WPA3

GIUSEPPE COMPARE

JHACKERS.IT

SOMMARIO

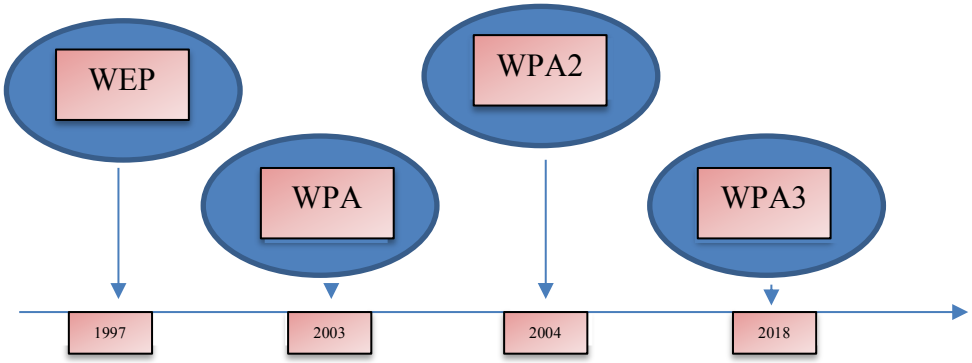
1. INTRODUZIONE E CENNI STORICI

L'utilizzo di nuove tecniche di attacco e l'aumento degli attacchi alle reti wireless negli ultimi anni ha portato la WiFi Alliance a fare un passo avanti nel mondo della sicurezza delle reti. Il protocollo WPA (WiFi Protected Access) è stato reso disponibile nel 2003 come misura intermedia per superare le debolezze legate al WEP.

Il **WEP** (Wired Equivalent Privacy) è uno standard che punta a implementare lo stesso livello di sicurezza delle reti cablate. Cifra i dati con RC4 che nello specifico utilizza due chiavi, 40 bit e 104 bit. A queste chiavi vengono aggiunti 24 bit per il vettore di inizializzazione. Attualmente è inaffidabile ed è stato sostituito dalle reti WPA e WPA2. Il vettore di inizializzazione (24 bit) è così corto che si ripete spesso. Intercettando due pacchetti con lo stesso vettore di inizializzazione e mettendoli a confronto si può intercettare la password.

WPA e WPA2 (Wi-FI Protected Access) sono due protocolli che si basano sullo standard 802.11i. Il protocollo WPA funziona con lo stesso hardware utilizzato per il WEP mentre il WPA2 ha bisogno di un hardware dedicato. WPA si basa su TKIP (Temporal Key Integrity Protocol) che usa sempre RC4 ma risolve le debolezze WEP cambiando la chiave di cifratura ad ogni pacchetto, mentre, WPA2 si basa sul protocollo CCMP (Counter-Mode/CBC-Mac Protocol) che usa l'algoritmo AES, uno dei più sicuri. A seconda del tipo di autenticazione si parla di WPA personal e WPA enterprise. Il WPA personal richiede una chiave uguale per tutti gli utenti mentre nel WPA enterprise ogni utente accede con le proprie credenziali o con un certificato. WPA2 è diventato disponibile nel 2004. Le chiavi pre-condivise WPA e WPA2 restano vulnerabili agli attacchi di cracking della password se gli utenti utilizzano una password debole. L'attacco di tipo brute force della password può essere tentato utilizzando la suite Aircrack a partire dall'operazione di handshake di autenticazione a quattro vie scambiata durante l'associazione o una nuova autenticazione.

Dopo 14 anni di progettazione per ovviare alle carenze dei precedenti protocolli di sicurezza di rete, la WiFi Alliance ha annunciato il rilascio del **WPA3** nel gennaio 2018.



2. IL WPA3

Le carenze del WPA e del WPA2, come l'imperfetta handshake a quattro vie e l'utilizzo di una PSK(Pre-Shared Key), fanno sì che le connessioni Wi-Fi siano esposte a rischi. C'è inoltre da considerare che la maggior parte delle reti wireless soffre di tutte le vulnerabilità delle reti cablate a cui si sommano altre minacce specifiche:

1. **JAMMING/INTERFERENZA**

   Questa tecnica utilizza un trasmettitore per fare interferenza sulle comunicazioni Wi-Fi e sferrare un attacco DoS (Denial of Service). Esistono dei semplici moduli Wi-Fi che vengono configurati con specifici software per interrompere connessioni. Un esempio semplice del funzionamento di questi dispositivi è: il dispositivo invia tanti pacchetti di de-autenticazione al router per far scollegare dalla rete tutti gli utenti connessi. Un esempio di utilizzo di questa tipologia di attacco può essere approfondita in un mio video (https://www.youtube.com/watch?v=0uwtt3DTvxM)

2. **ROGUE ACCESS POINT**

   Si può posizionare un access point nelle aree pubbliche di aeroporti, hotel o stazioni nel caso in cui si voglia fare un attacco non mirato per rubare informazioni e dati sensibili ai danni di utenti sconosciuti. Per questo motivo bisogna evitare di accedere a informazioni importanti personali (accesso ai siti della banca) sotto una rete pubblica. Anche in questo caso si può approfondire la tipologia di attacco in un video realizzato da me (https://www.youtube.com/watch?v=jROa0PWuxss)

3. **EVIL TWIN**

   Configurare un AP (Access Point) con l'SSID di una rete Wi-Fi per persuadere i Client a connettersi. Questo attacco può essere utilizzato insieme al jamming. In questo modo gli utenti verranno disconnessi continuamente dalla rete reale e tenteranno di connettersi alla rete "malevola" creata da Evil Twin (https://www.youtube.com/watch?v=jROa0PWuxss)

4. **EAVESDROPPING**

   L'eavesdropping è l'atto di ascoltare segretamente una conversazione privata. Sulle connessioni Wi-Fi, se non cifrate, è più facile intercettare le comunicazioni rispetto alla rete LAN.

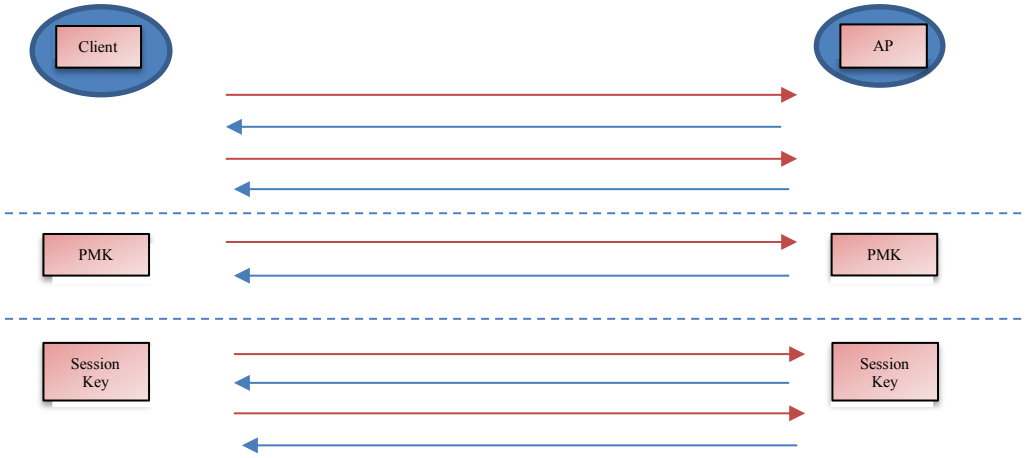
5. **IV ATTACK**

   L'Initialization Vector Attack sottrae password su reti cifrate con WEP.

Il WPA3 apporta quindi miglioramenti alla sicurezza che rendono più difficile l'accesso alle reti da parte di utenti malintenzionati. Prima di tutto esistono due tipologie di WPA3: il **WPA3-Personal** e **WPA3-Enterprise**.

WPA3-Personal

Il WPA3 Personal è caratterizzato da una selezione di password più facile da ricordare per gli utenti. Il sistema offre inoltre un livello di sicurezza più elevato, in cui i dati memorizzati e il traffico di dati nella rete non saranno compromessi anche se la password è stata violata e i dati sono già stati trasmessi.
L'aggiornamento ha anche permesso la **Simultaneous Authentication of Equals** (SAE) che ha sostituito le Chiavi Pre-Shared Keys (PSK) in WPA2-Personal. Nella crittografia , un metodo **SAE**, noto anche come Dragonfly Key Exchange Protocol, è un metodo interattivo che consente a due o più parti di stabilire chiavi crittografiche in base alla conoscenza di una password da parte di una o più parti. Una proprietà importante è che utente malintenzionato non può ottenere informazioni sufficienti per utilizzare un attacco brute force senza interazione diretta con le parti. Ciò significa che è possibile ottenere una protezione avanzata utilizzando password deboli.
Il protocollo *Simultaneous Authentication of Equals* (SAE) prevede lo scambio di chiavi basandosi sulla *zero-knowledge proof*, quindi nessuna password è effettivamente scambiata. Il concetto è lo stesso che sta alla base di ogni protocollo per lo scambio di chiavi: i due attori vengono autenticati usando un *segreto condiviso* (ad esempio una password) e alla fine si avrà un *oggetto segreto* che può essere utilizzato nelle comunicazioni tra i due attori.



In dettaglio il metodo SAE viene usato dai vari client per autenticarsi e creare una chiave di sessione; supporta sia l'FFC (Finite Field Cryptography) sia l'ECC (Elliptic Curve Cryptography), anche se di default viene utilizzato l'ECC. Dopo lo scambio con SAE viene generata un'unica **Pairwise Master Key** (PMK) condivisa tra il client e AP (Access Point). Una volta creata la PMK, il processo di associazione si completa e inizia il 4-Way Handshake per creare una chiave di sessione.
Come detto in precedenza SAE è un protocollo che resiste ad alcune tipologie di attacchi, sia passivi che attivi, ad attacchi a dizionario e ad attacchi di tipo replay. In particolare:

- **gli attacchi passivi**, in cui l'attaccante semplicemente trasmette il traffico tra due intermediari, cercando di ricavare informazioni utili (password o chiave condivisa) dai messaggi, non sono fattibili; lo stesso vale per gli attacchi attivi, in cui l'attaccante interviene direttamente sui messaggi cercando di modificarli.
- **gli attacchi a dizionario** non sono efficienti perché manca la possibilità, da parte dell'attaccante, di verificare se la password non è corretta, e quindi occorre rieseguire il protocollo utilizzando un'altra password e così via. Quindi un attaccante non può eseguire un attacco e fare ripetuti tentativi offline finché non trova la password giusta.
- **il protocollo implementa la forward secrecy**, ovvero anche la conoscenza della chiave di cifratura a lungo termine non fornisce all'attaccante un vantaggio nella conoscenza delle chiavi di sessione. Chiavi

di sessione che si basano anche su dei contributi casuali delle due parti che rimangono sconosciuti all'attaccante.
- infine, compromettere la chiave intermedia **PMK** (Denning-Sacco attack) non rappresenta per un attaccante un vantaggio nel determinare una diversa chiave di cifratura di un'altra esecuzione del protocollo.

WPA3-Enterprise

Questo tipo è stato costruito principalmente per un'applicazione più rigorosa e coerente dei protocolli di sicurezza attraverso le reti di governi, stabilimenti, imprese e istituzioni finanziarie. Rispetto al WPA2, in questo caso, il WPA3 non presenta particolari modifiche. C'è però da evidenziare che, nelle reti dove la sicurezza è un fattore critico, è prevista, seppur opzionalmente, una modalità di sicurezza a 192 bit.

In dettaglio, la modalità a 192 bit del **WPA3-Enterprise** prevede:

- l'utilizzo del protocollo *256-bit Galois/Counter Mode Protocol* (**GCMP-256**) per l'autenticazione e la cifratura;
- l'utilizzo di *384-bit Hashed Message Authentication Mode* (**HMAC**) con *Secure Hash Algorithm* (**HMAC-SHA384**) per la gestione e la verifica della chiave;
- l'utilizzo degli algoritmi *Elliptic Curve Diffie-Hellman* (**ECDH**) e *Elliptic Curve Digital Signature Algorithm* (**ECDSA**) per lo scambio e l'autenticazione della chiave.

In questa modalità non sono permesse configurazioni che abbassano il livello di sicurezza, portandolo ad un grado inferiore a quello stabilito; di conseguenza, ogni client presente nella rete deve operare in modalità 192-bit, pena l'esclusione dalla stessa. Infine, per il WPA3-Enterprise, non c'è bisogno di nessuna modalità di transizione, perché, come detto prima, non c'è stata nessuna modifica sostanziale rispetto al WPA2-Enterprise.

3. VULNERABILITA' WPA3

Nonostante il WPA3 abbia presentato notevoli evoluzioni nei confronti dei suoi predecessori rendendo la rete WiFi più sicura sotto diversi punti di vista, sono state evidenziate alcune vulnerabilità grazie ai due ricercatori **Mathy Vanhoef** (NYUAD) e **Eyal Ronen** (Tel Aviv University & KU Leuven). Le vulnerabilità evidenziate prendono il nome di dragonblood e, purtroppo, anche con WPA3, un utente malintenzionato può ancora recuperare informazioni sensibili (ad esempio la password) se quest'ultimo non utilizza alcuna protezione aggiuntiva come HTTPS.

In dettaglio l'handshake Dragonfly viene utilizzato anche in alcune reti Wi-Fi aziendali che richiedono un nome utente e una password per il controllo dell'accesso. Più precisamente è stato testato che Dragonfly viene utilizzato anche dal protocollo EAP-pwd e gli attacchi dragonblood funzionano anche contro questo protocollo.

Sono stati scoperti inoltre anche gravi bug nella maggior parte dei prodotti che implementano EAP-pwd. Questi bug consentono ad un avversario di impersonare qualsiasi utente e quindi accedere alla rete Wi-Fi, senza conoscere la password dell'utente. Sebbene EAP-pwd venga utilizzato abbastanza raramente nella pratica, questi risultati illustrano i rischi di un'errata implementazione dell'handshake di Dragonfly.

I difetti di progettazione che sono stati scoperti possono essere suddivisi in due categorie:

- La prima categoria è costituita da **attacchi di downgrade** contro dispositivi compatibili con WPA3
- La seconda categoria è costituita da **punti deboli nell'handshake** Dragonfly di WPA3, noto come SAE. I difetti scoperti possono essere utilizzati in modo improprio per recuperare la password della rete Wi-Fi, lanciare attacchi che mirano al consumo di risorse e costringere i dispositivi a utilizzare gruppi di sicurezza più deboli. Tutti gli attacchi sono contro le reti domestiche (ad esempio WPA3-Personal), dove una password è condivisa tra tutti gli utenti.

Le vulnerabilità evidenziate sono sostanzialmente le seguenti:

- **CERT ID #VU871675** : Downgrade attack against WPA3-Transtition mode leading to dictionary attacks.
    - Il primo attacco sfrutta la retrocompatibilità di WPA3. Per soddisfare i client meno recenti che supportano solo WPA2 e per motivare la transizione verso WPA3, è stata definita una modalità di transizione nella specifica WPA3. In questa modalità una rete Wi-Fi supporta l'utilizzo sia di WPA3 che di WPA2 con una password identica. È stato scoperto che un avversario può creare una rete non autorizzata e costringere i client che supportano WPA3 a connettersi alla rete non autorizzata WPA2 e ciò consente ad un avversario di recuperare la password della rete utilizzando attacchi brute force o a dizionario.

- **CERT ID #VU871675**: Security group downgrade attack against WPA3's Dragonfly handshake.
    - È stato scoperto un attacco di downgrade contro l'handshake Dragonfly stesso del WPA3, in cui la vittima può essere costretta a utilizzare un security group debole. Il dispositivo che

avvia l'handshake (in genere il client) invia un frame di commit che include il security group che desidera utilizzare. Se l'AP non supporta questo gruppo, risponde con un messaggio di rifiuto, costringendo il client a inviare un frame di commit utilizzando un altro gruppo. Questo processo continua finché non viene trovato un gruppo di sicurezza supportato da entrambe le parti. Un utente malintenzionato può impersonare un AP e falsificare i messaggi di rifiuto per costringere i client a scegliere un security group debole.

- **CVE-2019-9494**: Timing-based side-channel attack against WPA3's Dragonfly handshake.
    - È stato evidenziato che il tempo impiegato da un AP per rispondere ai frame di commit potrebbe far trapelare informazioni sulla password. Quando l'AP utilizza security group basati su curve ellittiche NIST, che tutti i dispositivi WPA3 devono supportare, non vengono trapelate informazioni sulla temporizzazione. Tuttavia, quando l'AP supporta curve Brainpool o gruppi MODP, il tempo di risposta dipende dalla password utilizzata. Un avversario può abusare di queste informazioni per eseguire un attacco con dizionario, simulando quanto tempo impiegherebbe l'AP a elaborare ogni password e confrontandolo con i tempi osservati. Da notare inoltre che, contrariamente ad alcune affermazioni, Dragonfly è stato effettivamente progettato per supportare i gruppi MODP. Dopo tutto, la variante Dragonfly utilizzata in TLS-PWD include una piccola modifica in modo che questi gruppi MODP possano essere utilizzati in sicurezza. Sfortunatamente queste modifiche non sono state trasferite alla variante Dragonfly utilizzata in WPA3.

- **CVE-2019-9494**: Cache-based side-channel attack against WPA3's Dragonfly handshake.
    - Se un utente malintenzionato è in grado di osservare i modelli di accesso alla memoria sul dispositivo di un utente vittima mentre costruisce il frame di commit per l'handshake di Dragonfly, potrebbe riuscire ad ottenere informazioni sulla password utilizzata.
      L'osservazione di questi schemi è possibile solo se l'avversario controlla qualsiasi applicazione sul dispositivo della vittima oppure nel caso in cui l'avversario riesca a controllare il codice JavaScript nel browser della vittima.
      Ovviamente il pattern identificato può essere utile per l'esecuzione di un attacco a dizionario. Secondo i ricercatori è necessario che i protocolli moderni forniscano una guida esplicita su come evitare che i modelli di accesso alla memoria perdano informazioni segrete e per questo motivo ritengono che questo sia un difetto nelle specifiche dell'handshake Dragonfly di WPA3.

- **CERT ID #VU871675**: Resource consumption attack (i.e. denial of service) against WPA3's Dragonfly handshake.
    - Il dispositivo che avvia l'handshake di Dragonfly inizia inviando un frame di commit. L'elaborazione di questo frame e la generazione di una risposta sono computazionalmente costosi. Sebbene WPA3 contenga un metodo di scambio di cookie per impedire agli aggressori di falsificare i frame di commit utilizzando indirizzi MAC falsi, è banale aggirarlo e così un utente malintenzionato può sovraccaricare gli Access Point (AP) generando 16 frame di commit contraffatti al secondo.
      Questo attacco di "consumo delle risorse" causa un elevato utilizzo della CPU sull'AP e impedisce o ritarda la connessione di altri dispositivi all'AP tramite WPA3 e può arrestare o rallentare anche altre funzionalità dell'AP stesso. Sebbene l'attacco possa essere mitigato elaborando il frame di commit in un thread in background a bassa priorità, le varianti dell'attacco rimangono possibili. A seconda della difesa precisa che i fornitori implementano, sarà comunque possibile attivare un elevato utilizzo della CPU sull'AP, oppure sarà possibile impedire o ritardare la connessione di altri dispositivi all'AP utilizzando WPA3.

Anche il protocollo EAP-pwd utilizza internamente Dragonfly e fornisce l'autenticazione basata su un nome utente e una password in alcune reti Wi-Fi aziendali. È vulnerabile agli stessi attacchi scoperti contro WPA3. Inoltre, tutte le implementazioni di EAP-pwd testate dai 2 ricercator sono vulnerabili ad invalid curve attack, che consentono all'avversario di aggirare completamente l'autenticazione. La maggior parte delle implementazioni erano inoltre vulnerabili ai reflection attack.

Gli strumenti che sono stati utilizzati per condurre gli attacchi sono stati messi a disposizione in modo tale da consentire a tutti gli altri ricercatori di replicare gli attacchi e constatare le vulnerabilità riscontrate. I tool principalmente utilizzati sono:

- **Dragonslayer**: esegue attacchi di tipo invalid curve contro client e server EAP-pwd. Questi attacchi aggirano l'autenticazione e l'unica risorsa richiesta è un nome utente valido.
- **Dragondrain**: questo strumento può essere utilizzato per verificare se, o fino a che punto, un Access Point è vulnerabile agli attacchi DoS contro l'handshake SAE di WPA3.
- **Dragontime**: questo è uno strumento sperimentale per eseguire attacchi a tempo contro l'handshake SAE se sono supportati i gruppi MODP 22, 23 o 24. Notare che la maggior parte delle implementazioni WPA3 per impostazione predefinita non abilitano questi gruppi.
- **Dragonforce**: si tratta di uno strumento sperimentale che prende le informazioni recuperate dagli attacchi temporali o basati sulla cache ed esegue un attacco di partizionamento delle password. Questo è simile a un attacco del dizionario.

4. CONCLUSIONI

Ricapitolando il WPA3 ha introdotto importanti novità dal punto di vista della sicurezza a livello WiFi. Tra queste vanno sicuramente tenute in considerazione:

- Il **Dragonfly Handshake** o il protocollo SAE
- **Sostituzione del WPS**
- **WiFi Device Provisioning Protocol** o DPP che è un modo nuovo e semplice per aggiungere nuovi dispositivi in modo più sicuro. La funzione Easy Connect rende più facile la connessione a casa e all'Internet degli oggetti (IoT) tramite un codice QR.
- Quando si utilizzano gli hotspot in pubblico, gli utenti ricevono una migliore protezione attraverso il **Wi-Fi Enhanced Open** che fornisce una crittografia non autenticata.
- Dimensioni delle **chiavi di sessione più grandi**
- La maggiore dimensione della chiave di sessione rende le password più difficili da decifrare. Questa funzione è disponibile per WPA3-Enterprise che supporta la **sicurezza a 192 bit** durante tutta la fase di autenticazione
- **Autenticazione NFC**
- **Connessioni rapide** dei dispositivi Wi-Fi
- Invece di password condivise, WPA3 sarà in grado di registrare nuovi dispositivi che non lo richiedono nel processo. Il nuovo sistema si chiama **WiFi Device Provisioning Protocol** (WiFi DPP). Il sistema funziona trasmettendo la procedura per ottenere l'accesso senza trasmettere una password. I codici QR e i tag NFC sono utilizzati dagli utenti per connettersi alla rete.

Per quanto riguarda le vulnerabilità evidenziate e descritte precedentemente, grazie al risultato della ricerca condotta da Mathy Vanhoef e Eyal Ronen, sia lo standard Wi-Fi che EAP-pwd verranno aggiornati con un protocollo più sicuro. Sebbene questo aggiornamento non sia retrocompatibile con le attuali distribuzioni di WPA3, impedisce la maggior parte degli attacchi descritti in precedenza.