Sécurité des réseaux non-filaires
Sécurité Wi-Fi

Carlos Aguilar

carlos.aguilar@enseeiht.fr

IRIT-IRT

Sources

Basé sur les cours de :

- Cédric Blancher (EADS)
- Dan Boneh de Stanford University
- Pierre-François Bonnefoi du Master CRYPTIS à Limoges
- Céline Boyer (Canal+)
- Julien Cartigny du Master CRYPTIS à Limoges
- Ron Rivest du M.I.T.

Plan

Alternatives pour l'authentification/chiffrement

« Réseau » ouvert

Pas d'authentification pour se connecter au Wi-Fi et pas de chiffrement

Portail captif : authentification avant de que la borne commute et route normalement nos paquets

WEP (Wired Equivalent Privacy)

Protocole de chiffrement initialement prévu dans la norme 802.11 (1999)

Vous protège de la mamie voisine du dessus, et encore ...
Devrait plutôt s'appeler *Weak Encryption Protocol* → Ne pas utiliser

WPA (1,2,PSK, EAP, 802.1X, Personal, Enterprise)

WPA = WPA1 et WPA2 diffèrent sur le chiffrement utilisé
Deux modes d'authentification :
- Personal ou PSK : authentification par secret commun prepartagé
- Enterprise ou 802.1X ou EAP : authentification indép. de chaque utilisateur

Les trames de gestion (1/2)

Le déni de service par déauthentification

Les trames de déauthentification ne sont pas authentifiées ou chiffrées ...
Il suffit d'écouter le trafic pour voir :

- Quelles stations sont connectées à un AP
- Quelle est l'adresse MAC de l'AP

Puis il suffit de scapy ou d'un logiciel dédié pour spoofer l'AP

Utilisation de `aircrack-ng`

```
# airmon-ng start wlan0
[ monitor enabled on mon0 ]
# airodump-ng -c canaldevotreAP mon0
# aireplay-ng -deauth 3 -a «BSSID de l'AP» -c [«MAC de la cible»] mon0
```

Possible d'utiliser une adresse de broadcast !

Les trames de gestion (2/2)

MITM en utilisant les trames de gestion

1. Déauthentification systématique de STA
2. Mise en place d'un faux AP (carte en mode infrastructure) avec l'ESSID et MAC de l'AP sur un autre canal
3. La station va essayer de se connecter sur le faux AP (sur le vrai elle est systématiquement déauthentifié)
4. Quand une association entre STA et l'AP pirate commence, l'attaquant relaye le trafic entre STA et le vrai AP se plaçant en homme du milieu

Marche même si on ne connaît pas le mdp du réseau (contrairement à ARP)

L'attaque casse le chiffrement ?

Si le client utilise WPA[2]-{802.1X,Enterprise} et est mal configuré

802.11w-2009

Supposé réparer le problème ... mais pas utilisé encore (Windows 8 ?)

Le chiffrement

WPA[2]-{PSK,Personal}

Si le 4-way handshake est enregistré (facile avec une déauthentification) :
Possible de chercher la clé utilisée par force brute
→ Utiliser des mots de passe VRAIMENT aléatoires

Faille dans WPS (WiFi Protected Setup)
→ Désactiver

Les réseaux cachés

Sécurité par obscurité ...

Il est possible pour un AP de ne pas diffuser son ESSID
Exemple clair de technique n'apportant pas de la sécurité mais une *impression de sécurité*
Très très mauvais principe

Pb

Le WiFi n'est pas pensé pour cacher l'ESSID et même si conceptuellement ça aurait pu avoir du sens ... ça n'apporte rien en pratique

ESSID transmis lors d'une nouvelle association $\rightarrow$ déauth.

Plan

Catégories d'utilisateurs

Invités

Besoin d'accès à l'extérieur (ports classiques)

Utilisateurs internes lambda

Besoin d'accès à l'extérieur (ports classiques)
Aux outils de l'intranet (web, fs, etc.)
Accès aux imprimantes

Power users

Utilisateurs lambda + extérieur sur d'autres ports

Le portail captif

Principes

1. Mettre en place un réseau ouvert avec un nom parlant
2. Mettre en place un renvoi systématique vers une page d'accueil
3. Authentifier les utilisateurs avec un serveur tiers (par ex. LDAP)
4. Informer les utilisateurs des conditions et des dangers

Redirection

Plusieurs options :

- Redirection par HTTP : Interception des requêtes HTTP et renvoi d'une réponse HTTP 302 (redirection)
- Redirection DNS : En deux pas
  - Rediriger toutes les requêtes DNS vers un serveur qu'on contrôle
  - Répondre avec ce serveur toujours avec l'adresse IP de notre portail

→ Lèvera des alertes pour les protocoles sécurisés

Plan

Utilisation par usurpation

Authentification

Dans un premier temps page https + auth. utilisateur locale ou distante

Puis, tant que MAC/IP/MAC+IP est inchangé on prend

Usurpation

MAC : Plus simple en Wi-Fi que dans un réseau commuté
IP : Comme toujours, par ARP poisoning (e.g. sur le routeur d'entrée)
MAC + IP ? Plus compliqué ... Que se passe-t-il si on fait :

- Un ARP poisoning pour usurper l'IP
- Du MAC spoofing uniquement pour l'envoi

```
# modprobe bridge
# brctl addbr br0; brctl addif br0 ath0
[configure bridge interface br0]
# ebtables -t nat -A POSTROUTING -o ath0 -d $FW_MAC -j snat -to-source $B_MAC
```

Merci Cédric !

Tunnel DNS : principe

Pré-requis

Acheter un domaine et mettre en place un serveur DNS pour celui-ci

Principe : fuite par canal caché

On installe sur notre machine un client DNS qui

- Prend en entrée des données à envoyer (par ex. des paquets IP)
- Crée des requêtes DNS valides pour notre domaine
- Introduit dans certains champs les données à envoyer (μ-fragments)

Les requêtes doivent être valides du point de vue du DNS local

On installe un serveur DNS sur le net qui

- Extrait des champs des requêtes et reconstruit les données
- Les envoie et reçoit les réponses associées
- Introduit les données reçues dans certains champs des réponses DNS

Les réponses doivent être valides du point de vue du DNS local

Tunnel DNS : pratique

Iodine

`http://code.kryo.se/iodine`
Tout ce qu'il faut (client, serveur, config SE)

Configuration du DNS

```
t1              IN      NS      t1ns.mydomain.com.          ; note the dot!
t1ns            IN      A       10.15.213.99
```

Performances

En upload ... qqs kilobits/s
En download ... entre qqs kilobits/s et 1Mbit/s

Autres moyens

Tunnel ICMP

Si on peut émettre en ICMP on peut ajouter un payload pour les données
Plus performant que le tunnel DNS (e.g. `icmptx`)...

... Mais ICMP souvent bloqué

Ports ouverts en TCP/UDP

Tester si des ports sont ouverts avant l'authentification (e.g. DNS=53)
Si c'est le cas essayer de faire passer un autre protocole par là

Proxy HTTP

Des fois il y a un proxy HTTP dans le réseau ...
Tester le portail lui-même ! !

Attaques sur les autres stations

Écoutes

Tout ouvert et pas de commutation (canal commun) ...

Injection

Soit normalement si l'AP accepte les requêtes ToDS
Soit en spoofant le bit FromDS ...

Plan

Un historique rapide

Origine

Nombreuses attaques sur WEP :

- Un système de chiffrement dangereux (RC4)
- Une mauvaise gestion des clés (vecteurs d'initialisation petits)
- Un contrôle d'intégrité ridicule (CRC)

Norme draft (brouillon) 802.11i en 2003
Norme full 802.11i (ou 802.11i-2004) en 2004

La sécurité dans WPA[2]

Confidentialité et intégrité

- WPA : TKIP Temporary Key Integrity Protocol (basé sur RC4)
- WPA2 : CCMP Counter-mode with Cbc-Mac Protocol (basé sur AES)

Authentification

- Personal : PSK Pre-Shared Key authentication
  - Présent depuis la norme 802.11 (1999)
  - Bon pour la maison et les tous petits bureaux
  - Quel que soit le contexte un secret commun est une mauvaise idée
- Enterprise : 802.1x
  - Introduit dans le draft 802.11i (2003)
  - Authentification par utilisateur
  - Utilise un serveur d'authentification typiquement RADIUS
  - Plus complexe à mettre en oeuvre mais indispensable

Failles

TKIP

Considéré comme obsolète (par l'IEEE depuis 2009)
Vulnérable à plusieurs attaques

WPA short packet spoofing

- Découverte par Beck-Tews en 2008
  - Nécessite que la QoS soit activée
  - Ne dévoile pas la clé de chiffrement
  - Permet d'introduire qqs faux paquets
- Améliorée par Ohigashi-Morii en 2009
  - Ne nécessite plus de la QoS
  - Il faut faire un MITM

Wi-Fi Protected Setup

Procédure pour se connecter sans avoir à mémoriser un mdp long

- Introduit une faille importante dans WPA[2] $\rightarrow$ désactiver

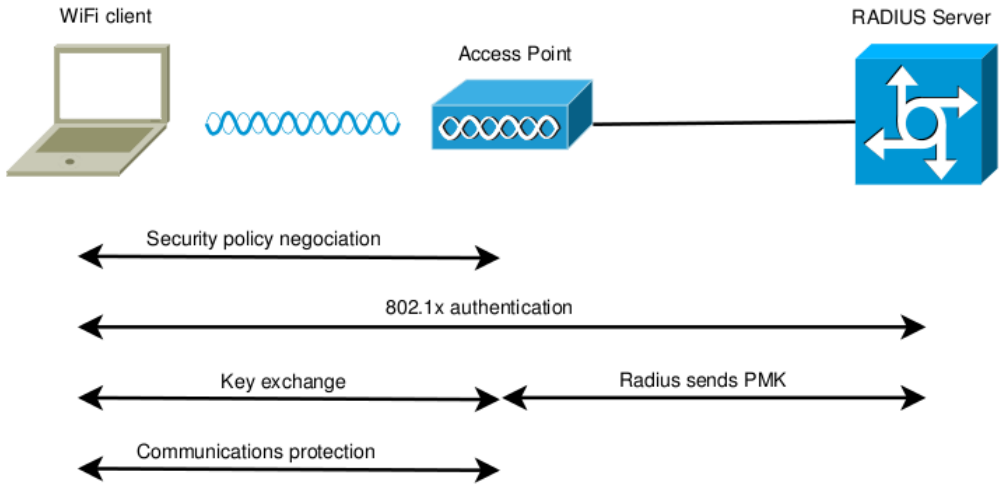
Plan

Robust Security Network Association (RSNA)

C'est quoi ?

La bonne manière de s'associer à un AP selon 802.11i-2004

$\rightarrow$ Il faut suivre le bon protocole et utiliser les bons mécanismes crypto



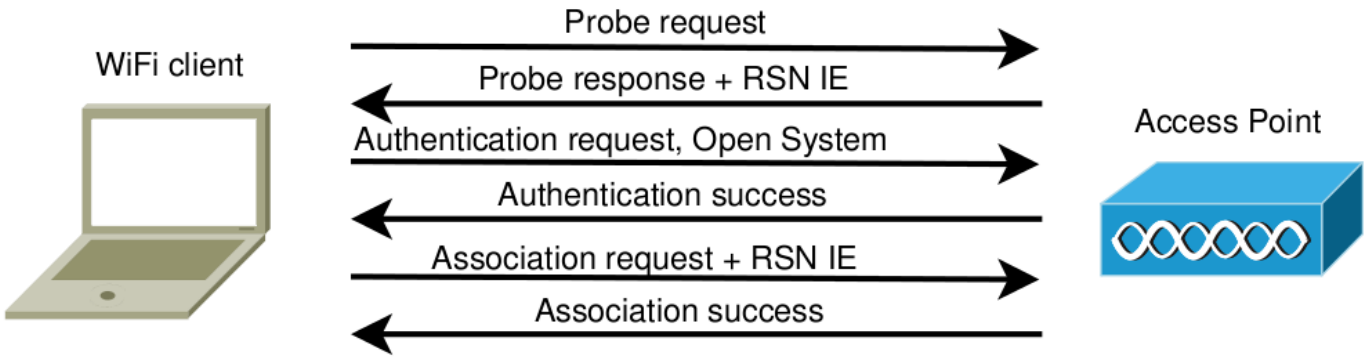
Principe

Décrit dans la figure mais ... 802.1X est sauté si on utilise un PSK

Robust Security Network (RSN)

Seule option pour s'associer : RSNA

Security Policy Negotiation



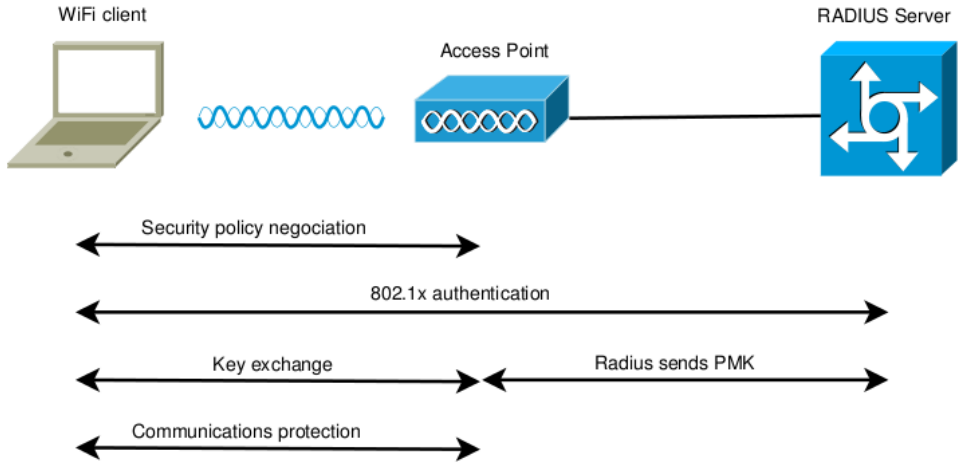
Robust Security Network Information Element (RSN IE)

- Bloc d'informations présent ssi l'AP accepte les RSNAs
- Contient les moyens d'authentification et crypto proposés
- Présent également dans les beacons de l'AP

Ce n'est qu'une négociation (sécurisée a posteriori)

- Open System Authentication
  - Marche toujours
  - Maintenu pour préserver la machine à états de 802.11
- Association : ne marche que si les RSN IEs permettent un accord

Authentification



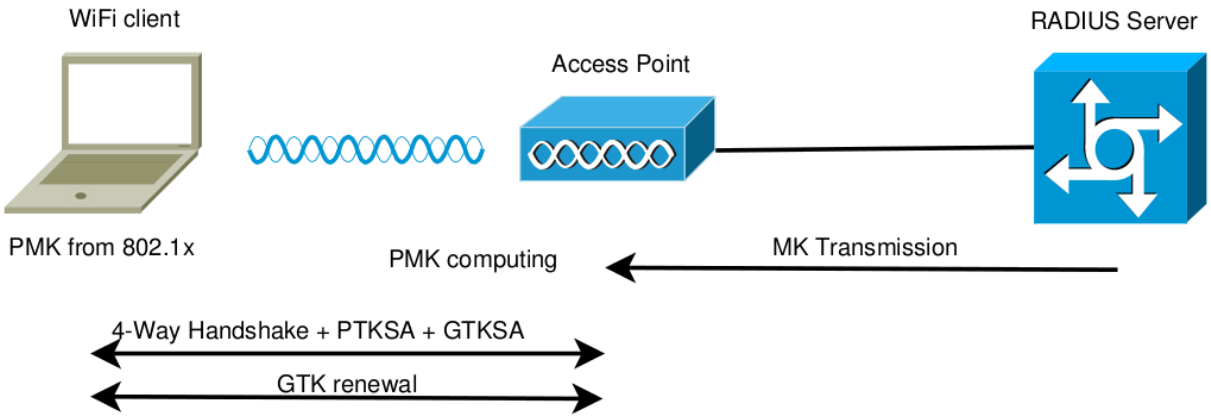
802.1X ...

802.11i-2004 impose que pour 802.1X on utilise une méthode EAP donnant en cas d'authentification réussie un secret commun au supplicant et à l'AS.

... ou pas

Si le protocole d'authentification négocié est PSK, le mot de passe du réseau remplace le secret commun d'EAP

Négociation des clés (1/2)

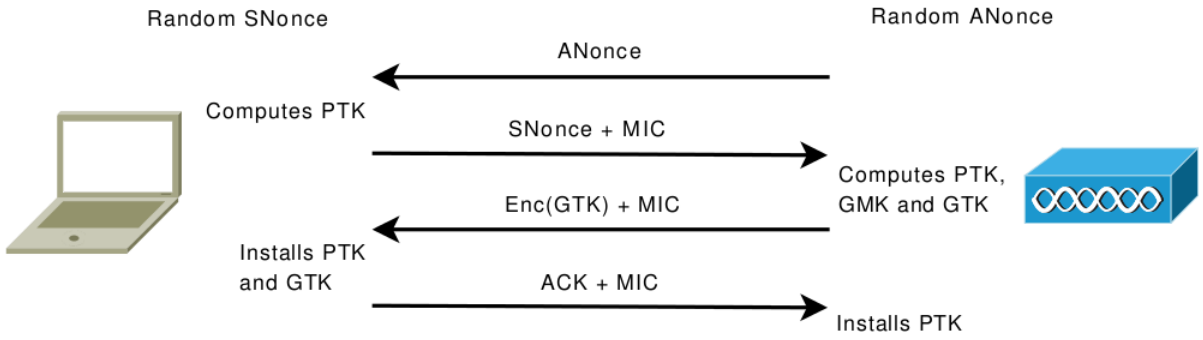


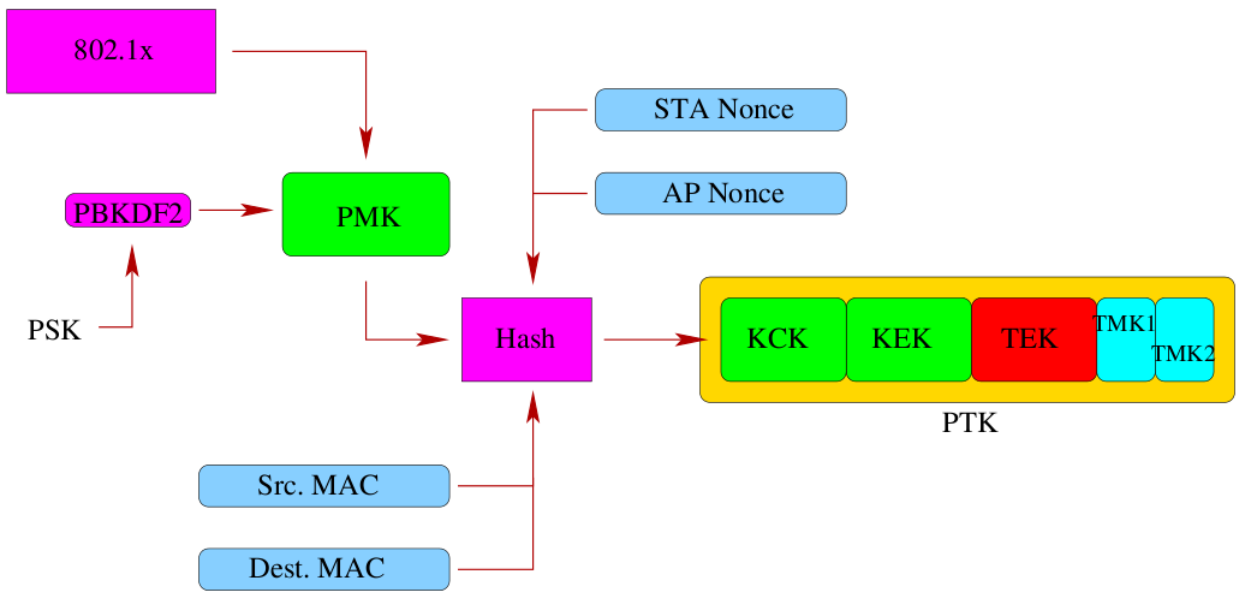
Du secret aux clés

Une fois qu'on a le secret commun (par 802.1X ou PSK) on fait

- Un handshake pour échanger un peu d'aléa
- Une dérivation pour obtenir une clé de session unique
- Un envoi d'une clé de groupe pour les broadcasts

Négociation des clés (2/2)





Plan

Fin !

Prochain cours

802.1X (considérations de sécurité)
Extensible Authentication Protocol