Projet de cryptographie M1

Étude du WPA3

Réalisé par :
Ilyes ACHAQ

Encadré par :
Mr CHENEVERT

Année académique : 2024-2025

Table des matières

Table des matieres **2**

1 Introduction : Contexte **3**

2 Détails techniques du WPA3 **4**
2.1 Authentification renforcée avec Simultaneous Authentication of Equals (SAE) . 4
2.1.1 Fonctionnement du SAE (Dragonfly Key Exchange) 4
2.1.2 4-Way Handshake 6
2.2 Amélioration de la sécurité avec AES-GCMP 7

3 Faiblesses et attaques connues **8**
3.1 Attaques Dragonblood 8
3.1.1 Attaque par Canal Caché Basée sur le Temps (Timing Side-Channel Attack) 8
3.1.2 Attaque par Canal Caché Basée sur le Cache (Cache Side-Channel Attack) 8
3.1.3 Attaques de Rétrogradation (Downgrade Attack) 9
3.2 Contre mesures 9
3.2.1 Désactivation de la mise en cache 9
3.2.2 Contrer Timing et Cache Attacks 9
3.2.3 Limitation des tentatives d'authentification 9

4 Conclusion **10**

5 Sources **10**

1 Introduction : Contexte

La cybersécurité est devenue un domaine stratégique dans le monde moderne, où les réseaux sans fil, en particulier les connexions Wi-Fi, sont au cœur de nos vies numériques. Que ce soit dans un environnement domestique, professionnel ou public, la plupart des appareils utilisent des réseaux Wi-Fi pour se connecter à Internet. Cette ubiquité des connexions sans fil, combinée à la multiplicité des appareils connectés (bracelet connecté, machine à laver connectée, patate connectée...), fait des réseaux sans fil un point d'entrée privilégié pour les cyberattaques. Dans ce contexte, la sécurité de ces réseaux est essentielle pour protéger la confidentialité, l'intégrité et la disponibilité des données qui circulent sur ces canaux.

Le Wi-Fi Protected Access (WPA) a été introduit au début des années 2000 pour pallier les failles majeures du protocole WEP (Wired Equivalent Privacy), qui utilisait un chiffrement par flux basé sur le RC4 avec une clé de 40 bits et un vecteur d'initialisation de 24 bits. Le WEP était vulnérable à des attaques comme le bit flipping et le brute force, en raison de l'utilisation d'une clé unique pour tout le réseau. Pour améliorer la sécurité, le WPA a intégré le TKIP (Temporal Key Integrity Protocol) avec une clé plus longue de 128 bits et une re-négociation périodique des clés, réduisant les risques associés aux attaques par écoute.
Le WPA2, défini par le standard IEEE 802.11i, a marqué une avancée significative en introduisant le chiffrement par bloc avec l'AES (Advanced Encryption Standard) et le protocole d'authentification par échange à quatre voies (4-way handshake). Cependant, même le WPA2 n'était pas à l'abri, comme l'a montré l'attaque KRACK (Key Reinstallation Attack), permettant de réinstaller des clés de chiffrement sur des appareils vulnérables.

Le développement du WPA3 a été dirigé par la Wi-Fi Alliance, qui s'est appuyée sur des standards déjà établis dans l'industrie des réseaux sans fil, comme ceux définis par l'IEEE (Institute of Electrical and Electronics Engineers). Le standard IEEE 802.11i, par exemple, a définit les méthodes de chiffrement et d'authentification nécessaires pour sécuriser les communications sans fil, et ses principes ont directement inspiré les choix technologiques du WPA3.

L'importance du WPA3 réside dans sa capacité à répondre à plusieurs enjeux :

La protection contre les attaques par interception de paquets : En rendant beaucoup plus difficile l'interception et la décryptage des communications Wi-Fi, WPA3 augmente la sécurité des échanges. L'amélioration de la sécurité dans les environnements publics : Avec l'adoption de mécanismes comme le Simultaneous Authentication of Equals (SAE), le WPA3 rend les réseaux Wi-Fi publics ou partagés beaucoup plus difficiles à compromettre.
L'adaptation à l'Internet des objets (IoT) : Un exemple est l'attaque Mirai de 2016, qui a utilisé des objets connectés mal sécurisés pour créer un botnet massif. Ce botnet a ensuite été utilisé pour lancer des attaques par déni de service distribué (DDoS) sur des sites comme Dyn.

Dans la suite de ce projet, nous examinerons de manière plus détaillée les spécificités techniques du WPA3, ainsi que sur ses forces et ses faiblesses. Nous aborderons également les mécanismes de sécurité intégrés dans ce protocole et la manière dont ils répondent aux attentes.

2 Détails techniques du WPA3

2.1 Authentification renforcée avec Simultaneous Authentication of Equals (SAE)

Le protocole Simultaneous Authentication of Equals (SAE), aussi appelé Dragonfly Key Exchange, est un mécanisme d'authentification par échange de clés appartenant à la famille des PAKE (Password-Authenticated Key Exchange). Le Pre-Shared Key (PSK) utilisé dans WPA2, était vulnérable aux attaques par force brute hors ligne. SAE protège contre ce type d'attaques en utilisant un échange interactif basé sur la cryptographie à courbe elliptique.

2.1.1 Fonctionnement du SAE (Dragonfly Key Exchange)

1. Initialisation des paramètres

— On utilise une courbe elliptique définie par un groupe (G) de grande taille, notée par p (le nombre premier définissant le champ) un générateur g (un point sur la courbe), et un ordre q.
— Les valeurs spécifiques comme p, g, q sont généralement définies à l'avance par des standards tels que edwards25519.

2. Sélection du secret (Alice et Bob)

Les deux parties, Alice et Bob, partagent un mot de passe P. Ensuite, chaque partie génère un nombre secret aléatoire pour effectuer les calculs suivants :
Alice génère un nombre secret x choisi aléatoirement dans l'intervalle $[1, q-1]$.
Bob génère un nombre secret y choisi aléatoirement dans l'intervalle $[1, q-1]$.

3. Calcul des éléments publics

Alice et Bob effectuent maintenant des calculs pour générer leurs éléments publics respectifs à envoyer à l'autre partie. Ces calculs impliquent l'utilisation d'une transformation du mot de passe en un point de la courbe elliptique.

Alice :
Alice applique un hachage du mot de passe P avec un sel aléatoire N et le générateur g, produisant

$$P_{WE} = H(P, N, g)$$

Ensuite, Alice calcule son élément public T comme suit :

$$T = g^x \times P_{WE}$$

où g^x est la multiplication du générateur g par le secret x, et P_{WE} est ajouté à ce calcul via une addition de points sur la courbe elliptique.

Bob :
Bob applique le même processus pour obtenir une valeur P_{WE} identique, puis calcule son élément public S de manière similaire :

$$S = g^y \times P_{WE}$$

5. Calcul des clés partagées

Alice et Bob échangent leurs valeurs. Après que chacun ait obtenu l'éölément public de l'autre, on peut maintenant calculer la clé partagée en utilisant son propre secret.

Alice :
Alice reçoit S et calcule la clé partagée K_{Alice} comme suit :

$$K_{\text{Alice}} = \left(\frac{S}{P_{\text{WE}}}\right)^x = \left(\frac{g^y \times P_{\text{WE}}}{P_{\text{WE}}}\right)^x = g^{xy}$$

Alice effectue ici une multiplication et une division de points sur la courbe elliptique.

Bob :
Bob reçoit T et calcule la clé partagée K_{Bob} comme suit :

$$K_{\text{Bob}} = \left(\frac{T}{P_{\text{WE}}}\right)^y = \left(\frac{g^x \times P_{\text{WE}}}{P_{\text{WE}}}\right)^y = g^{xy}$$

Tout comme Alice, Bob effectue une multiplication de points sur la courbe elliptique.

Alice et Bob ont donc tous les deux calculé une clé partagée identique $K{=}g^{xy}$

6. Vérification

Une fois la clé partagée K calculée, les deux parties échangent des preuves cryptographiques pour vérifier que chacune d'elles a bien obtenu la même clé, sans révéler directement la clé elle-même. Dans le cadre du WPA3 c'est réalisé avec du HMAC (Hash-based Message Authentication Code) :

Alice :
Alice crée un HMAC du message en utilisant la clé partagée K comme clé secrète :

$$\text{HMAC}_K(\text{message}) = \text{HMAC}(K, \text{message})$$

La preuve $\text{HMAC}_K(\text{message})$ est ensuite envoyée à Bob.

Bob :
Bob crée également un HMAC du même message en utilisant la même clé partagée K :

$$\text{HMAC}_K(\text{message}) = \text{HMAC}(K, \text{message})$$

Bob compare ensuite la preuve reçue d'Alice avec la sienne. Si elles sont identiques, cela signifie qu'ils partagent la même clé K.

Comme nous avons pu le voir, SAE repose sur des principes similaires à ceux du Diffie-Hellman traditionnel, mais avec une différence importante : il utilise des courbes elliptiques. Comme Diffie-Hellman, Dragonfly permet à deux parties de générer une clé partagée sans avoir à la transmettre explicitement.

À ce stade, aucun chiffrement des données n'est encore effectué, l'objectif est uniquement d'établir une clé secrète partagée qui pourra être utilisée pour sécuriser les échanges futurs.

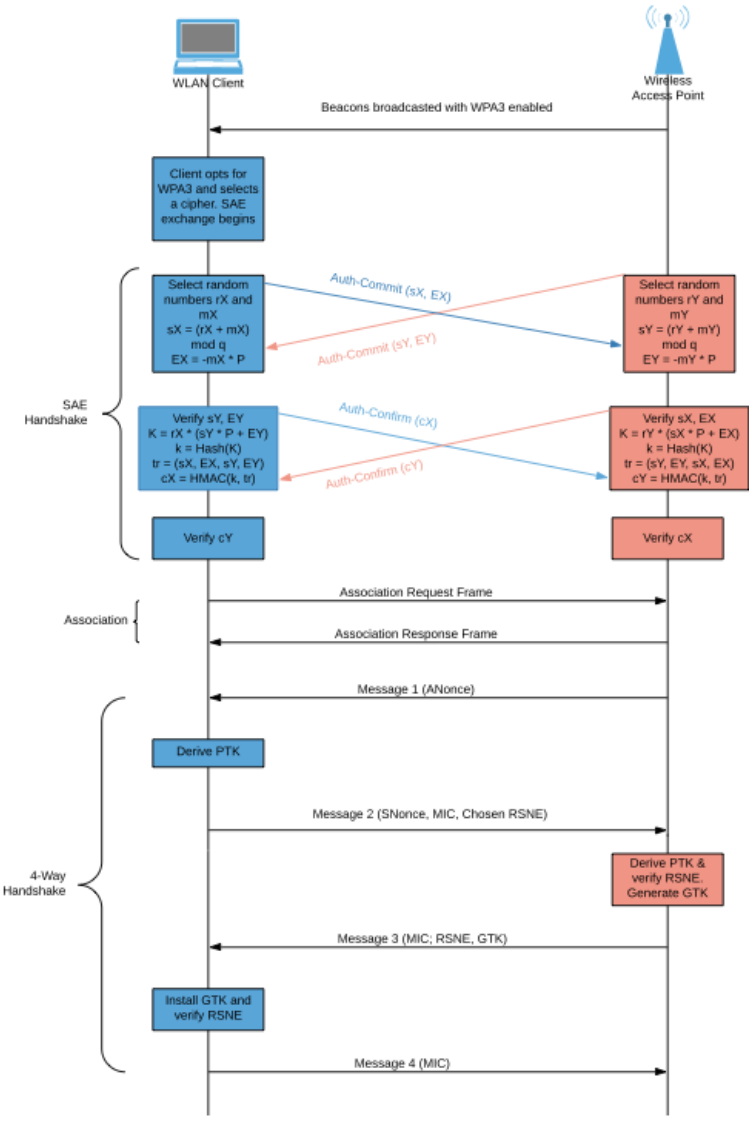
2.1.2 4-Way Handshake

Après avoir terminer le SAE et la délivrance des clés, un 4 way handshake est utilisé pour configurer les clés de chiffrement des communications futures. Cela permet de finaliser l'établissement des clés de session et de vérifier leur validité avant que le chiffrement ne soit vraiment utilisé.

Le 4-way handshake a pour objectif principal de :

- Confirmer que les deux parties possèdent bien la même clé de session.
- Protéger contre les attaques de type replay en synchronisant les numéros de séquence des paquets.
- Distribuer de nouvelles clés de chiffrement (pairwise master key, PMK) pour protéger les données échangées.

Voici un schéma résumant du protocol complet :



Les 4 étapes du 4 way handshake sont :
Message 1 : Le point d'accès envoie son nonce (ANonce) au client.
Message 2 : Le client répond avec son nonce (SNounce), la clé de session, et un MIC pour l'intégrité.
Message 3 : Le point d'accès vérifie et envoie un message confirmant la clé de session avec un MIC.
Message 4 : Le client confirme la validité de la session, finalisant l'établissement des clés de chiffrement et d'intégrité.

Figure : https://balramdot11b.com/2020/05/17/wpa3-and-dragonfly-sae/

2.2 Amélioration de la sécurité avec AES-GCMP

L'algorithme de chiffrement AES-GCMP (AES-Galois/Counter Mode Protocol) est utilisé pour assurer une protection renforcée contre les attaques potentielles sur les données transmises. AES-GCMP est une combinaison de deux éléments clés :

AES (Advanced Encryption Standard) : C'est un algorithme de chiffrement symétrique largement utilisé dans le monde entier, connu pour sa robustesse. Dans WPA3, AES est utilisé pour chiffrer les données avec une clé dérivée au cours de la phase de l'échange SAE, garantissant ainsi que seules les parties authentifiées peuvent déchiffrer et interpréter les informations.

Mode Galois/Counter Mode (GCM) : Ce mode de chiffrement assure non seulement la confidentialité des données, mais également leur intégrité. GCM combine le chiffrement de type counter (CTR) pour la confidentialité et un mécanisme de code d'authentification de message (MAC) basé sur l'algorithme de Galois pour l'intégrité des données. L'authentification GCM protège contre les attaques par manipulation de données et garantit que toute tentative de modification d'un paquet (par exemple, une altération de la charge utile) est détectée immédiatement.

L'usage du GCM dans WPA3 rend plus difficiles les attaques par replay ou par modification de paquets, car chaque bloc de données est authentifié. Contrairement à d'autres modes de chiffrement, où une modification du texte chiffré pourrait ne pas être détectée, AES-GCMP empêche toute modification non autorisée de manière fiable grâce à son mécanisme d'intégrité.

L'un des principaux avantages de l'utilisation d'AES-GCMP dans WPA3 est de rendre les attaques par dictionnaire inefficaces. En effet, même si un attaquant parvient à obtenir un paquet chiffré, il lui est pratiquement impossible de reconstruire la clé de session en raison de la combinaison d'AES avec le GCM. Cela rend l'attaque par force brute beaucoup plus coûteuse et complexe, car chaque tentative échouée pour une clé incorrecte entraîne une vérification de l'intégrité du paquet qui échouera.

3 Faiblesses et attaques connues

3.1 Attaques Dragonblood

En 2019, peu de temps après la sortie de WPA3, une série de vulnérabilités connues sous le nom d'attaques Dragonblood a été découverte par Mathy Vanhoef et Eyal Ronen. Ces attaques exploitent des failles dans le protocole Simultaneous Authentication of Equals (SAE), aussi appelé Dragonfly Handshake.

3.1.1 Attaque par Canal Caché Basée sur le Temps (Timing Side-Channel Attack)

L'attaque repose sur une fuite d'informations temporelles lors de l'exécution de l'algorithme de hachage utilisé dans le handshake Dragonfly. Plus précisément, lorsque des courbes elliptiques alternatives comme Brainpool sont utilisées, le temps nécessaire pour obtenir un hash inférieur au premier de la courbe peut varier en fonction du mot de passe.
Les courbes par défaut de la NIST ne présentent pas cette faiblesse, car le hash valide est trouvé immédiatement, mais Brainpool nécessite parfois plusieurs itérations [1]. Cette différence peut être observée par un attaquant à proximité, permettant ainsi de déduire des informations sur le mot de passe.

— Algorithme utilisé : Quadratic Residue Test avec Brainpool curves.

— Point faible : Dépendance au nombre d'itérations, influencé par le mot de passe et l'adresse MAC du client.

— Exploitabilité : En mesurant le temps de réponse pour divers mots de passe simulés, un attaquant peut effectuer une attaque par dictionnaire plus efficace.

3.1.2 Attaque par Canal Caché Basée sur le Cache (Cache Side-Channel Attack)

Cette attaque cible les patterns d'accès mémoire lors de la construction du commit frame du Dragonfly Handshake. Dans certaines implémentations de SAE, pour des raisons de performance, les points de courbe elliptique ou les valeurs dérivées du mot de passe (comme les éléments de Diffie-Hellman) peuvent être mis en cache.

Etapes d'une attaque classique cache :

1. Déconnexion forcée : L'attaquant envoie des paquets de désauthentification pour forcer à réinitier un handshake SAE.
2. Capture du handshake SAE : Pendant de la reconnexion, l'attaquant capture les messages d'authentification échangés entre le client et le point d'accès (les messages SAE Commit et Confirm).
3. Exploitation du cache : Si l'implémentation du point d'accès met en cache des éléments comme le Password Element (PE) ou les points de courbe utilisés dans le calcul du SAE, ces éléments restent les mêmes d'une tentative à l'autre. Il n'y a plus qu'à réutiliser les valeurs obtenues des précédents handshakes pour accélérer une attaque par dictionnaire. L'idée est de réutiliser des valeurs pré-calculées pour tester rapidement différents mots de passe.

[voir page 43] [voir page 10].

3.1.3 Attaques de Rétrogradation (Downgrade Attack)

Dans le mode de transition WPA3-WPA2, un réseau est configuré pour accepter les connexions WPA2 et WPA3 avec le même mot de passe, facilitant la transition pour les anciens appareils. Cependant, un attaquant peut forcer un client WPA3 à se connecter en mode WPA2, où il est alors possible d'exécuter des attaques classiques par dictionnaire. Voir en détail la réalisation de cette attaque : Demo of downgrade attack

3.2 Contre mesures

3.2.1 Désactivation de la mise en cache

Pour contrer les attaques par cache, il suffit de simplement désactiver la mise en cache de valeurs critiques, comme les éléments de clé partagée préalables (PE) dans les implémentations de WPA3-SAE, Évidemment cela ralentit le système et donne une expérience moins fluide, consomme beaucoup plus de ressource, mais c'est sécurisé.

3.2.2 Contrer Timing et Cache Attacks

Il faut utiliser la randomisation des délais pour éviter que les attaquants ne puissent tirer parti des différences de temps d'exécution dans les étapes critiques du processus d'authentification.

3.2.3 Limitation des tentatives d'authentification

Limiter les tentatives d'authentification d'un user pour ralentir les attaques par force brute en ligne. Bien que les attaques par force brute ne soient pas privilégiées par les attaquants étant donné du SAE qui complique la tâche.

4 Conclusion

Le WPA3, en introduisant des mécanismes comme l'authentification renforcée via le Simultaneous Authentication of Equals (SAE) et un chiffrement plus solide avec l'AES-GCMP, améliore sensiblement la sécurité des réseaux Wi-Fi par rapport au WPA2. L'utilisation des courbes elliptiques dans le SAE, en particulier, rend les attaques par dictionnaire beaucoup plus difficiles, grâce à un échange de clés plus sécurisé. Toutefois, le WPA3 n'échappe pas aux vulnérabilités, comme le montre l'attaque Dragonblood, qui révèle des failles liées à la gestion des courbes elliptiques et aux attaques par canaux latéraux.

5 Sources

https://www.dcs.warwick.ac.uk/~fenghao/files/Dragonfly_final.pdf
https://asecuritysite.com/encryption/spake
https://balramdot11b.com/2020/05/17/wpa3-and-dragonfly-sae/
https://www.rfc-editor.org/rfc/rfc7664
Dan Harkins. 2015. Dragonfly Key Exchange. RFC 7664. (Nov. 2015).
Dan Harkins. 2019. Finding PWE in Constant Time. Retrieved 24 July 2019 from https ://mentor.ieee.org/8
19-1173-08-000m-pwe-inconstant-time.docx. (July 2019).