NAeS Consulting SRL

KRACK ATTACK

Versione 1.5

Jacopo Saladini
24/10/2017

1.INTRODUZIONE

Tutte le reti Wi-fi protette non trasmettono i pacchetti in chiaro nell'aria, ma utilizzano processi di crittografia che non consentono l'interpretazione delle comunicazioni da parte di terzi, anche qualora fossero in grado di intercettare le trasmissioni. In particolare il processo di crittografia implementato nel modello WPA2, ormai universalmente adottato, utilizza chiavi di crittografia precedentemente note ai Client e agli AP (comunicate per altre vie e pre-configurate dall'Utente e dal Gestore della rete nel caso di implementazione di tipo "PreSharedKey" oppure negoziate tra i dispositivi durante il processo di autenticazione nel caso di implementazione di tipo "Enterprise"). Tali chiavi, denominate Pairwise Master Key (PMK), non vengono direttamente utilizzate per la cifratura delle comunicazioni, ma vengono combinate con altri elementi specifici dei Client e degli AP e con elementi casuali per generare le reali chiavi di cifratura denominate Pairwise Transient Key (PTK). Mentre le PMK rimangono le stesse e non vengono trasmesse, le PTK sono diverse per ogni Client e per ogni sessione dello stesso Client rendendo praticamente impossibile la loro intercettazione in tempi utili per essere usate per decifrare il traffico.

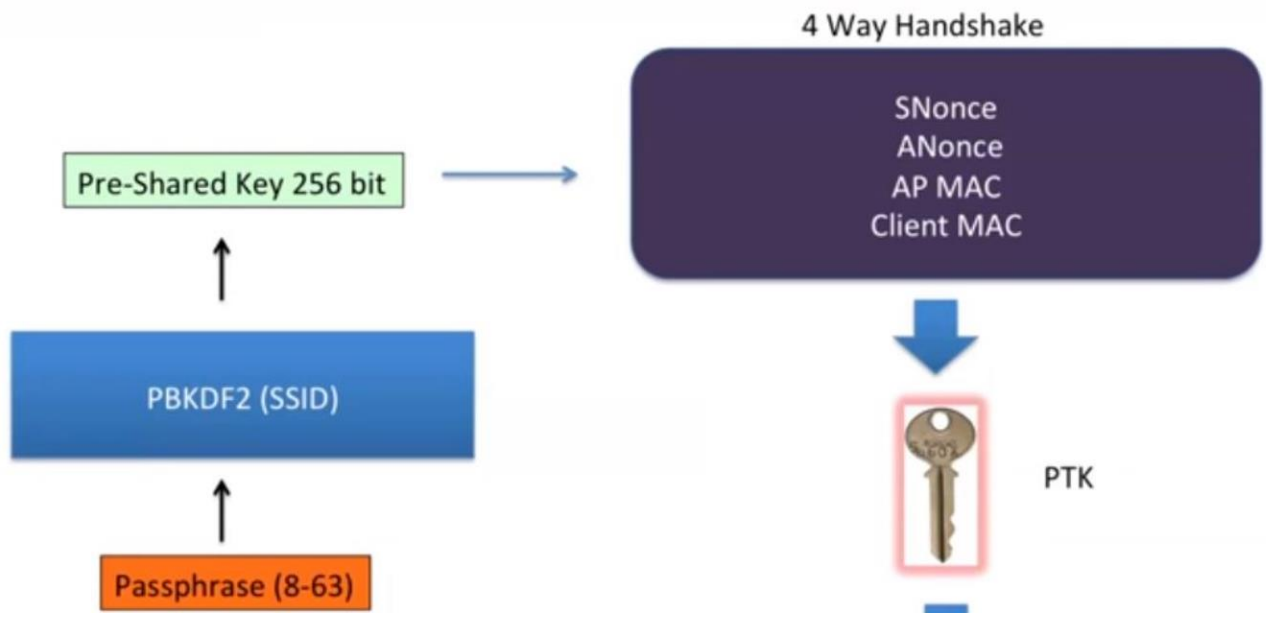
Il processo con cui Client e AP si scambiano le informazioni necessarie a costruire la suddetta chiave di sessione è chiamato 4-way handshake una tecnica che per oltre 14 anni è rimasta al riparo da attacchi, ma ora non è più così: Mathy Vanhoef, un ricercatore esperto di sicurezza, ha scoperto che il processo di 4-way handshake è vulnerabile in diverse modalità alla re-installazione delle chiavi di sessione, ossia che è possibile attraverso determinati comportamenti ottenere il riutilizzo della stessa chiave di sessione. Sebbene l'impatto dell'attacco dipenda da molti fattori tra cui la tipologia di client, la tipologia di AP e la configurazione della rete, la scoperta di diverse vulnerabilità in un protocollo sin qui ritenuto totalmente sicuro è di fatto una rivelazione sconvolgente. Nei casi più gravi è possibile decifrare completamente il traffico e iniettare del traffico malevolo. Questo attacco è eseguibile sia verso WPAv2-PSK che WPAv2-Enterprise.

Va anche detto che l'attacco non permette il recupero diretto della password WPA-PSK o delle credenziali di accesso dell'Utente, ma basandosi su falle nell'implementazione del 4-way handshake (non è stata mai formalizzata una macchina a stati del 802.11i) e su una vera e propria falla protocollare nell' 802.11r, il protocollo utilizzato per fare roaming veloce (FAST BSS TRANSACTION), consente di forzare il riutilizzo delle stesse chiavi di sessione rimuovendo di fatto il fattore di sicurezza garantito dal continuo cambio delle chiavi di cifratura. Come vedremo nel seguito, alcuni sistemi vanno oltre la vulnerabilità scoperta, ma sottoposti a determinati comportamenti azzerano addirittura la chiave trasmettendo di fatto in chiaro le comunicazioni successive all'attacco (in questo caso si aggiunge alle vulnerabilità del protocollo anche una errata implementazione da parte degli sviluppatori del sistema operativo).

1.1 4-HANDSHAKE

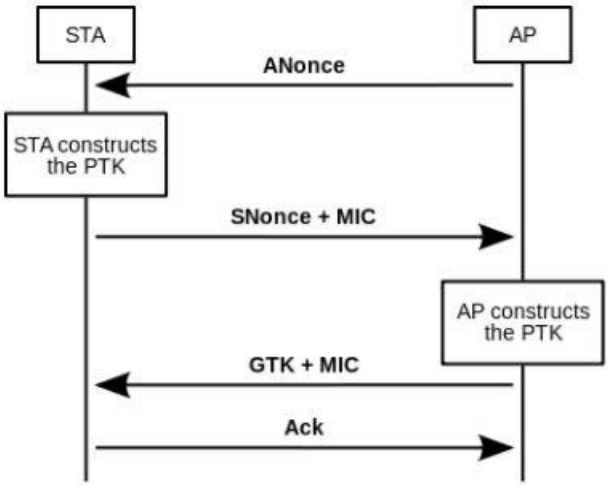
Prima di entrare nel merito dell'attacco spieghiamo velocemente il processo di 4-way handshake.

La chiave di sessione PTK è derivata dalla PMK e dal 4-way Handshake come si vede in figura. Le informazioni che Client e AP si scambiano durante il processo, e che verranno combinate con la PTK, sono i rispettivi MAC Address e due numeri casuali unici, generati uno dal Client e uno dall'AP. All'interno della comunicazione tra un Client e un AP, rimanendo invariati PMK e MAC Address, gli unici elementi che cambiano e che daranno luogo a PTK non ripetute sono i numeri casuali (SNonce generato dal client e ANounce generato dall'AP).



Nel WPA2-PSK (modalità utilizzata prevalentemente nelle reti personali, ma anche in molte aziende o esercizi pubblici), la PMK è derivata direttamente dalla password di accesso alla rete combinata con l'SSID come illustrato in figura, mentre nel WPA2 Enterprise (modalità utilizzata soprattutto nelle aziende strutturate) la PMK è negoziata attraverso il protocollo di autenticazione 802.1x.

L'attacco riguarda principalmente il rinvio "programmato" dall'attaccante del messaggio 3 del 4-way Handshake (GTK+MIC vedi figura sotto) che produce nel client (o nell'AP) la reinstallazione della chiave, il reset del nonce e del replay counter. Questo comportamento può essere continuamente indotto in modo da riutilizzare sempre lo stesso nonce. Un tale riutilizzo rende vulnerabili i protocolli di cifratura dei dati (data-confidentiality protocol) CCMP, TKIP , GCMP.



2. Le 3 TIPOLOGIE DI ATTACCO

2.1 ATTACCO AL 4-WAY HANDSHAKE.

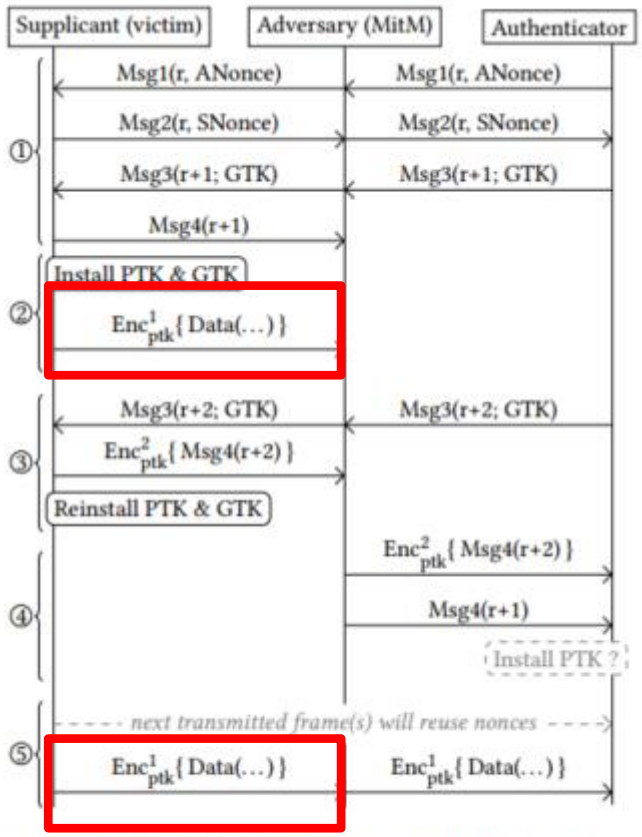


Figure 4: Key reinstallation attack against the 4-way handshake, when the supplicant (victim) still accepts plaintext retransmissions of message 3 if a PTK is installed.

Nella Figura si vede l'attacco nelle sue 5 fasi:

1- Per iniziare l'attacco bisogna eseguire un MITM (Man in the middle) tra supplicant (client) e autenticator (AP).
   Nella prima fase rispetto al normale handshake a 4 vie si blocca il messaggio finale e non lo si fa pervenire all'AP.
2- Il client, come protocollo, conclude 4-way handshake e installa le chiavi PTK e GTK (quella usata per criptare broadcast e multicast).
3- Nella fase 3 l'AP reinvia il messaggio 3 perché non ha ricevuto "ACK" ovvero il messaggio 4. L'attaccante esegue il forwarding di questo pacchetto al client che reinstalla la key e resetta nonce e il replay counter usato dal protocollo di encryption.

4- La fase 4 conclude il 4-way handshake verso l'AP. Da notare che sebbene questo attacco sia diretto al client, anche l'AP deve avere il comportamento di accettare tutti i replay counter generati durante la 4-way handshake (in questo caso MSG4(r+1) anche se era già stato inviato il MSG4(r+2)).

5- Il client invia un pacchetto criptato ma riutilizza la stessa chiave (IN ROSSO).

Ricapitolando, per portare l'attacco bisogna conquistare una posizione di MIMT, interrompere il 4-way handshake e reinviare il messaggio 3, così da reinstallare in modo programmato dall'attaccante la key che resetta nonce e replay counter sul client. La re-inizializzazione rende attaccabile il protocollo di cifratura.

2.2 ATTACCO AL GROUP KEY HANDSHAKE

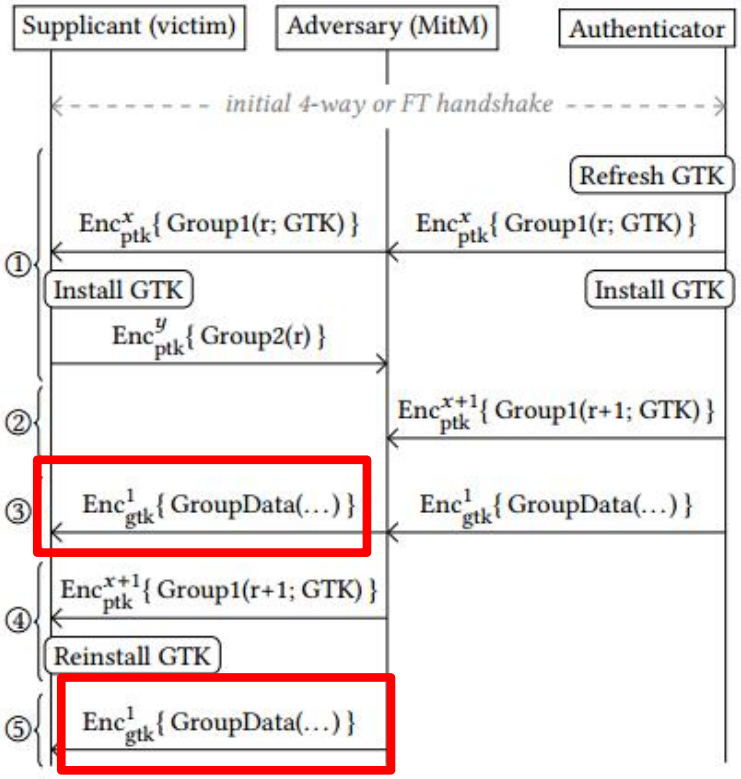


Figure 7: Key reinstallation attack against the group key handshake, when the authenticator (AP) immediately installs the GTK after sending a Group Message 1 to all clients.

Nella Figura si vede l'attacco nelle sue 5 fasi; da notare che i pacchetti scambiati per l'aggiornamento della GTK, utilizzato per criptare i pacchetti per l'invio di broadcast ed multicast, sono criptati.

1- L'AP invia un aggiornamento della GTK tramite un message 1 che viene ricevuto dal client . Il client installa la chiave. E risponde con un message 2 , l'attaccante blocca la risposta.
2- L'AP non ha ricevuto nessun riscontro per il messagge 1, reinvia un nuovo message 1 che viene bloccato.
3- In questa fase arriva un messaggio di brodcast / multicast che l'AP deve inviare al client. Lo invia e viene ricevuto correttamente dal client .
4- A questo punto l'attaccante reinvia il messaggio 1 inviato dall'AP nello stage 2, provocando sul client la re-inizializzazione del replay counter.

5- L'attaccante reinvia il brodcast multicast catturato nello stage 3 che in condizioni normali non sarebbe stato accettato (replay counter non sarebbe stato coerente); a causa della re-inizializzazione, viene invece accettato dal client.

2.3 ATTACCO AL 802.11R FT HANDSHAKE.

L'802.11r è il protocollo utilizzato per fare roaming veloce tra AP della stessa rete e accorciare le normali tempistiche; questo è ottenuto "incapsulando" il 4-way handshake nei pacchetti di authentication e reassociation . Questo attacco è indirizzato all'AP e, rispetto agli altri due, non necessita di una posizione MITM.

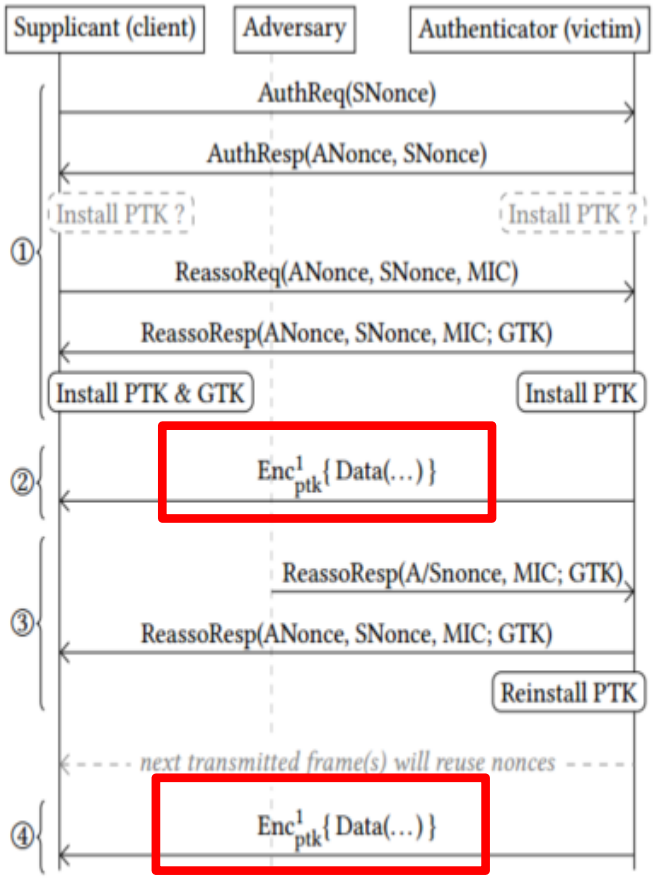


Figure 9: Key reinstallation attack against the Fast BSS Transition (FT) handshake. Note that a MitM position is not required, only the ability to eavesdrop and replay frames.

Nella Figura si vede l'attacco nelle sue 4 fasi:

1- Normale ft handshake. Dove l'attaccante salva il messaggio 3 (ReassoReq) del client.
2- L'Ap invia un pacchetto al client .
3- L'attaccante invia un messaggio di ReassoResp è forza l'AP a reinstallare le chiavi re-inizializzando il nonce utilizzato per criptare il pacchetto.
4- Ap invia un secondo pacchetto ed avendo appena installato le chiave ri-utilizza nonce della trasmissione 2.

Questo attacco è più facile da implementare perché FT handshake non ha il replay counter quindi è possibile re-inviare continuamente il ReassoReq e dunque forzare continuamente il riuso del nonce che rende attaccabile il protocollo di cifratura.

3. IMPATTO

Questa tipologia di attacchi definiti come "KEY REINSTALLATION ATTACKS: FORCING NONCE REUSE IN WPA2" per avere successo dipendono da molti fattori: dalla configurazione della rete , dai client utilizzati e dagli AP utilizzati. In queste due tabelle riassumiamo alcuni dati ad oggi noti:

Table 1: Behaviour of clients: 2nd column shows whether retransmission of message 3 are accepted, 3rd whether plaintext EAPOL messages are accepted if a PTK is configured, 4th whether it accepts plaintext EAPOL messages if sent immediately after the first message 3, and 5th whether it is affected by the attack of Section 3.4. The last two columns denote if the client is vulnerable to a key reinstallation attack against the 4-way or group key handshake, respectively.

Implementation	Re. Msg3	Pt. EAPOL	Quick Pt.	Quick Ct.	4-way	Group
OS X 10.9.5	✓	✗	✗	✓	✓	✓
macOS Sierra 10.12	✓	✗	✗	✓	✓	✓
iOS 10.3.1 [c]	✗	N/A	N/A	N/A	✗	✓
wpa_supplicant v2.3	✓	✓	✓	✓	✓	✓
wpa_supplicant v2.4-5	✓	✓	✓	✓[a]	✓[a]	✓
wpa_supplicant v2.6	✓	✓	✓	✓[b]	✓[b]	✓
Android 6.0.1	✓	✗	✓	✓[a]	✓[a]	✓
OpenBSD 6.1 (rum)	✓	✗	✗	✗	✗	✓
OpenBSD 6.1 (iwn)	✓	✗	✗	✓	✓	✓
Windows 7 [c]	✗	N/A	N/A	N/A	✗	✓
Windows 10 [c]	✗	N/A	N/A	N/A	✗	✓
MediaTek	✓	✓	✓	✓	✓	✓

[a] Due to a bug, an all-zero TK will be installed, see Section 6.3.
[b] Only the group key is reinstalled in the 4-way handshake.
[c] Certain tests are irrelevant (not applicable) because the implementation does not accept retransmissions of message 3.

Per un spiegazione completa della tabella guardare https://papers.mathyvanhoef.com/ccs2017.pdf, ci limitiamo qui a mettere in evidenza tre aspetti:

- Windows e iOS non sono attaccabili con il 4-way handshake perché non reinstallano le chiavi dopo il re-invio del messaggio 3 (COLONNA 1)
- tutti i sistemi sono suscettibili all'attacco al Group Key handshake. (COLONNA 6)
- alcuni modelli di Android, circa il 30% del mercato, hanno un baco tale per cui, sottoposti all'attacco, installano una chiave di tutti zeri annullando quindi ogni tipo di cifratura delle trasmissioni successive e rendendone il contenuto intellegibile a terzi in grado di intercettarle.

Table 3: Impact of our key reinstallation attack against the 4-way, FT, and group key handshake, in function of the data-confidentiality protocol used. Each cell shows in which direction frames can be replayed, decrypted, or forged.

	Replay [c]	Decrypt [a]	Forge
4-way impact			
TKIP	AP → client	client → AP	client → AP [b]
CCMP	AP → client	client → AP	
GCMP	AP → client	client → AP	client ↔ AP [b]
FT impact			
TKIP	client → AP	AP → client	AP → client
CCMP	client → AP	AP → client	
GCMP	client → AP	AP → client	AP ↔ client [b]
Group impact			
any	AP → client [c]		

[a] With this ability, we can hijack TCP connections to/from an Internet endpoint and inject data into them.

[b] With this ability, we can use the AP as a gateway to inject packets towards *any* device connected to the network.

[c] This denotes in which direction we can replay unicast and group-addressed frames. For the group key handshake, only group-addressed frames can be replayed.

In questa tabella, a seconda della tipologia di attacco portato (4-way, FT, Group) e del protocollo di Encryption utilizzato nel WPA2 (TKIP, CCMP, GCMP) si mostra quali azioni può riuscire a fare l'attaccante: può replicare pacchetti, decifrarne il contenuto o forgiarne di nuovi e immetterli in rete. In tabella è mostrata anche la direzione in cui si può eseguire l'attacco.

La possibilità di forgiare nuovi pacchetti è la più pericolosa perché permette di iniettare traffico malevolo nella rete, come mostrato in questo video esplicativo https://www.youtube.com/watch?v=Oh4WURZoR98