HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

les attaques par écoutes des réseaux sans fil :

Risques réels?

Matthieu Caron
<Matthieu.Caron@hsc.fr>

Hervé Schauer Consultants (HSC)

- **Hervé Schauer Consultants fondée en 1989**
  - Plus ancien acteur français de la SSI
  - PME classique – Modèle économique stable
  - HSC n'est pas revendeur de solutions commerciales

- **Rapprochement de Deloitte France en 2014**
  - « Centre de responsabilité » intégré à la cellule IT Advisory

- **Expertise unique** = Sécurité des systèmes d'information
  - Prestation intellectuelle exclusivement
  - Centrée sur son métier
  - 25% de R&D

Hervé Schauer Consultants (HSC)

- **2 métiers**
  - La formation SSI
  - Le conseil et l'expertise SSI
- **3 Pôles** permettant d'englober **tous les enjeux de la SSI**
  - Pôle Technique (Tests d'intrusion, audits, études, etc.)
  - Pôle Organisation, Risques et Conformité (Audit de procédures, analyse de risques, AMO, AMOA, etc.)
  - Pôle Juridique (Conseil juridique SSI à titre accessoire)
- **35 salariés dont 28 consultants**
  - 14 experts techniques
  - 11 spécialistes de la gouvernance SSI
  - 3 juristes

Hervé Schauer Consultants (HSC)

- **Consultants (certifications individuelles)**
  - CISSP
  - CISA
  - PCI DSS QSA
  - ISO 27001 LA / LI
  - Auditeur de certification 27001
  - ISO 27005 Risk Manager
  - GIAC GCFA
  - ITILv3
- **Société**
  - Organisme certificateur ARJEL
  - OPQCM (juridique)
  - SMQ 9001 (formations certifiantes)
  - PASSI (17 consultants certifiés)

Matthieu Caron

- **Diplômé de l'École Nationale des Arts et Métiers (ENSAM)**
- **Ingénieur R&D dans l'industrie**
- **Consultant en Sécurité des systèmes d'information**
  - Tests d'intrusion
  - Audits
  - Conseils

- **Certifié GIAC**
  - Web Pentester
  - Network Pentester
  - Forensic Examiner
- **Offensive Security Certified Professionnal (OSCP)**

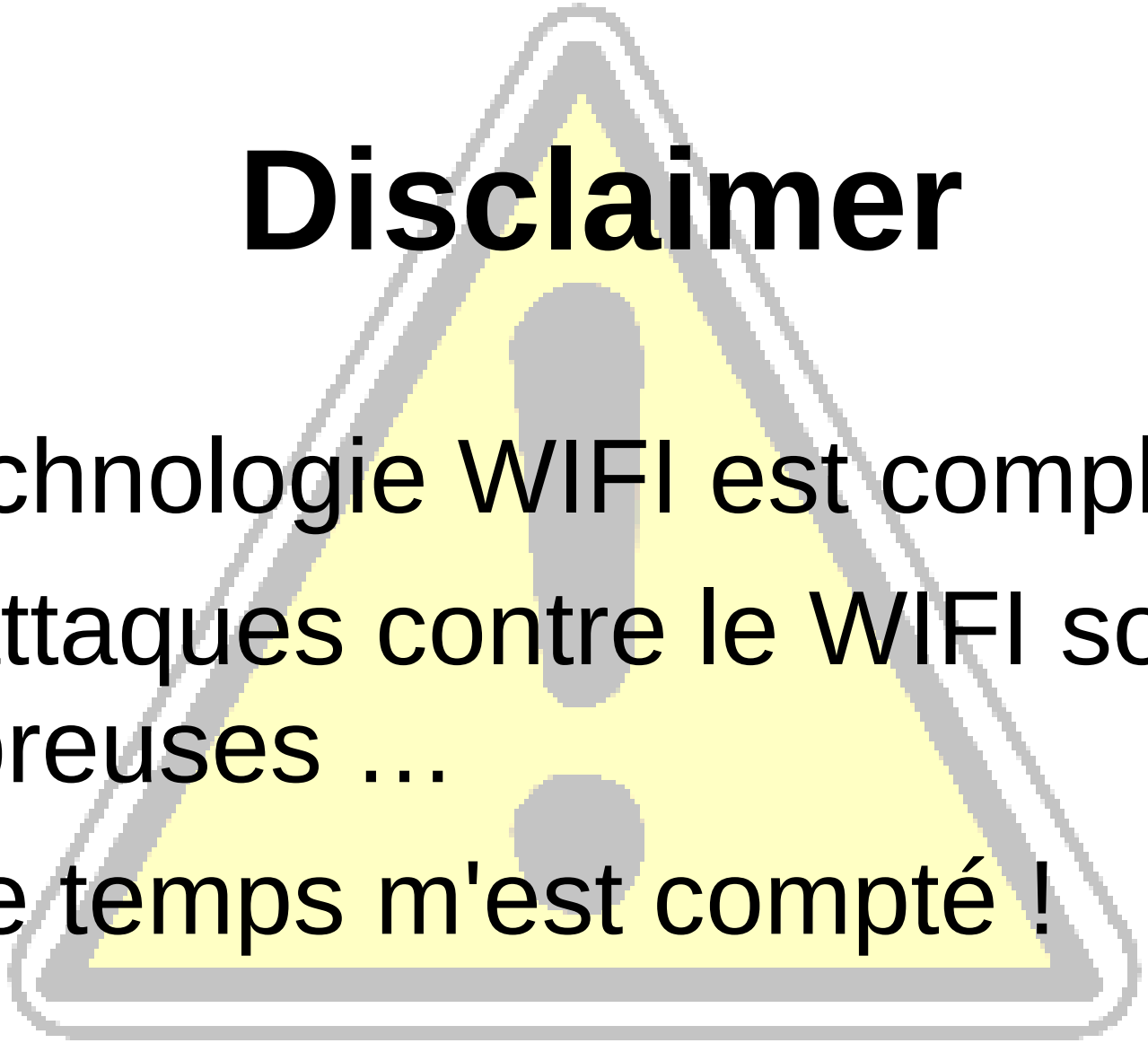
Les piliers de la sécurité

- **Disponibilité**
  - Accès fiable et permanent aux ressources et aux données à toute personne autorisée
- **Intégrité**
  - Précision et fiabilité des informations
  - Prévention contre des modification non autorisées
- **Confidentialité**
  - Le secret des données est assuré contre toute divulgation non autorisée

La sécurité du WIFI

- Usage privé & professionnel
- Véhicule beaucoup d'informations confidentielles
- Usage important par les smartphones pour faire transiter des informations sur le cloud
- De plus en plus utilisé par les objets connectés
- Grande variété de configurations
- Points d'accès en libre service
- Cible facile

- *Activité d'audit fréquemment réalisée par HSC*
- *Formation Sécurité du WIFI dispensée par HSC*

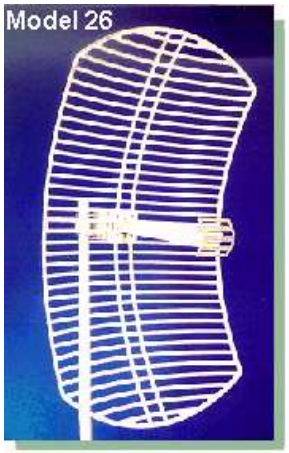


Disclaimer

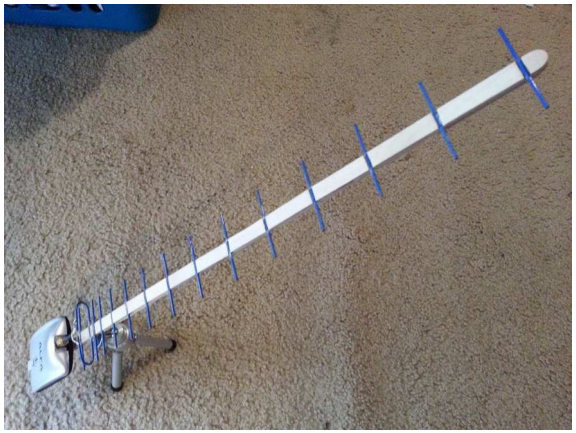
- La technologie WIFI est complexe
- Les attaques contre le WIFI sont nombreuses ...
- ...et le temps m'est compté !

Le périmètre du WIFI

- 10m à 100m généralement (selon l'environnement)
- Portée allongée (jusqu'à quelques km) avec du matériel adapté …



- … ou DIY



- **Record de 382 km !**

Caractéristiques de l'attaquant

- Localisation physique :
  - Dans votre entourage proche
  - Sur le parking de l'entreprise
  - A quelques centaines de mètres (concurrent ?)
- Relation :
  - Proche de confiance (collaborateur, membre de la famille …)
  - Entourage (client, fournisseur, intervenant extérieur...)
  - Inconnu

Caractéristiques de l'attaquant

- Motivations :
  - Nuire au fonctionnement
  - Récupérer des informations
  - Usurper une identité
  - Obtenir un point d'entrée sur un réseau
  - Prendre le contrôle d'un système

- Profil :
  - Script Kiddies, adolescent, curieux…
  - Hacker (Pirate), Auditeur ...
  - Agences gouvernementales (armée, espionnage..)

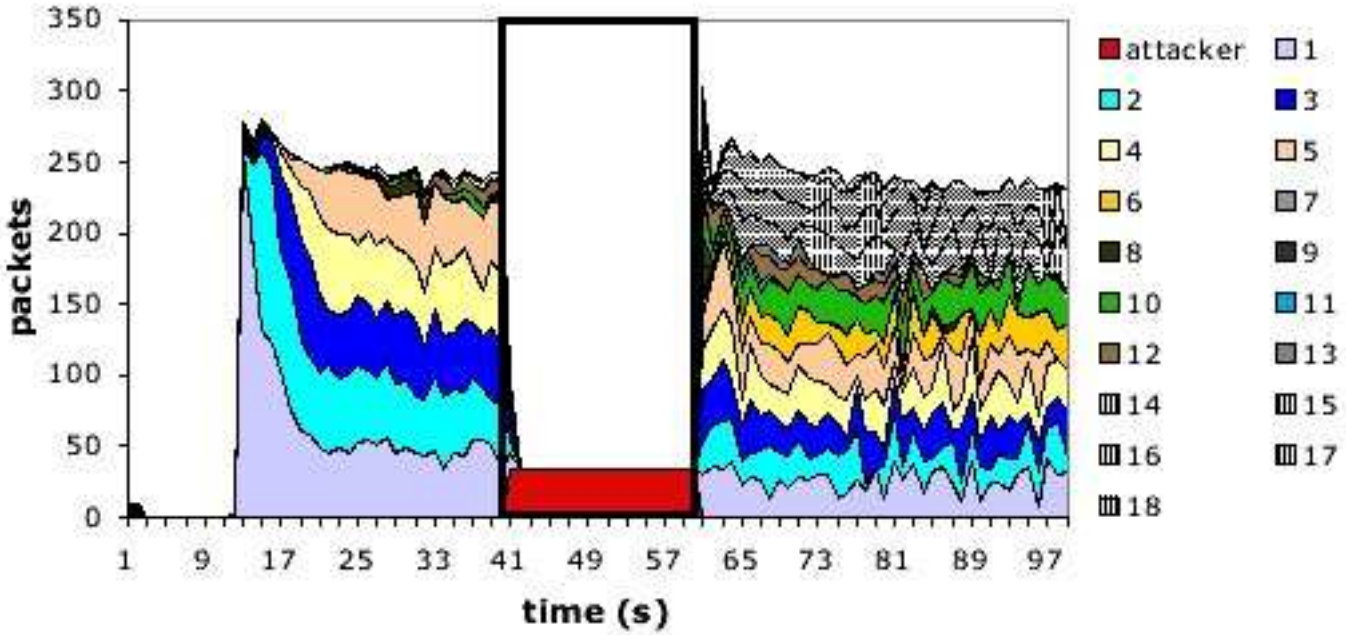
Scénario 1 : Nuisance

- Motivation :
  - Nuire au fonctionnement = empêcher les points d'accès WIFI de communiquer avec leurs clients
- Attaques :
  - Brouillage des ondes 2,4GHz
  - Corruption des trames de gestion CSMA/CA
    - *Virtual Carrier Sense Attack*
  - Envoi de trames de désassiociation / désauthentification
  - En dernier recours, vider les batteries de la victime !

Scénario 1 : Nuisance

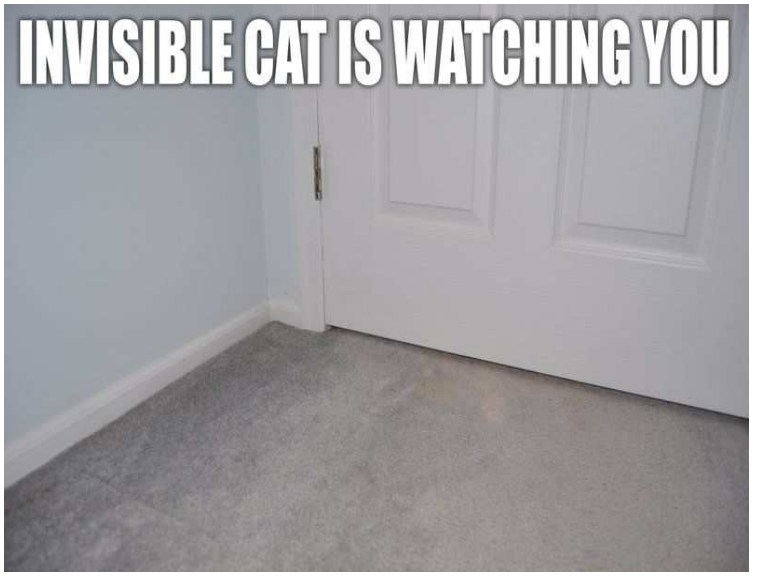
- *Brouilleur WIFI :*

- *Virtual Carrier Sense Attack :*



Scénario 2 : le WIFI invisible !

- Motivation :
  - Récupérer des informations
  - Usurper une identité
  - Obtenir un point d'entrée sur un réseau
  - Prendre le contrôle d'un système



- Cible :
  - Un réseau WIFI dont l'ESSID n'est pas diffusé (masqué)

Scénario 2 : le WIFI invisible !

- *Difficulté de l'attaque : 0/10*

- Attaques :
  - Écouter les communications entre les utilisateurs et la borne WIFI
  - … ou provoquer des communications en envoyant des paquets de désassociation / déauthentification

```
CH  6 ][ BAT: 3 hours 9 mins ][ Elapsed: 8 s ][ 2012-05-20 11:09

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 28:EF:01:35:34:85  -42       17        0    0   6  54e  WPA2 CCMP   PSK  <length:  6>

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

 28:EF:01:35:34:85  28:EF:01:23:45:67  -57    0 - 1      0        1
```

```
CH  6 ][ BAT: 3 hours 9 mins ][ Elapsed: 12 s ][ 2012-05-20 11:09

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 28:EF:01:35:34:85  -42       17        0    0   6  54e  WPA2 CCMP   PSK  hacked

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

 28:EF:01:35:34:85  28:EF:01:23:45:67  -57    0 - 1      0        1   hacked
```

Scénario 3 : Réseau ouvert

- Cible :
  - Réseau ouvert sans mécanisme de chiffrement
  - Portail captif ou non
- Cas concrets :
  - Free Wifi, SFR WiFi Fon, Bouygues Telecom Wi-Fi
  - Réseau WIFI invité
  - Mc Donald's, Quick
  - Gare SNCF, 1ere classe SNCF

Scénario 3 : Réseau ouvert

- *Difficulté de l'attaque : 0/10*

- Attaques :
  - Aucune ! Il suffit d'écouter le trafic

Scénario 3 : Réseau ouvert

Protocol	Length	Info
HTTP	235	GET /hotspot-detect.html HTTP/1.0
HTTP	491	HTTP/1.1 302 Moved Temporarily (text/html)
HTTP	491	[TCP Retransmission] HTTP/1.1 302 Moved Temporarily (text/html)
HTTP	235	GET /hotspot-detect.html HTTP/1.0
HTTP	242	HTTP/1.1 400 Bad Request
HTTP	267	[TCP ACKed unseen segment] HTTP/1.1 503 Service Temporarily Unavailable
HTTP	158	[TCP ACKed unseen segment] HTTP/1.1 200 OK (text/html)
HTTP	815	GET /api/widget/getwidget/mdtk/01737835/zone/?url=http%3A%2F%2Fwww.programme-tv
HTTP	815	[TCP Retransmission] GET /api/widget/getwidget/mdtk/01737835/zone/?url=http%3A%
HTTP	573	HTTP/1.1 200 OK (text/javascript)
HTTP	573	[TCP Retransmission] HTTP/1.1 200 OK (text/javascript)
HTTP	283	[TCP ACKed unseen segment] GET /fit/http.3A.2F.2Fimages.2Eone.2Eprismamedia.2Ec
HTTP	262	GET /fit/http.3A.2F.2Fimages.2Eone.2Eprismamedia.2Ecom.2Fnews.2F7.2F8.2F7.2F7.2
HTTP	586	HTTP/1.1 200 OK (JPEG JFIF image)
HTTP	488	HTTP/1.1 200 OK (JPEG JFIF image)
HTTP	810	[TCP ACKed unseen segment] GET /fit/http.3A.2F.2Fimages.2Eone.2Eprismamedia.2Ec
HTTP	810	[TCP ACKed unseen segment] [TCP Retransmission] GET /fit/http.3A.2F.2Fimages.2E
HTTP	810	[TCP ACKed unseen segment] [TCP Retransmission] GET /fit/http.3A.2F.2Fimages.2E
HTTP	799	GET /fit/http.3A.2F.2Fimages.2Eone.2Eprismamedia.2Ecom.2Fnews.2Fa.2F1.2F8.2F4.2
HTTP	219	GET /fit/http.3A.2F.2Fimages.2Eone.2Eprismamedia.2Ecom.2FproviderPerson.2F8.2Ff
HTTP	214	GET /fit/http.3A.2F.2Fimages.2Eone.2Eprismamedia.2Ecom.2FproviderPerson.2Fc.2F9
HTTP	597	GET /Imaginarium/api/uuid/859a2f18deacdf282715f96092131754b846e93e797228a3718a3
HTTP	519	GET /ajax/libs/swfobject/2.2/swfobject.js HTTP/1.1
HTTP	537	GET /shared/global.css?1470923374 HTTP/1.1
HTTP	510	GET /shared/global.js HTTP/1.1

Scénario 4 : Réseau WEP

- Cible :
  - Réseau protégé par un mot de passe
  - Protection WEP
- WEP (Wired Equivalent Privacy) :
  - Repose sur une clé partagée entre les clients et le point d'accès
  - La clé sert à s'authentifier sur le réseau
  - La clé sert à chiffrer les communications
    - Échange d'un IV en clair
    - Concaténation de l'IV et de la clé, puis chiffrement RC4 → PRGA

Scénario 4 : Réseau WEP

- Le WEP souffre de vulnérabilités majeures :
  - Clé plus courte que prévue
  - RC4 est une suite cryptographique faible
  - Collisions d'IV (4823 paquets = 50% de chance d'avoir le même IV)
  - PRGA découverte durant la phase de « handshake »
  - Pas de mécanisme empêchant le rejeu de messages
- *Difficulté des attaques : 4/10*
- Attaques :
  - Injection de paquets arbitraires sur le réseau
  - Déchiffrement des communications sans même connaître la clé (Chop Chop)
  - Découverte de la clé par analyse statistique et brute force

Scénario 4 : Réseau WEP

- Un attaquant possédant la clé a un accès au réseau et peut intercepter les communications en clair

- Attaques simples à réaliser
  - Nombreux tutoriels en ligne
  - Nombreux outils en ligne
  - Ne nécessite aucun moyen particulier
  - Très rapide à exécuter
  - Taux de réussite de 100 %
- *Démonstration vidéo*
  - **3min20 pour découvrir la clé WEP « HSCConsulting »**

WPA/WPA2, la solution ?

- WPA (WIFI Protected Access) :
  - Solution de transition qui corrige les vulnérabilités du WEP (TKIP)
    - Introduction de la notion de clés temporaires
  - Nécessite uniquement une mise à jour du matériel
  - Utilisable en PSK (Pre Shared Keys) ou MGT (authentification centralisée)
    - WPA Personnel = PSK
    - WPA Entreprise = MGT (IEEE 802.1x)

  - **Les attaques WEP ne sont plus efficaces contre WPA / WPA2**
  - **… Mais il est toujours possible d'écouter temporairement les communications sous certaines conditions**

WPA/WPA2, la solution ?

- WPA2 (WIFI Protected Access 2) :
  - Protection la plus aboutie du WIFI (CCMP)
    - Suite cryptographique AES (inviolée pour le moment)
    - Algorithmes robustes
    - Déclenchement de contre mesures lors de l'altération des messages
  - Requiert du matériel compatible
  - Reste rétrocompatible (TKIP)
  - Utilisable en PSK (Pre Shared Keys) ou MGT (authentification centralisée)
    - WPA Personnel = PSK
    - WPA Entreprise = MGT

Personnal / Enterprise

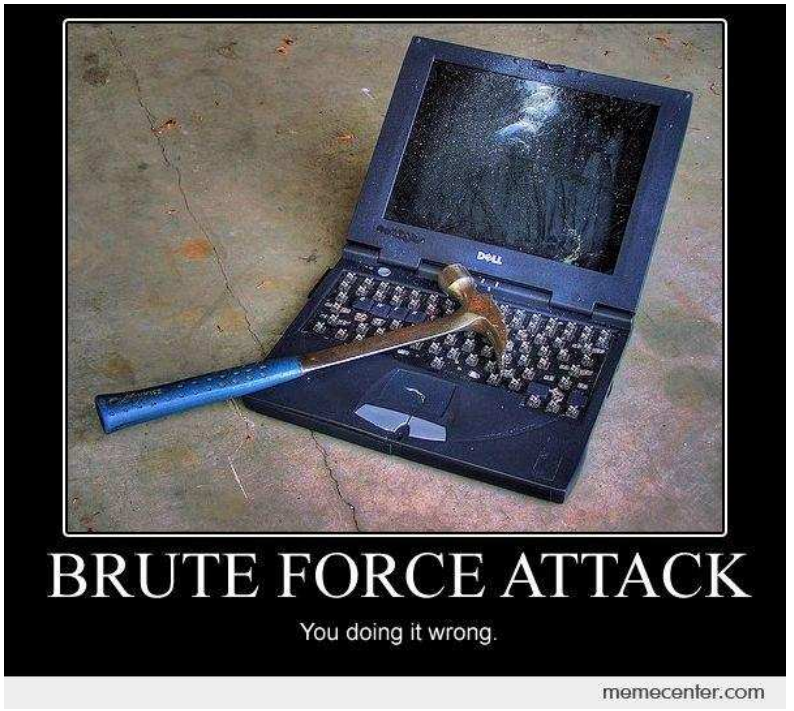
- WPA et WPA2 proposent 2 modes :
  - Personnel = PSK (Pre Shared Keys)
  - Entreprise = MGT(authentification centralisée)

- Personnel (PSK)
  - Une seule clé partagée par tout le monde

- Entreprise (MGT)
  - L'authentification est différente pour chaque utilisateur
  - Un serveur RADIUS et une base de données administrent les authentifications et les accès aux ressources
  - Plusieurs méthodes EAP proposées : EAP-TLS, EAP-TTLS, EAP-PEAP...

Scénario 5 : WPA/WPA2 Personal

- Cible :
  - Réseau protégé par un mot de passe
  - Protection WPA ou WPA2 Personnel



- *Difficulté de l'attaque : 0/10*

- Attaque :
  - Tenter de se connecter avec des mots de passe (Force brute):
    - par défaut du contructeur : « Belkin », « ZyXEL »
    - Triviaux : « wifi » « motdepasse » « freebox »
    - Ciblés : « [entreprise]Wifi » « [nom de famille]Wifi » « [entreprise]2016 »

Scénario 5 : WPA/WPA2 Personal

- Cible :
  - Réseau protégé par un mot de passe
  - Protection WPA ou WPA2 Personnel

- *Difficulté de l'attaque : 6/10*
- Attaque :
  - Interception de la première authentification (4-way handshake)
    - Forcée si nécessaire (envoi de trames de désassociation / déauthentification)
  - Découverte de la clé par force brute

Scénario 5 : WPA/WPA2 Personal

- La découverte par force brute est longue et l'issue incertaine :
  - Demande des ressources de calcul importantes
  - Requiert un dictionnaire de clés possibles à tester
    - Les dictionnaires sont classés par nombre et par type de caractères
    - Les dictionnaires peuvent être très volumineux
  - L'usage de dictionnaires pré calculés est très restreint

- **Une clé longue (14+ caractères) et complexe (minuscules + majuscules + chiffres + caractères spéciaux) protège bien le réseau WIFI WPA / WPA2**

Scénario 6 : WPA/WPA2 Enterprise

- Cible :
  - Réseau protégé par login / mot de passe et/ou certificat
  - Protection WPA ou WPA2 Entreprise

- *Difficulté de l'attaque : 8/10 à 10/10 selon la méthode EAP*

- Attaques : (si protection login / mot de passe)
  - S'insérer dans le canal de communication sécurisé
    - Mauvaise configuration de la sécurité du client
    - … ou inciter le client à installer le certificat de l'attaquant

- **Protection ultime si la méthode EAP n'a pas de faille**

Scénario 7 : WPS

- Cible :
  - Point d'accès qui propose une connexion WPS

- WPS (WIFI Protected Setup)
  - Code de 8 chiffres inscrits sur le point d'accès
  - Ou/et code de 8 chiffres sur l'équipement à connecter
  - Ou/et bouton poussoir sur le point d'accès

Scénario 7 : WPS

- *Difficulté des attaques : 4/10 à 7/10*

- Attaques :
  - « Race condition » : Connexion de l'attaquant avant le client légitime
  - Brute force du code PIN (seulement 10.000 + 1.000 combinaisons)
  - Pixie Dust : Attaque hors ligne à partir d'une capture d'authentification réussie

- **L'attaquant peut se connecter au point d'accès grâce au WPS**
- Les constructeurs ont rajouté des protections sur les modèles post 2012

Le SSL/TLS, le canal sécurisé

- Établit un canal sécurisé SSL / TLS entre le client et le serveur
  - Vérification de l'identité du serveur grâce à un certificat
  - Partage de clés de chiffrement entre le client et le serveur
  - Chiffre les communications avec les clés échangées
- Les communications ne sont plus visibles « en clair »

- **La protection miracle aux écoutes sur les réseaux WIFI ?**

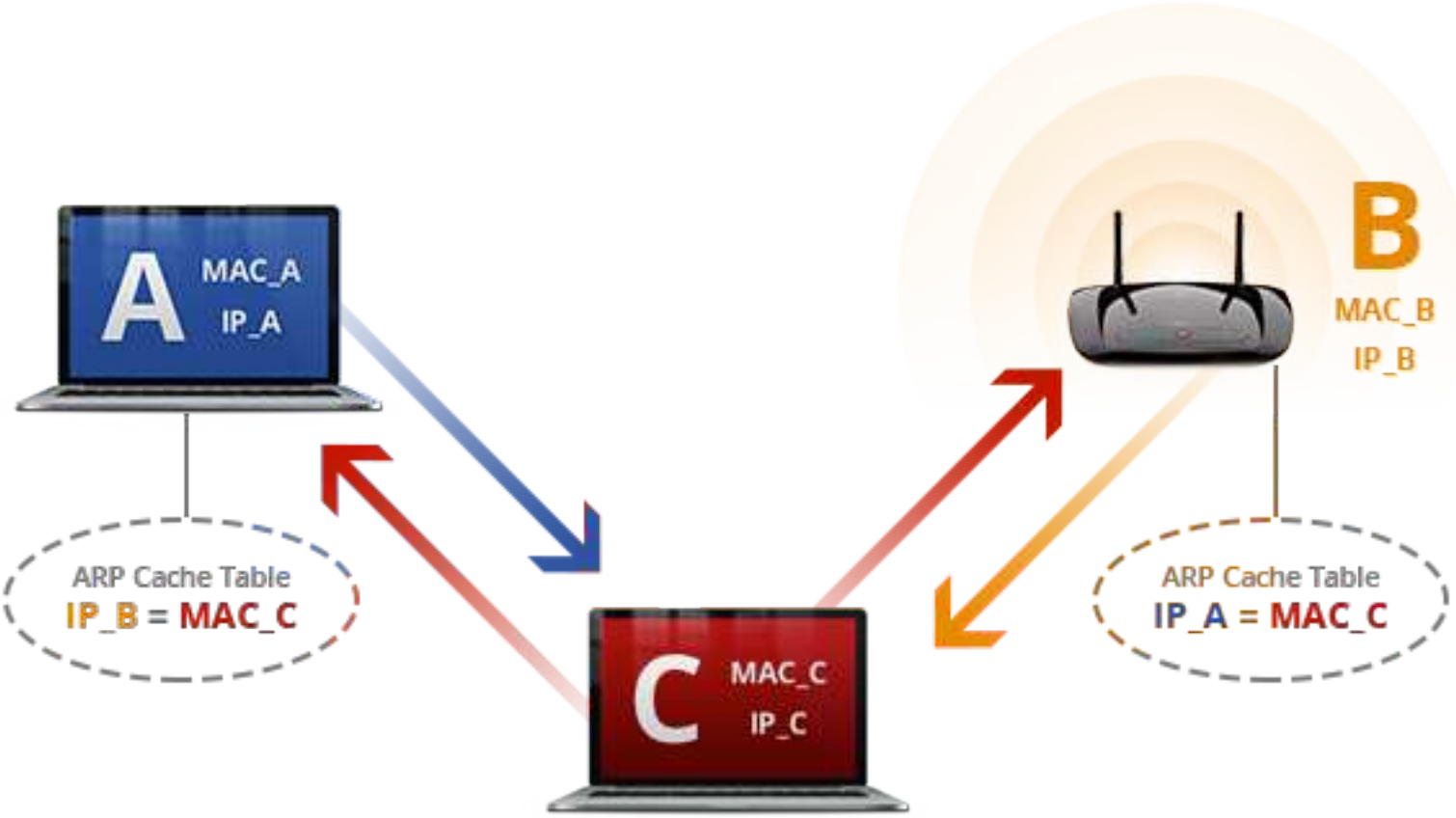
Le SSL/TLS, sécurité suffisante ?

- Les communications ne transitent plus en clair. Elles ne sont plus lisibles par un attaquant
- **… mais les pirates ont développé des parades !**
- *Difficulté de l'attaque : 4/10*

- Attaque :
  - Envoi de pages factices non sécurisée avant le serveur légitime
- D'autres attaques seront présentées plus loin...

Man-In-The-Middle

- Man-In-The-Middle ou Monkey-In-The-Middle (MITM)
  - Position de l'Homme du Milieu ou du Singe Intercepteur



Rogue AP

- Point d'accès factice au sein d'un réseau WIFI, contrôlé par l'attaquant
- *Difficulté de l'attaque : 6/10*
- Déroulement :
  - Créer un point d'accès factice dans le réseau WIFI de la victime
    - ESSID identique
    - Puissance d'émission forte
  - Forcer la déconnexion de la victime (envoi de trames de déassociation / déauthentification)
  - Accepter les demandes de connexion de la victime
  - Relayer les communications de la victime vers le point d'accès légitime

Rogue AP / MITM

- La position d'Homme du milieu offre à l'attaquant un large éventail d'attaques :
  - Écoute :
    - Rétrograder toutes les communications sécurisées SSL/TLS en clair
    - Inciter la victime à installer son propre certificat sur son dispositif afin disposer de ses communications chiffrées
    - Proposer des services non sécurisés (mail, web, partage, impression, multimédia…)
  - Exploitation :
    - Redirections
    - WI-Phishing
    - Exploitation des vulnérabilités du dispositif de la victime

Evil Twin

- Point d'accès entièrement factice
  - ESSID aguicheur (« WIFI Gratuit ») ou copié (« Free Wifi »)
  - Relaye ou non les communications vers le web
- *Difficulté de l'attaque : 6/10*

- Éventail d'attaques similaires au MITM sur Rogue AP avec une forte tendance au WI-Phishing

Evil Twin

- Evil Twin créé automatiquement !
  - Les dispositifs connectés envoient régulièrement des requêtes pour savoir s'ils sont à proximité d'un point d'accès connu (PNL)
  - L' Evil Twin est créé automatiquement à partir de l'ESSID mémorisé et diffusé par le dispositif
  - Le dispositif se connecte automatiquement à l'Evil Twin et divulgue potentiellement des informations confidentielles

Sécuriser son infrastructure WIFI

- **Minimum**
  - Utiliser le WPA, le WPA2 étant fortement recommandé
  - Désactiver TKIP
  - Configurer un mot de passe long (minimum 14 caractères) et complexe (minuscules, majuscules, chiffres, symboles)
  - Désactiver le WPS
  - Limiter les SSID auxquels les clients peuvent se connecter
  - Sensibiliser les utilisateurs !

Sécuriser son infrastructure WIFI

- **Professionnel**
  - Placer ses points d'accès WIFI dans la DMZ
  - Mettre en place un portail captif
  - Contrôler le trafic en entrée et sortie des points d'accès
  - Authentification RADIUS (choisir la méthode EAP qui répond au mieux aux besoins)
  - Cloisonner le réseau WIFI (VLAN)
- **Professionnel avec accès depuis l'extérieur**
  - Passage obligatoire par une tête de VPN pour une connexion sécurisée depuis n'importe quel point d'accès extérieur

Sécuriser son infrastructure WIFI

- **Idéale**
  - Ajout d'un IDS (Intrusion Detection System)
    - Détection de tentative de déni de service
    - Détection de tentative de Man-in-the-Middle
    - Détection de Rogue-AP
- **Alternative**
  - Ne pas utiliser le WIFI pour tout ce qui peut être fait en filaire
  - LIFI
  - Utiliser une autre technologie filaire qui n'impose pas l'installation de câbles : les réseaux sur courant porteur

Utiliser le WIFI en toute sécurité

- Ne pas laisser son équipement avec le WIFI activé
- Ne pas se connecter sur les WIFI ouverts ou WIFI WEP (et éviter WPA) pour réaliser des opérations confidentielles
- Vérifier la présence du petit cadenas sur les pages sécurisées
- Ne pas accepter sans comprendre les demandes sollicitées (installation de certificat)

Merci pour votre attention

Question ?

Matthieu Caron

<Matthieu.Caron@hsc.fr>