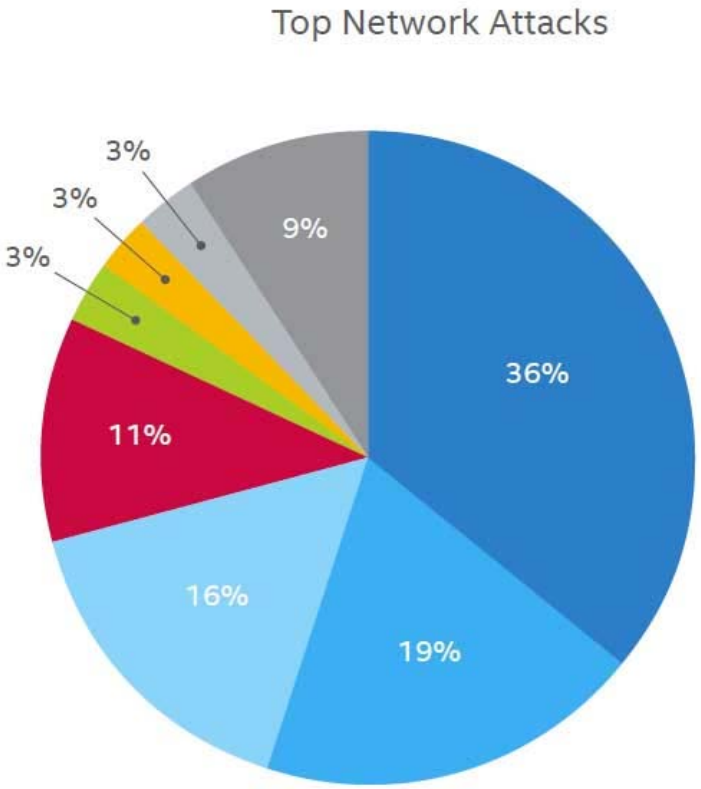
Type d'attaque	Description	Méthodes et outils
Shared Key Guessing	Tentative d'authentification de clé partagée 802.11 avec des clés WEP supposées et craquées.	WEP Cracking Tools
PSK Cracking	Récupération d'un PSPA / WPA2 PSK à partir de trames clés de handshake capturés en utilisant un outil d'attaque de dictionnaire.	coWPAtty, genpmk, KisMAC, wpa_crack
Application Login Theft	Capture des informations d'identification des utilisateurs (par exemple, adresse e-mail et mot de passe) à partir des protocoles d'application en clair.	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
Domain Login Cracking	Récupération des informations d'identification des utilisateurs (par exemple, connexion et mot de passe du Windows) en crachant les hachages de mot de passe NetBIOS en utilisant un outil d'attaque de force brute ou de dictionnaire.	John the Ripper, L0phtCrack, Cain
VPN Login Cracking	Récupération des informations d'identification des utilisateurs (par exemple, le mot de passe PPTP ou la clé Secret pré-partagé IPsec) en exécutant des attaques de force brute sur les protocoles d'authentification VPN.	ike_scan et ike_crack (IPsec), anger et THC-pptp-bruter (PPTP)
802.1X Identity Theft	Capture d'identité des utilisateurs à partir de paquets de réponse d'identité 802.1X en clair.	Capture Tools
802.1X Password Guessing	Utilisation d'une identité capturée, tentative répétée d'authentification 802.1X pour deviner le mot de passe de l'utilisateur.	Password Dictionary
802.1X LEAP Cracking	Récupération des informations d'identification des utilisateurs à partir des paquets légers EAP (LEAP) 802.1X capturés à l'aide d'un outil d'attaque de dictionnaire pour déchiffrer le hash du mot de passe NT.	Anwrap, Asleap, THC-LEAPcracker
802.1X EAP Downgrade	Forcer un serveur 802.1X à offrir un type d'authentification plus faible en utilisant des paquets forés EAP.	File2air, libradiate

Attaques contre la disponibilité

- Ces attaques empêchent la livraison de services sans fil à des utilisateurs légitimes, soit en leur refusant l'accès aux ressources WLAN, soit en paralysant ces ressources.

Type of Attack	Description	Methods and Tools
AP Theft	Suppression physique d'un AP d'un espace public.	"Five finger discount"
Queensland DoS	Exploiter le mécanisme d'évaluation des canaux clairs (CCA) CSMA / CA pour que le canal apparaisse occupé.	Un adaptateur prenant en charge le mode CW Tx, avec un utilitaire de bas niveau pour invoquer une transmission continue
802.11 Beacon Flood	Générer des milliers de balises contrefaites 802.11 pour rendre difficile aux stations de trouver un AP légitime.	FakeAP
802.11 Associate / Authenticate Flood	Remplir le tableau d'association d'AP cible.	FATA-Jack, Macfld
802.11 TKIP MIC Exploit	Générer des données TKIP non valides pour dépasser le seuil d'erreur MIC cible AP pour suspendre le service WLAN.	File2air, wnet dinject, LORCON
802.1X EAP-Start Flood	Inondant un AP pour consommer des ressources ou bloquer la cible.	QACafe, File2air, libradiate
802.1X EAP-Failure	En observant un échange EAP 802.1X valide, puis en envoyant à la station un message falsifié.	QACafe, File2air, libradiate
802.1X EAP-of-Death	Envoi d'une réponse d'identité EAP 802.1X mal formée connue pour provoquer une panne de certains points d'accès.	QACafe, File2air, libradiate
802.1X EAP Length Attacks	Envoi de messages spécifiques au type EAP avec des champs de longueur incorrecte pour tenter de bloquer un serveur AP ou RADIUS.	QACafe, File2air, libradiate

Les attaques réseaux (Les plus fréquentes)



Les attaques contre navigateurs

L'attaque par force brute est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles.

Une attaque informatique ayant pour but de rendre indisponible un service

Les attaques contre Secure Sockets Layer (SSL) et Transport layer security (TLS)

DNS flood est un type d'attaque de déni de service distribué (DDoS) dans lequel l'attaquant cible un ou plusieurs serveurs DNS (Domain Name System) appartenant à une zone donnée, ce qui tente d'entraver la résolution des enregistrements de ressources de cette zone et de ses sous-zones .

Les pirates utilisent les programmes de backdoor pour accéder au réseau de la victime.

Les attaques de l'accès physique

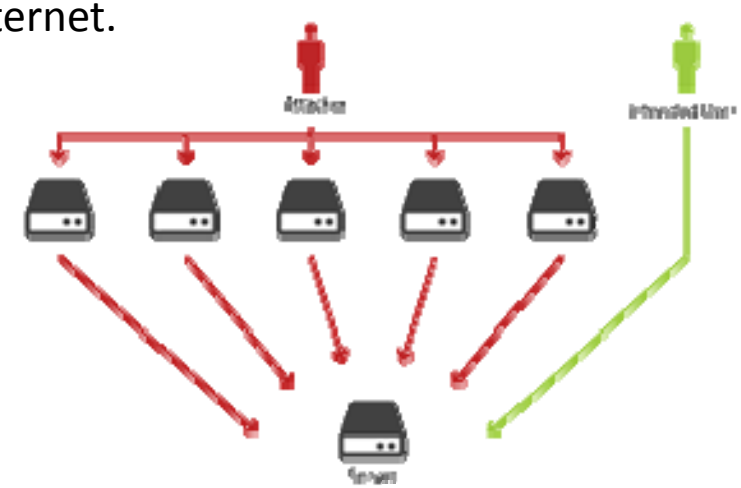
Il s'agit d'un cas où l'attaquant à accès aux locaux, éventuellement même aux machines :

- Coupure de l'électricité
- Extinction manuelle de l'ordinateur
- Ouverture du boîtier de l'ordinateur et vol de disque dur
- Ecoute du trafic sur le réseau

Les attaques DoS

Une attaque par déni de service (en anglais, denial of service attack [DoS] ou distributed denial of service attack [DDoS]) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il peut s'agir de :

- l'inondation d'un réseau afin d'empêcher son fonctionnement ;
- la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- l'obstruction d'accès à un service à une personne en particulier ;
- également le fait d'envoyer des milliards d'octets à une box internet.



Historique sur les attaques DoS

- La première attaque DDoS officielle a eu lieu en août 1999 : un outil appelé « Trinoo DDO » a été déployé dans au moins 227 systèmes, dont 114 étaient sur Internet, pour inonder les serveurs de l'université du Minnesota. À la suite de cette attaque, l'accès internet de l'université est resté bloqué pendant plus de deux jours.
- La première attaque DDoS médiatisée dans la presse grand public a eu lieu en février 2000, causée par Michael Calce, mieux connu sous le nom de Mafiaboy. Le 7 février, Yahoo! a été victime d'une attaque DDoS qui a rendu son portail Internet inaccessible pendant trois heures. Le 8 février, Amazon.com, Buy.com, CNN et eBay ont été touchés par des attaques DDoS qui ont provoqué soit l'arrêt soit un fort ralentissement de leur fonctionnement. Le 9 février, E-Trade et ZDNet ont à leur tour été victimes d'attaques DDoS. (il n'était âgé que de 15 ans)

- …. Aujourdhui, c'est par tout…

Références

- Pieprzyk, J., Hardjono, T., & Seberry, J. (2013). *Fundamentals of computer security*. Springer Science & Business Media.

- Goodrich, M., & Tamassia, R. (2010). *Introduction to computer security*. Addison-Wesley Publishing Company.

- Peltier, T. R. (2013). *Information security fundamentals*. CRC Press.

- Easttom II, W. C. (2016). *Computer security fundamentals*. Pearson IT Certification.