14/02/2024

Réalisation professionnelle

La mise en place d'une solution Wifi Sécurisée

Etude comparative des différents protocoles Wi-Fi

ASSURMER

EVIEUX Lucas – COTTIN Elouan – BOUVIER Tristan
BTS SIO SISR A2

I. Etude Comparative des différents protocoles de sécurité Wifi

A. Différents protocoles de sécurité

Il existe 4 principaux protocoles de sécurité Wifi :

- Wired Equivalent Privacy (WEP)
- WiFi Protected Access (WPA)
- WiFi Protected Access 2 (WPA2)
- WiFi Protected Access 3 (WPA3)

B. Fonctionnement du protocole Wired Equivalent Privacy

Le protocole de sécurité WiFi WEP a été l'une des premières méthodes de sécurisation du Wifi en 1999.

Lors de la configuration initiale du réseau WiFi, une clé WEP est choisie et configurée sur le routeur ou le point d'accès sans fil.

Cette clé est utilisée pour chiffrer les données transmises sur le réseau WiFi. Elle peut être de 64 ou 128 bits de longueur.

Pour s'authentifier, les périphériques sans fil qui tentent de se connecter au réseau doivent connaître la clé WEP pour être autorisés à accéder au réseau. Cette clé doit généralement être entrée manuellement dans les paramètres du périphérique.

Le chiffrement utilisé par WEP est RC4 (Rivest Cipher 4). RC4 est un algorithme de chiffrement symétrique, la même clé est utilisée pour le chiffrement et le déchiffrement des données.

Un vecteur d'initialisation (IV ou Initialization Vector) est ajouté aux données avant le chiffrement. Ce vecteur d'initialisation est un nombre aléatoire qui est envoyé avec chaque paquet de données pour garantir que même si les données sont les mêmes, les paquets chiffrés seront différents.

Le protocole WEP présente cependant plusieurs faiblesses de sécurité importantes.

L'une des plus notables est la faible longueur de la clé (64 ou 128 bits), qui rend les attaques par force brute plus pratiques.

De plus, la mauvaise gestion des vecteurs d'initialisation (IV) a permis le développement d'attaques plus sophistiquées, telles que les attaques par réinjection de paquets.

C. Fonctionnement du protocole WiFi Protected Access

Le protocole de sécurité WPA est conçu en 2003 pour sécuriser les réseaux Wifi en utilisant des méthodes de chiffrement et d'authentification robustes et pour remédier aux faiblesses de WEP.

WPA utilise principalement le protocole de chiffrement TKIP (Temporal Key Integrity Protocol).

Cette méthode de chiffrement génère une nouvelle clé de chiffrement pour chaque paquet de données envoyé, ce qui rend les attaques de type "rejouer" plus difficiles.

Cette rotation des clés renforce la sécurité par rapport à WEP, où la même clé est utilisée de manière statique.

Pour l'authentification, WPA utilise un protocole d'authentification appelé EAP (Extensible Authentication Protocol) pour vérifier l'identité des utilisateurs souhaitant accéder au réseau Wifi.

L'authentification est souvent gérée via un serveur RADIUS (Remote Authentication Dial-In User Service), qui centralise et gère les informations d'identification des utilisateurs.

Les utilisateurs doivent fournir un nom d'utilisateur et un mot de passe valides pour se connecter au réseau Wi-Fi, ce qui renforce la sécurité en comparaison avec WEP, qui utilisait des clés partagées statiques.

Le protocole présente cependant des faiblesses :

- L'utilisation de TKIP car ce protocole a hérité de certaines vulnérabilités de l'ancien protocole WEP
- Une vulnérabilité aux réinjections de paquets
- Une faiblesse dans la vérification de l'intégrité des messages, en effet, le mécanisme pour protéger l'intégrité des données peut être compromis, facilitant certaines ainsi attaques
- Une faiblesse dans le processus d'authentification, les méthodes d'authentification de WPA peuvent être vulnérables, notamment si la méthode utilisée est plus ancienne et moins sécurisée.
- Une vulnérabilité aux attaques de dictionnaire contre le WPA-PSK : Les clés pré-partagées, si elles sont faibles, peuvent être devinées par des attaques de dictionnaire ou par force brute.

D. Fonctionnement du protocole WiFi Protected Access 2

Le protocole de sécurité WPA2 est une amélioration du protocole WPA conçu pour sécuriser les réseaux Wifi. WPA2 a été lancé en 2004 et est devenu la norme de sécurité recommandée pour les réseaux Wifi. Il utilise des méthodes de chiffrement avancées pour protéger les données transmises entre les appareils et le point d'accès Wifi.

WPA2 offre deux modes d'authentification :

- WPA2-Personal (ou PSK, Pre-Shared Key) : Convient pour les réseaux domestiques et les petites entreprises. Il utilise une clé partagée ou un mot de passe que tous les utilisateurs doivent connaître pour se connecter au réseau. La clé est utilisée pour initialiser la connexion et garantir que seuls les utilisateurs autorisés peuvent accéder au réseau.
- WPA2-Enterprise : Utilisé dans les environnements d'entreprise, ce mode repose sur un serveur d'authentification 802.1X pour valider les identifiants des utilisateurs avant qu'ils puissent accéder au réseau. Cela permet une gestion centralisée des accès et une sécurité accrue.

WPA2 utilise le protocole de chiffrement AES (Advanced Encryption Standard) dans un mode appelé CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol), remplaçant le TKIP utilisé par WPA pour un niveau de sécurité accru.

AES est un standard de chiffrement robuste et largement reconnu.

Le fonctionnement du protocole :

Négociation de la clé : Lorsqu'un appareil tente de se connecter à un réseau WPA2, le processus commence par une négociation de clé appelée "Four-Way Handshake".

Ce processus vise à confirmer que l'appareil et le point d'accès possèdent la clé pré-partagée correcte (dans le cas de WPA2-Personal) ou à établir une nouvelle clé d'encryption après une authentification réussie (dans le cas de WPA2-Enterprise).

Four-Way Handshake : Ce mécanisme permet d'établir une nouvelle clé d'encryption, appelée Pairwise Transient Key (PTK), qui est utilisée pour protéger les données échangées pendant la session. Le handshake assure également que la clé partagée n'est pas compromise pendant le processus d'authentification.

WPA2 offre une protection robuste contre de nombreuses formes d'attaques sur les réseaux Wifi, y compris les attaques de réinjection et de déchiffrement.

Cependant, WPA2 n'est pas infaillible, par exemple, en 2017, une vulnérabilité appelée KRACK (Key Reinstallation Attacks) a été découverte, permettant à un attaquant de contourner le chiffrement WPA2 sous certaines conditions

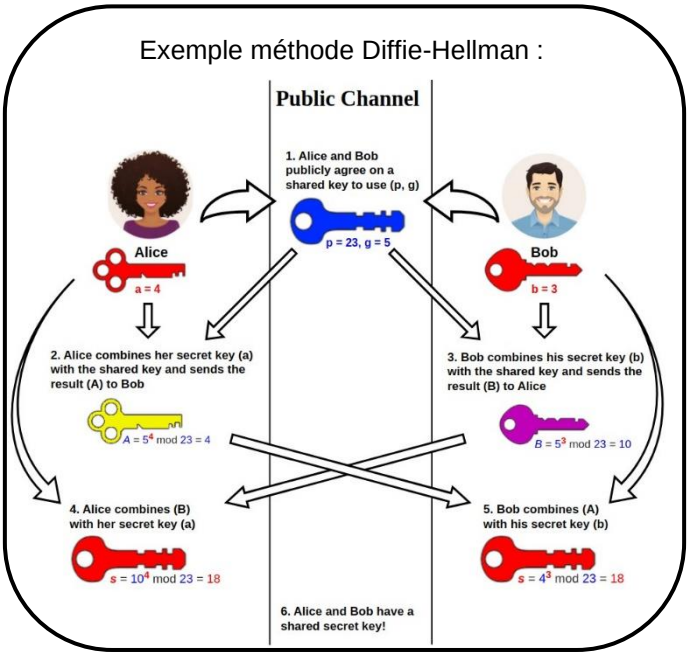
E. Fonctionnement du protocole WiFi Protected Access 3

Le protocole de sécurité WPA3 est conçu pour renforcer la sécurité des réseaux sans fil par rapport à ses prédécesseurs, WEP, WPA et WPA2.

WPA3 introduit un protocole d'authentification similaire à la méthode de Diffie-Hellman pour établir une connexion sécurisée entre le périphérique client et le point d'accès Wi-Fi.

Il utilise le protocole Simultaneous Authentication of Equals (SAE) ou "Dragonfly" qui protège contre les attaques par dictionnaire et de force brute.

Exemple méthode Diffie-Hellman :



WPA3 utilise le protocole de chiffrement Galois/Counter Mode (GCMP-256) pour le chiffrement des données, qui offre une meilleure sécurité que le chiffrement basé sur le protocole CCMP utilisé dans WPA2.

Le chiffrement GCMP-256 est basé sur l'algorithme de chiffrement de bloc AES-256.

WPA3 propose une protection renforcée contre les attaques de type "brute-force" grâce à l'authentification SAE, qui rend ces attaques beaucoup plus difficiles à exécuter efficacement.

Cette méthode d'authentification offre également la sécurité de la "forward secrecy", ce qui signifie que même si une session est compromise, les sessions futures ne le seront pas.

F. Tableau comparatif des protocoles

Caractéristique	WEP	WPA	WPA2	WPA3
Année de lancement	1999	2003	2004	2018
Méthode de chiffrement	RC4	TKIP (RC4)	AES (CCMP)	AES (GCMP) ou TKIP
Intégrité des données	CRC-32 (facilement falsifiable)	MIC (Michael) pour protéger contre les attaques de falsification	CCMP pour une protection renforcée	CCMP-256 pour une protection renforcée
Authentification	Authentification ouverte ou partagée	PSK (Pre-Shared Key) ou EAP (Extensible Authentication Protocol)	PSK ou EAP	Similaire à WPA2, plus SAE (Simultaneous Authentication of Equals)
Sécurité	Faible, cassé en quelques minutes	Meilleure que WEP, mais des vulnérabilités ont été découvertes	Très sécurisé, recommandé jusqu'à l'introduction de WPA3	Encore plus sécurisé, résiste aux attaques offlines de déchiffrement des mots de passe
Mode d'opération	Obsolète	Mode WPA-Personal (PSK) et WPA-Enterprise	Idem, avec la recommandation d'utiliser WPA2-Enterprise pour les entreprises	WPA3-Personal (avec SAE), WPA3-Enterprise pour une sécurité renforcée
Compatibilité	Large, avec les anciens appareils	Bonne, avec la plupart des appareils depuis 2003	Très bonne, standard pour les appareils modernes	Doit être supporté, peut ne pas être compatible avec les appareils plus anciens
Vulnérabilités notables	Nombreuses, dont l'attaque IV courte	Attaques contre TKIP, comme l'attaque chopchop	KRACK (Key Reinstallation Attacks) dans certaines conditions	Aucune majeure connue à la date de ma dernière mise à jour, mais nécessite du matériel et des logiciels à jour pour la meilleure sécurité