WPA : une réponse à l'insécurité du WEP ?

Michel Chilowicz Jean-Paul Sov

Master 2 Informatique Recherche – Université de Marne-la-Vallée

31 janvier 2006

Plan

1 Le WEP et ses attaques

2 Authentification 802.1X

3 Le WPA

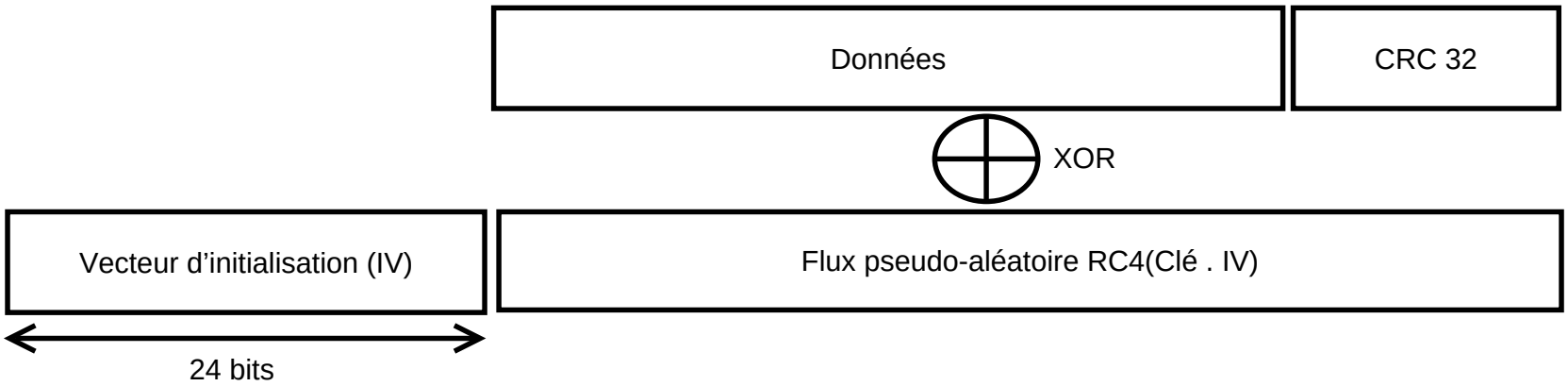
Introduction

- Protocole de sécurité WEP (Wired Equivalent Privacy) pour l'authentification et le chiffrement de trames Wi-Fi défini dans IEEE802.11.
- Procédé 802.1X pour l'authentification (serveur RADIUS).
- Protocole de sécurité Wi-Fi WPA et WPA2 (utilisation de l'AES).
- WPA2 avec 802.1X apportent-t-ils une sécurité acceptable ?

Objectifs et fonctionnement du protocole WEP

- Objectif : garantir l'authentification, la confidentialité et l'intégrité des communications Wi-Fi.
- Algorithme : flux RC4 pour le chiffrement (avec combinaison XOR avec le clair).
- Somme de contrôle : algorithme polynomial CRC32 (chiffré par RC4).

Trame WEP


Données
CRC 32
XOR
Vecteur d'initialisation (IV)
Flux pseudo-aléatoire RC4(Clé . IV)
24 bits

- Clé RC4 de 40 ou 104 bits.
- Vecteur d'initialisation (IV) de 24 bits.
  - Seulement 2^{24} IV différents (attaque sur collisions).
  - Politique de choix des IV (séquentiel, aléatoire, remise à zéro) ?

Authentification

- Authentification ouverte (par connaissance de SSID).
- Authentification défi-réponse :
  1. Demande d'authentification sur l'AP.
  2. Communication par l'AP d'un aléa a de 128 bits.
  3. Le client retourne $[IV, c_k(a), crc32(IV, c_k(a))]$
  4. L'AP vérifie la trame ($c_k(a)$ et la somme de contrôle) et autorise (ou non) l'association.

Récupération du SSID

- Diffusion du SSID désactivable.
- SSID récupérable par espionnage du trafic.

Collisions du vecteur d'initialisation

- IV de 24 bits $\longrightarrow 2^{24}$ IV.
- La connaissance du clair d'une trame permet de déchiffrer une autre trame utilisant le même IV.
- Utilisation de dictionnaires de déchiffrement pour stocker les flux RC4 avec clair choisi.

Injection et modifications de trames

- Connaissance d'un couple (IV, flux RC4) $\rightarrow$ injection de trames.
- Linéarité de CRC32 $\rightarrow$ modification de trames en aveugle (aucune connaissance préalable nécessaire).

Authentification avec clé partagée

- Capture d'aléa en clair et chiffré (avec IV) lors de l'authentification $\rightarrow$ Déduction d'un couple (IV, flux RC4).
- Authentification possible avec la connaissance d'un couple (IV, flux RC4).
- Authentification ouverte (paradoxalement) préférable.

Attaque par clé faible RC4

- Méthode cryptanalytique proposée par Fluhrer, Mantin et Shamir.
- Existence de clés faibles pour certains IV.
  - Environ 9000 IV sur 2^{24} sont faibles.
- Attaques pratiques facilitées (moins de paquets nécessaires).
- Parade : éviter l'utilisation des IV faibles.
- Utilisée par l'attaque statistique de KoreK (logiciel Aircrack).

Le 802.1X

Protocole d'authentification (mutuelle) entre une machine (client) et un commutateur réseau (switch filaire ou point d'accès Wi-Fi).
Possibilité d'utilisation en association avec le WEP.

Modes non-authentifié et authentifié

- Mode non-authentifié :
  - Accès limité par le point d'accès au serveur d'authentification.
- Mode authentifié :
  - Accès aux ressources du réseau après le succès de l'authentification.

Ré-authentification et pré-authentification

Ré-authentification

Possibilité de fixer une durée de validité de session.
Ré-authentification nécessaire à expiration.
Utile pour changer de clé WEP.

Pré-authentification

Adressage de trames EAP d'authentification vers un point d'accès utilisable ultérieurement.
Permet une itinérance rapide.

Quelques techniques d'authentification

- Password Authentification Protocol (PAP) : nom d'utilisateur et mot de passe.
- Challenge Handshake Authentification Protocol (CHAP) : défi/réponse (hachage MD4).
- Transport Layer Security (TLS) : authentification mutuelle avec certificat.
- Subscriber Identification Service (SIM) : authentification par carte à puce.

Authentification EAP-TLS

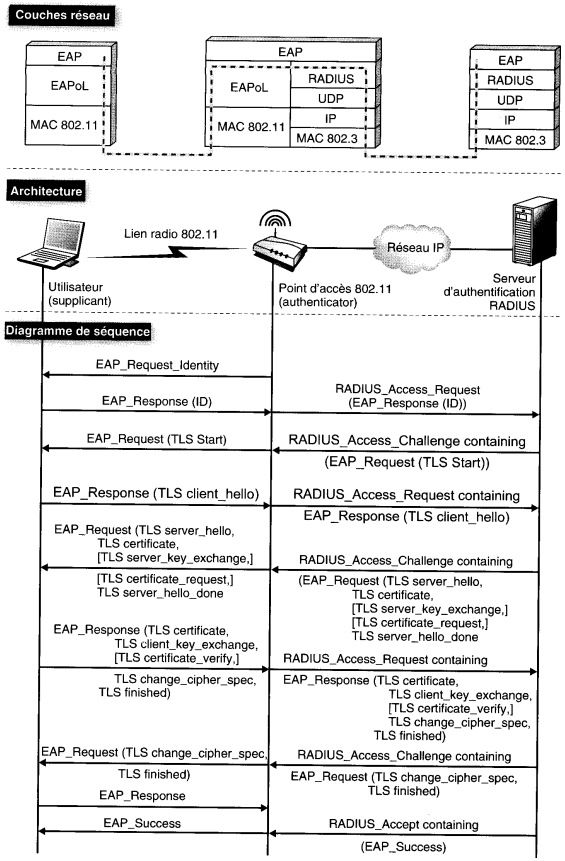


Figure: Echange EAP-TLS

Faiblesses de EAP-TLS

Vérification de validité du certificat

Nécessité de contacter OCSP pour vérifier la non-révocation du certificat.

- Aisé pour le serveur.
- Mais le client doit accepter l'authentification *puis* vérifier.

Attaque par déni de service

Envoi de nombreux messages *SERVER_HELLO* au client : saturation de la mémoire du client.

Présentation du WPA

- Souci de compatibilité avec le WEP.
  - Encapsulation WEP des trames, conservation de RC4.
  - Mise à jour du firmware du matériel.
- Usage d'un compteur de trames de 48 bits pour IV.
- Usage d'une clé dynamique temporaire avec TKIP.
- Ajout d'un procédé MIC Michael avec compteur de trame à CRC32.

Authentification par poignée de main en 4 temps

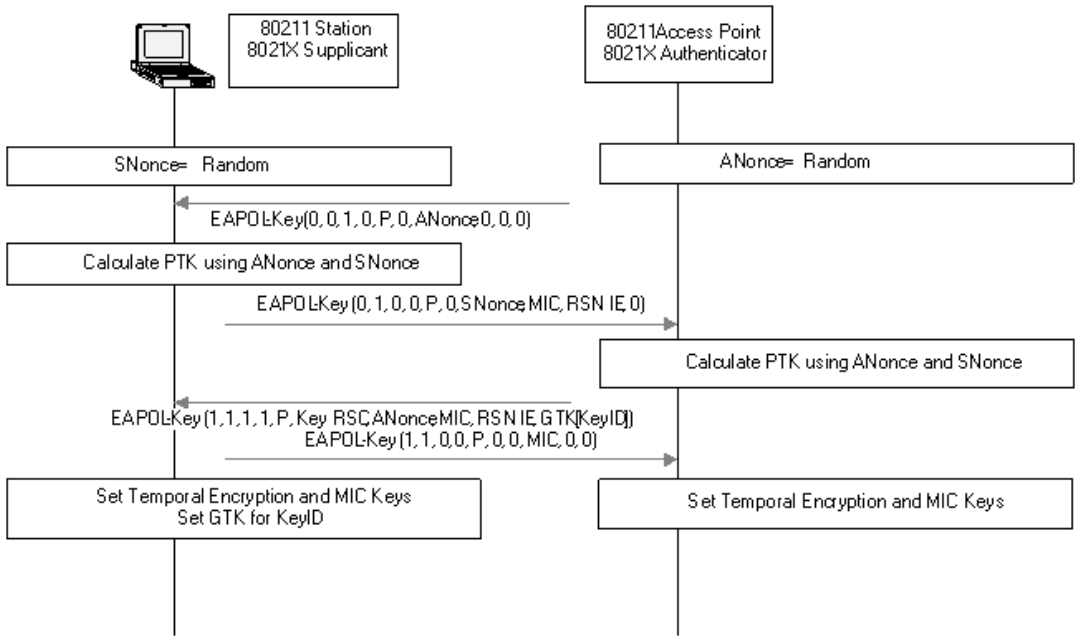


Figure: La poignée de main en 4 temps du WPA[4]

Utilisation de la *Temporal Key* (TK)

- Une clé-maître est convenue par authentification EAP.
- Des clés temporaires (TK) sont communiquées par l'AP à intervalle régulier (tous les 2^{16} trames).
  - Évite les collisions d'IV

Temporal Key Integrity Protocol (TKIP)

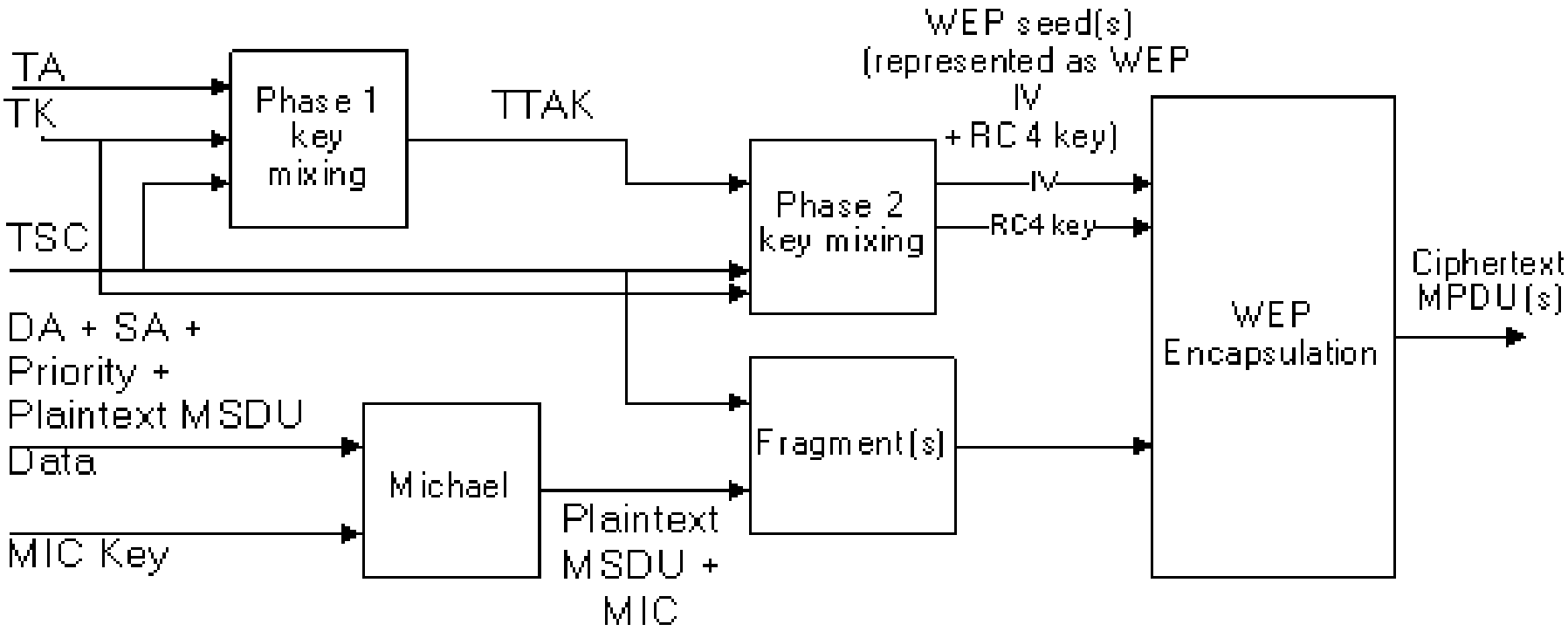


Figure: Mécanisme de chiffrement TKIP[4]

Format d'une trame TKIP

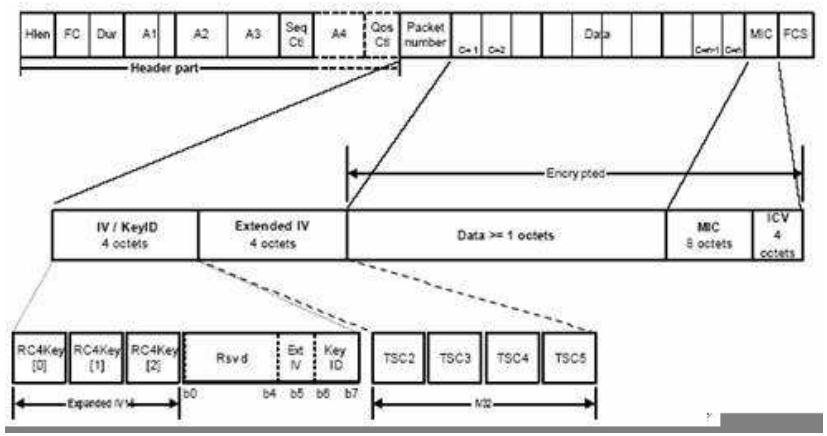


Figure: Trame TKIP[4]

Génération de la Per Packet Key

1. Génération de la TKIP mixed Transmit Address and Key (TTAK).
   Éléments utilisés par la fonction de mixage :
   - Clé temporaire TK.
   - Adresse MAC 48 bits de l'émetteur TA.
   - 16 bits du compteur de trame 48 bits TSC.

Génération de la Per Packet Key

1. Génération de la TKIP mixed Transmit Address and Key (TTAK).
   Éléments utilisés par la fonction de mixage :
   - Clé temporaire TK.
   - Adresse MAC 48 bits de l'émetteur TA.
   - 16 bits du compteur de trame 48 bits TSC.
2. Génération de la clé PPK de 128 bits $(24 + 104)$ par mixage :
   - du TTAK,
   - et de 32 bits du TSC.

Génération du MIC

Utilisation pour la génération du MIC avec l'algorithme Michael :

- L'adresse MAC de l'expéditeur.
- L'adresse MAC du destinataire.
- La priorité de la trame.
- Les données MSDU (dont longueur de trame)
  - Protection contre l'ajout de données
- Le texte en clair

Forces et faiblesses de Michael

Un algorithme MIC économe en ressources CPU...

Particulièrement adapté pour les microprocesseurs de cartes et points d'accès Wi-Fi
(seulement quelques cycles par octet).

Forces et faiblesses de Michael

Un algorithme MIC économe en ressources CPU...

Particulièrement adapté pour les microprocesseurs de cartes et points d'accès Wi-Fi
(seulement quelques cycles par octet).

...mais peu résistant

- Attaque par force brute : 2^{64} tentatives pour forger un MIC.
- Michael conçu pour 2^{20} tentatives.
- Émission de 2^{20} paquets (dont 1 valide) en une minute.
  - Protection par dé-association puis délai de 1 min si 2 paquets forgés en 1s $\longrightarrow$ risque de DoS.

Description de l'algorithme Michael

- $(L, R) := (K_1, K_2)$
- Pour i de 1 à n faire
  - $L := L$ XOR M_i
  - $(L, R) :=$ b(L, R)
- Retourner le MIC (L, R)

b applique des rotations et additions binaires.

Le mode PSK

Utilisation d'une clé PSK 256 bits statique pour les environnements où un serveur RADIUS est trop contraignant (maison, SoHo, ...).

Dérivation de la PSK d'une phrase de passe

Phrase de passe $\longrightarrow$ PSK de 256 bits

$PSK = PBDKF2(phraseDePasse, ssid, longueurSSid, 4096, 256)$
PBDKF2 : itération 4096 fois d'un HMAC-SHA1 sur le SSID avec la phrase de passe.

Attaque par dictionnaire

- En anglais, 1 caractère = 2,5 bits : 102 caractères pour une entropie de 256 bits.
- Généralement, utilisation de phrases de passe courtes :
  - Attaque par dictionnaire.
  - Pré-constitution de dictionnaires de hachés pour SSID standard.

Quelques mots sur le WPA2

Utilisation du protocole CCMP à la place de TKIP.

- Nouveau protocole indépendant de WEP
- Utilisation de AES (Rjindael).
- Utilisation de CBC-MAC pour le MIC de 64 bits (pas d'attaque réaliste).

En conclusion...

- WEP :
  - failles de conception,
  - faiblesses de RC4.
- WPA (TKIP) : amélioration de la sécurité
  - clé temporaire,
  - compteur de trames.
- WPA2 (CCMP) :
  - remplacement de RC4 par AES (plus solide),
  - MIC généré avec CBC-MAC.
- Problèmes non résolus par WEP, WPA{1,2} :
  - provocation de dé-associations/re-associations (DoS),
  - brouillage radio.
  - Pas de garantie de haute-disponibilité sur un réseau Wi-Fi.

Références


B. Aboba and D. Simon.
RFC 2716 : PPP EAP TLS authentication protocol, 1999.


S. Fluhrer, I. Mantin, and A. Shamir.
Weaknesses in the key scheduling algorithm of RC4.
Selected Areas in Cryptography, 2001.


IEEE.
IEEE standard 802.1x, 2001.


IEEE.
IEEE standard 802.11i – part 11 – amendment 6, 2004.


Guy Pujolle.
Sécurite Wi-Fi.
Eyrolles, 2004.