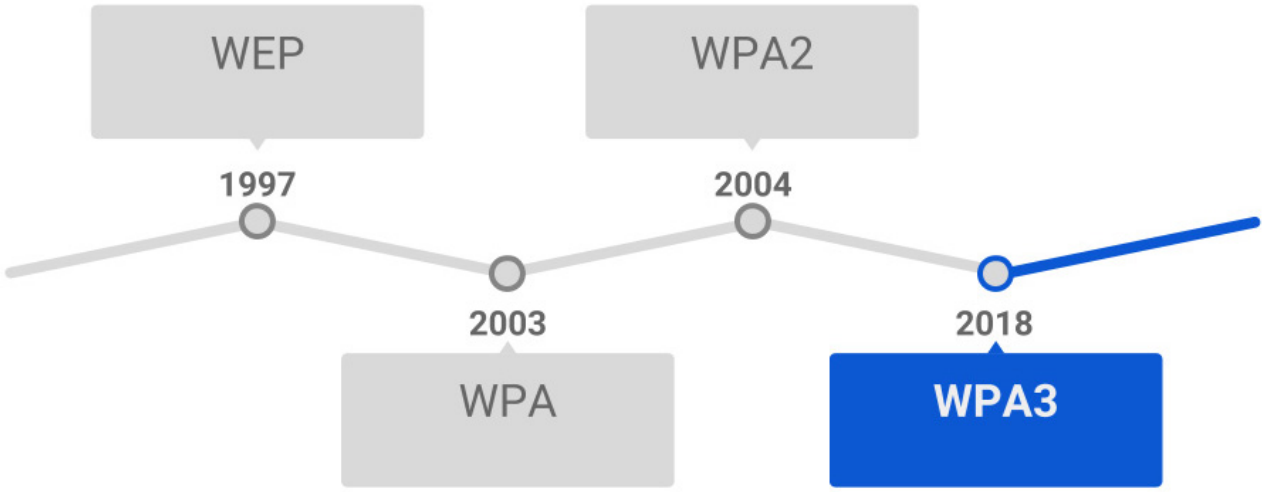
WPA3: analisi delle nuove reti WiFi

Author : Gianluigi Spagnuolo

Date : 27 settembre 2018

Nel 2003 la *Wi-Fi Alliance* ha introdotto la famiglia di protocolli Wi-Fi Protected Access (WPA), che si occupa della sicurezza della trasmissione via Wi-Fi. Nel 2004 è stata introdotta una versione più sicura del protocollo: il **WPA2**. Nel 2018, dopo aver constatato l'inadeguatezza dello standard WPA2 (dal punto di vista della sicurezza), è stata la volta del **WPA3** (Figura 1).



Nota: in realtà il WPA3 non è un nuovo standard o protocollo, ma specifica quali standard e protocolli un dispositivo deve seguire per essere certificato WPA3. D'ora in poi useremo il termine "protocollo" nella sua accezione più generica.

Un protocollo che si occupa dello scambio di chiavi, come quelli della famiglia WPA, dovrebbe presentare alcune proprietà di sicurezza; ad esempio, dovrebbe prevenire o quantomeno resistere ai seguenti attacchi:

- attacchi a dizionario (online e offline)
- attacchi attivi e passivi
- attacchi di tipo replay e pre-play
- attacchi *man-in-the-middle*

Inoltre

- dovrebbe impedire le intercettazioni fatte al fine di ricavare informazioni utili
- dovrebbe implementare la proprietà di *forward secrecy*

Il WPA3 appena definito implementa solo alcune di esse, vediamo quali. I principali vantaggi, come definiti dalla *Wi-Fi Alliance*, del WPA3 rispetto al WPA2, sono:

- Riduzione degli *attacchi* alle reti: il WPA3 riduce il successo degli attacchi, forzando i protocolli *legacy* ad usare l'algoritmo **Advanced Encryption Standard** (AES);
- Aumento della *resilienza* della rete (Network Resiliency): l'utilizzo dei **Protected Management Frames** (PMF), resi obbligatori dal WPA3, aggiunge un livello di sicurezza all'intera infrastruttura, utile soprattutto contro gli attacchi che mirano all'intercettazione delle comunicazioni e alla manomissione dei frame di gestione della connessione. Lo standard 802.11 prevede 3 tipi di frame: frame dati, frame di controllo e frame di gestione. Nel precedente protocollo, solo i *frame dati* erano protetti da cifratura, poiché quelli di gestione normalmente arrivano prima dell'associazione tra i dispositivi. Il problema è che tra i *management frame* ci sono anche quelli di gestione della de-autenticazione, della dissociazione e di alcuni parametri necessari al corretto riconoscimento di un dispositivo nella rete. Informazioni che possono essere facilmente utilizzate per ingannare un dispositivo; ad esempio, delle stazioni lecite possono essere estromesse dalla rete a causa di un falso Access Point (AP) che invia falsi messaggi. I PMF, introdotti con la revisione 802.11w, erano opzionali nel WPA2 e sono stati resi obbligatori con l'introduzione del WPA3.

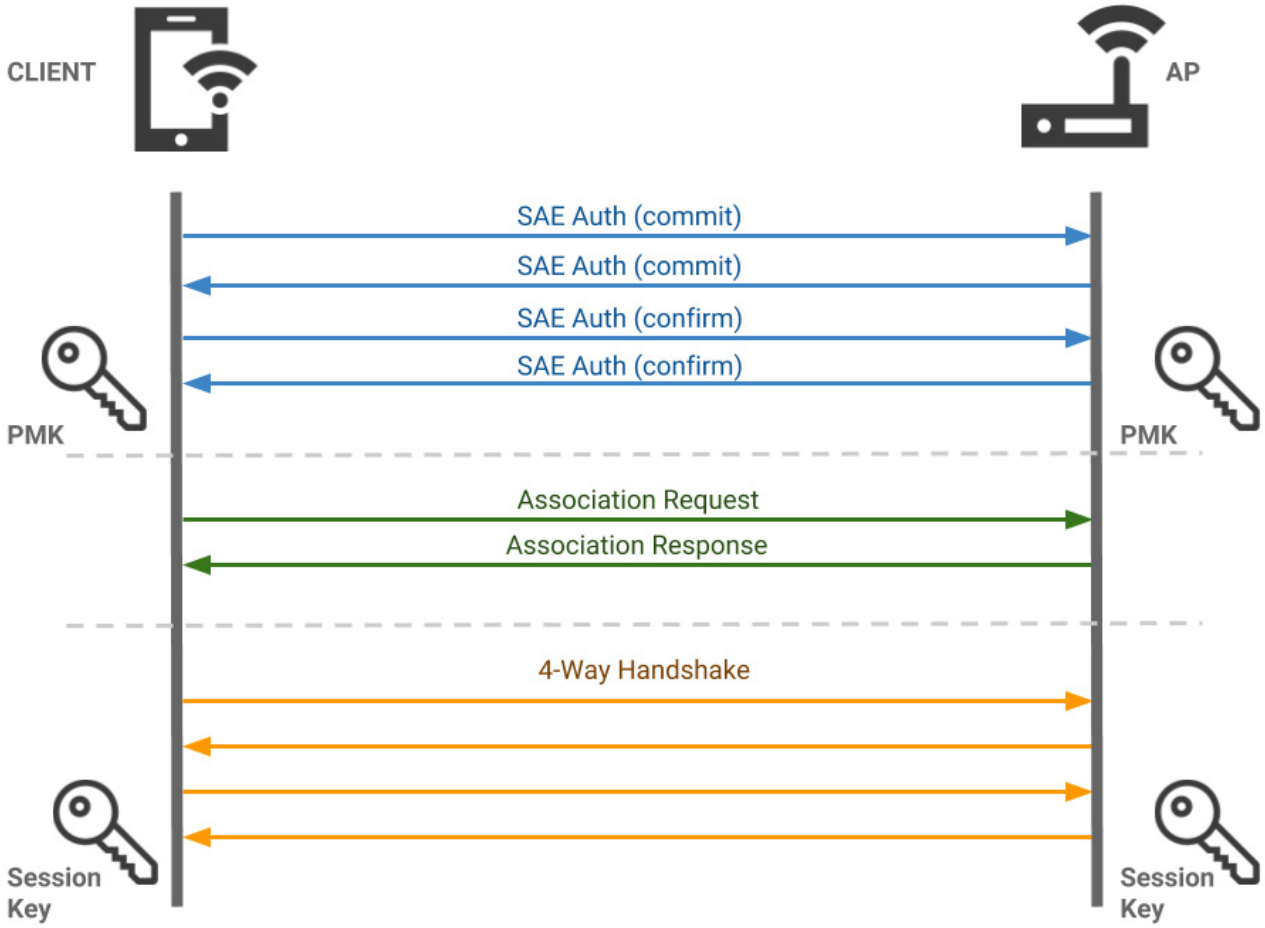
WPA3 personal

L'unica modifica rilevante allo standard WPA3-Personal riguarda il metodo di autenticazione: il *Pre-Shared Key (PSK)* è stato sostituito con il *Simultaneous Authentication of Equals* (SAE) (Riquadro 1). Nel WPA3-Personal, la password viene utilizzata solo per l'autenticazione, non per generare le chiavi, usando la conoscenza di questa da parte dei due attori. Il WPA3 garantisce in questo modo maggiore sicurezza, in particolare si ha:

- una completa resistenza agli attacchi a dizionario;
- una maggiore resistenza delle chiavi di sessione anche conoscendo la password;
- una scelta delle password più *naturale*, essendo il WPA3-Personal resistente agli attacchi a dizionario. In questo modo può essere scelta una password più semplice da ricordare e da digitare;
- una continuità con le versioni del protocollo precedenti.

Riquadro 1: Simultaneous Authentication of Equals

Il protocollo *Simultaneous Authentication of Equals* (SAE) è una variante di *Dragonfly* che 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 (Figura 2).

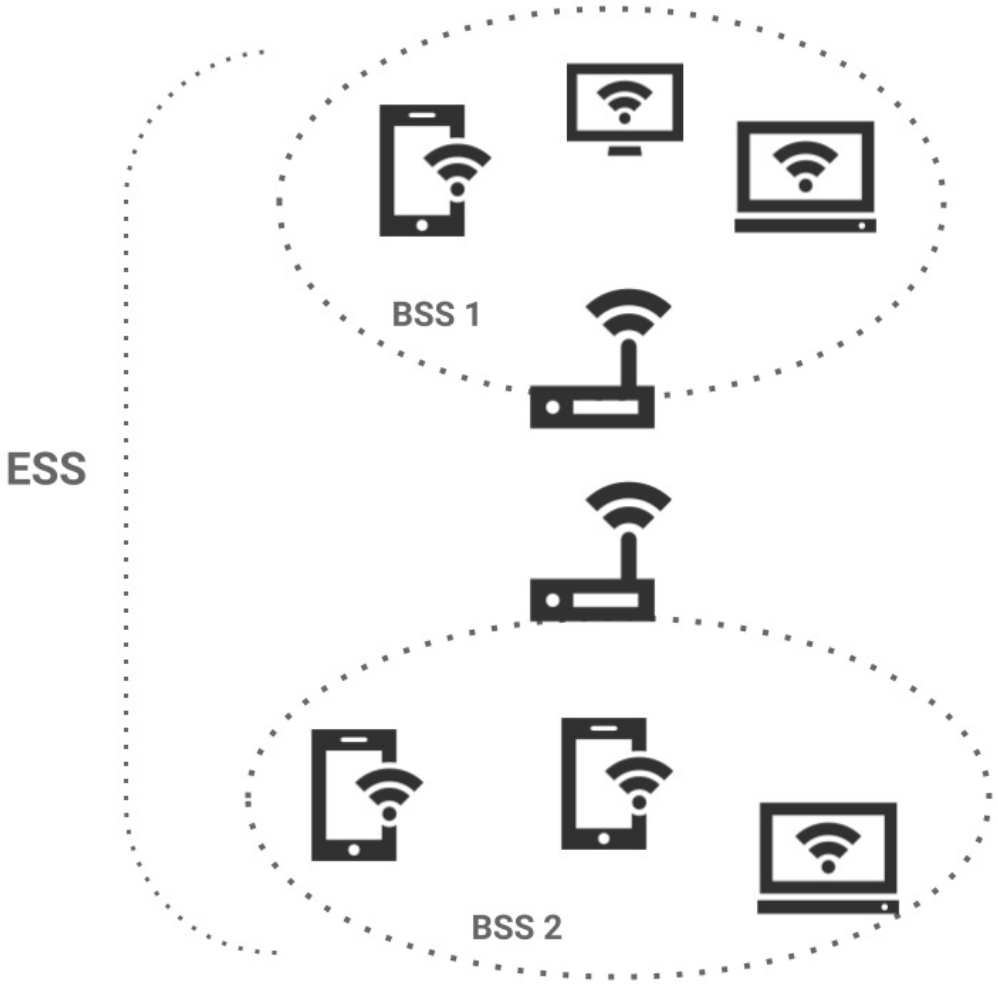


In dettaglio: il metodo SAE viene usato dai vari *client* per autenticarsi e creare una chiave di sessione; supporta sia l'FFC (*Finite Field Cryptography*) sia l'ECC (*Elliptic Curve Cryptography*), di default viene utilizzato l'ECC. Dopo lo scambio con SAE, viene generata un'unica *Pairwise Master Key* (PMK) condivisa tra il client e AP. Una volta creata la PMK, il processo di associazione si completa e inizia il *4-Way Handshake* per creare una chiave di sessione.

Dal punto di vista della sicurezza, SAE è un protocollo che resiste sia ad attacchi passivi che attivi, ad attacchi a dizionario e ad attacchi di tipo replay. In particolare:

- gli attacchi passivi, dove l'attaccante semplicemente trasmette il traffico tra due attori leciti, cercando di ricavare informazioni utili (password o chiave condivisa) dai messaggi, non sono fattibili; lo stesso vale per gli attacchi attivi, dove l'attaccante interviene direttamente sui messaggi, modificandoli.
- gli attacchi a dizionario non sono efficienti perché manca la possibilità, da parte dell'attaccante, di verificare l'ipotesi, ovvero, se la password non è corretta, occorre rieseguire il protocollo utilizzando un'altra ipotesi 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-SAE Transition Mode



Oltre alla modalità standard è presente anche una modalità di transizione. Quando in un *basic service set* (BSS) (Figura 3) sono presenti dispositivi che operano sia in *WPA2-PSK* sia in *WPA3-SAE*, un AP deve funzionare in modalità *WPA3-SAE Transition Mode*. In questo modo, è capace di garantire l'accesso alla WLAN ad entrambi i tipi di dispositivo utilizzando la stessa password. Un dispositivo, in modalità *WPA3-SAE Transition Mode*, *non* godrà appieno di tutti i vantaggi previsti dall'uso del WPA3, in quanto, per garantire l'interoperabilità e la compatibilità dei due sistemi, è stato necessario sacrificare alcune funzionalità. Ovviamente tale modalità è da intendersi solo per un utilizzo provvisorio della WLAN e si deve passare alla modalità pienamente compatibile con il WPA3 il prima possibile.

WPA3 Enterprise

Per quello che riguarda le reti di livello *enterprise*, il WPA3 non presenta particolari modifiche rispetto al WPA2. 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. Per garantire la coerenza, tale modalità fornisce un livello minimo di sicurezza per le *primitive crittografiche* di tutti gli elementi delle rete. 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.

Quindi ogni aspetto riguardante la gestione delle chiavi utilizzerà, in questa modalità, un sistema di crittografia sufficientemente robusto. 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.

Conclusioni

Mathy Vanhoef (@vanhoefm), il ricercatore che sta dietro al **KRACK attacks** (https://www.krackattacks.com), definisce il WPA3 come un'*occasione mancata*. Quello che Vanhoef contesta alla Wi-Fi Alliance è che solo una delle quattro nuove *feature*, previste a Gennaio 2018, è obbligatoria, mentre le altre misure sono gestite diversamente. È stato reso obbligatorio solo l'utilizzo dell'handshake basato sul protocollo *Simultaneous Authentication of Equals*; le altre caratteristiche o fanno parte di altre certificazioni (*Wi-Fi CERTIFIED Easy Connect* e *Wi-Fi CERTIFIED Enhanced Open program*) o sono opzionali (come l'incremento della dimensione delle chiavi per il WPA3-Personal). In conclusione, il WPA3 rappresenta un passo avanti nella sicurezza, però quanto è stato fatto non è sufficiente visto anche l'utilizzo del Wi-Fi.

Articolo a cura di **Gianluigi Spagnuolo**