Scuola Politecnica e
delle Scienze di Base
Università degli Studi di Napoli Federico II

Facoltà di Ingegneria delle Telecomunicazioni

KRACK Attack

Network Security - Bianca Ruggiero M59/167

WPA/WPA2

Protocollo di sicurezza introdotto nel 2003 nell' *amendment* di 802.11i per ovviare alla vulnerabilità del protocollo WEP.

L'*amendment* ha definito:

- **il 4-way-handshake**
- **Wi-Fi Protected Access-Temporal Key Integrity Protocol (WPA-TKIP)**
- **Advanced Encryption Standard-CCMP (AES-CCMP))**

Il protocollo WPA/WPA2 è considerato formalmente sicuro.

4-Way-Handshake

Algoritmo necessario per generare le chiavi temporanee per la crittografia, comincia dopo la fase di autenticazione ed associazione del client all'AP.

Vengono generate due tipi di chiave:

- **Pairwise Transient Key (PTK)**

  $f(PMK, A\ Nonce, S\ Nonce, A\ MAC, S\ MAC)$ PMK = Pairwise Master Key, segreto pre-condiviso

  viene poi suddivisa in:

  - Key Confermation Key (KVK)
  - Key Encription Key (KEK)
  - Temporal Key (TK)

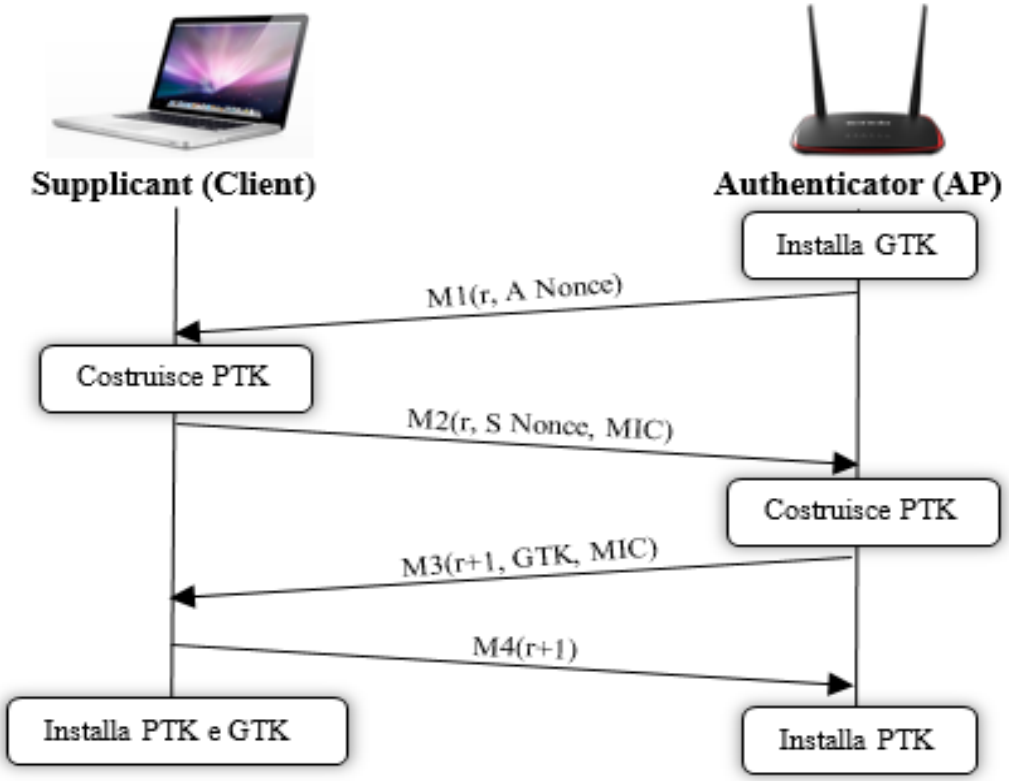
- **Group Temporal Key (GTK)**

  $f(GMK, A\ Address\ , G\ Nonce)$

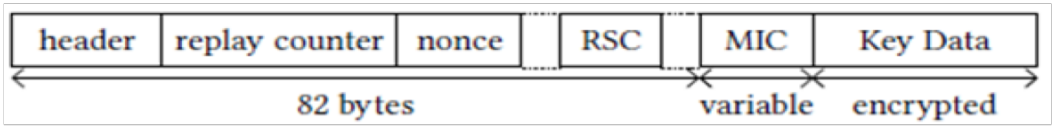
4-Way-Handshake

La PTK che viene generata, può essere aggiornata sempre attraverso un nuovo 4-way-handshake, dove però tutti i messaggi sono criptati utilizzando il PTK corrente.

Inoltre è possibile che si possano perdere le frame è dunque il client si troverà a gestire la ritrasmissione dei messaggi in particolare del primo e del terzo.



Frame EAPOL



La parte di dimensione fissa (82 bytes) è composta:

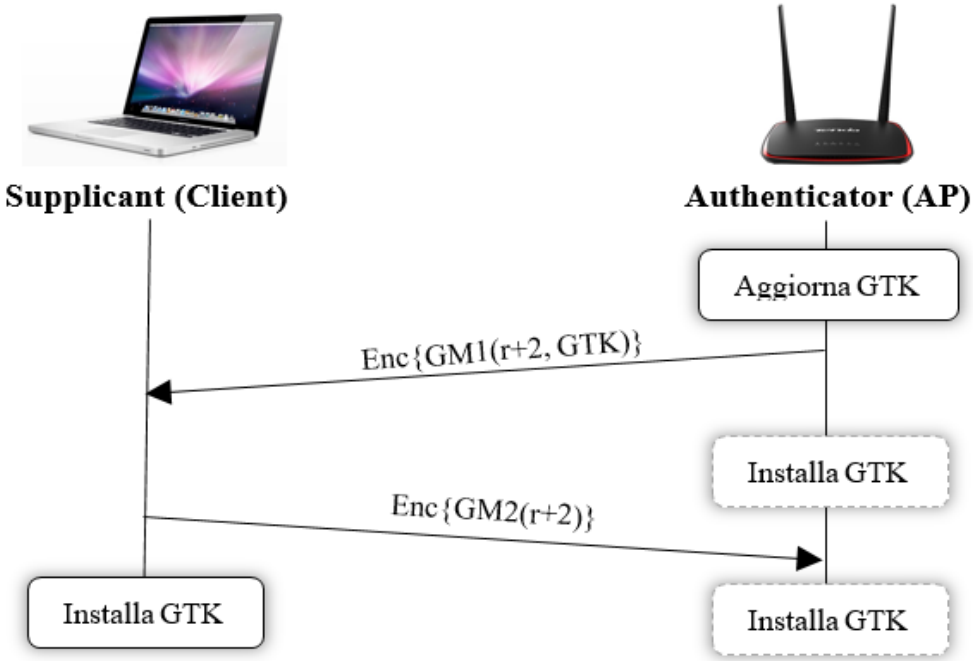
- **header**, identifica quale messaggio viene inviato
- **replay counter**, contatore incrementale utilizzato per rilevare eventuali frame ripetute
- **nonce**, nonce casuale che genera singolarmente il supplicant e l'authenticator.
- **reciver sequence counter (RSC)**, contiene il numero di pacchetto iniziale della GTK, se prevista.

La parte a dimensione variabile si compone dei campi:

- **key data**, contiene la GTK ed eventuali altri parametri, campo protetto dalla KEK.
- **Message integrity check (MIC)**, utilizzato per la verifica di autenticità della frame che viene protetta dalla KCK.

Group Handshake

La GTK viene aggiornata periodicamente dall'AP, che la distribuisce ai client connessi ad esso. Da notare che la GTK, contenuta nel campo key data della frame EAPOL, è protetta dalla KEK, legata alla PTK corrente.



Protocolli di integrità e riservatezza dei dati

- Temporal Key Integrity Protocol (TKIP)
  - La TK viene suddivisa in una chiave di 128 bit e due chiavi MIC rispettivamente usate per i due versi di comunicazione.
  - Viene usato RC4 per la crittografia che usa la chiave di 128 bit, l'indirizzo MAC del mittente e un nonce di 48 bit.
  - Il nonce viene incrementato per ogni frame trasmessa e viene inizializzato ad 1 dopo ogni installazione della TK, viene usato anche come replay counter.
  - Protocollo vulnerabile

Protocolli di integrità e riservatezza dei dati

- AES-CCMP
  - Protocollo basato su cifrario a blocchi
  - L'algoritmo crittografico che opera in modalità Counter Mode (CTR), viene accoppiato a un codice di autenticazione MAC (CBC-MAC) .
  - Utilizza un vettore di inizializzazione (IV) una concatenazione: indirizzo MAC mittente, nonce di 48 bit e flag aggiuntivi legati alla frame trasmessa
  - Nonce incrementato per ogni frame trasmessa ed inizializzato 0, viene usato anche come replay counter.
  - Protocollo più sicuro e più diffuso

Key Reinstallation Attack – 4-Way-Handshake

Requisiti:

- L'attaccante deve essere fisicamente presente e in posizione di Man-in-the-Middle (MitM), sul canale, tra il Client e l'AP.
- La vittima deve accettare la ritrasmissione della frame 3, nel 4-way-handshake
  - In chiaro
  - Protette dal protocollo di integrità e riservatezza dei dati, una volta installata la PTK.
- L'AP deve accettare messaggi di risposta con replay counter precedenti, non ancora ricevuti.
- Il client, nel caso riceve un messaggio 3 ritrasmesso crittografato con una PTK, non deve controllare se è stata effettivamente aggiornata.

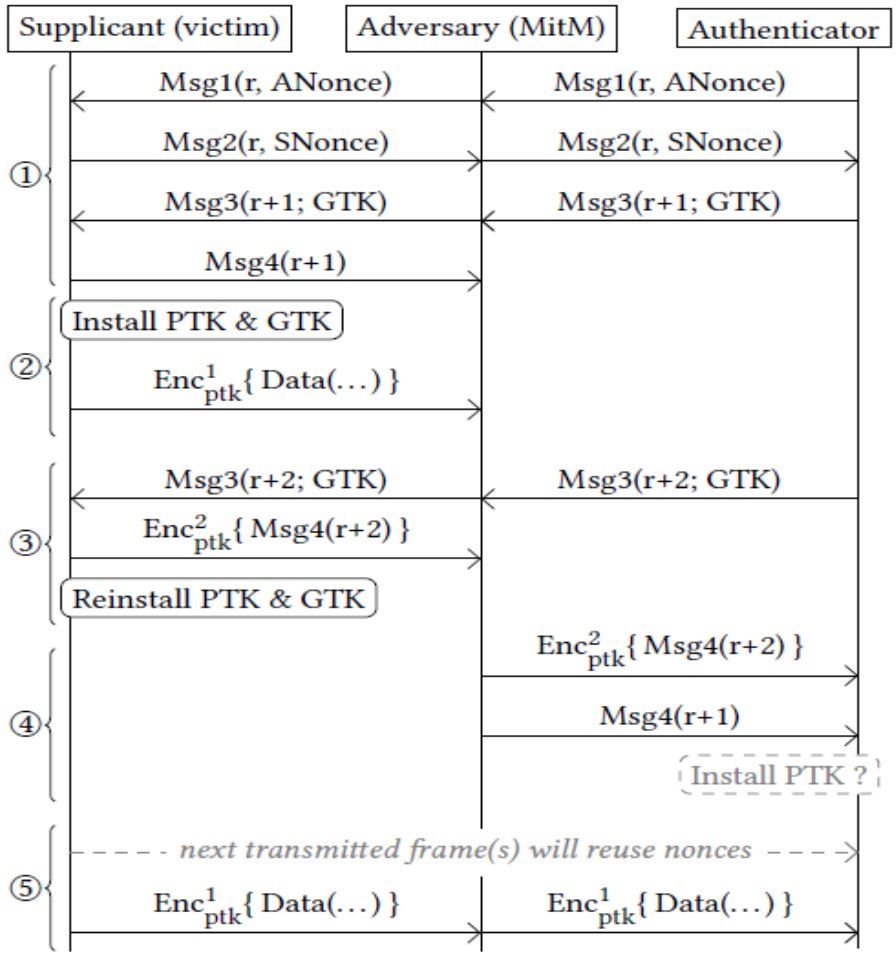
KRACK Attack

Key Reinstallation Attack – 4-Way-Handshake

La vittima accetta ritrasmissioni in chiaro del messaggio 3, dopo aver installato la PTK

Nota:

- L'attacco si può ripetere più volte, in quanto basta de-autenticare la vittima in modo da forzare un nuovo 4-way-handshake.
- La reinstallazione della PTK può verificarsi anche senza attaccante, a causa del rumore sul canale, per cui si può pensare anche ad un attacco jam.



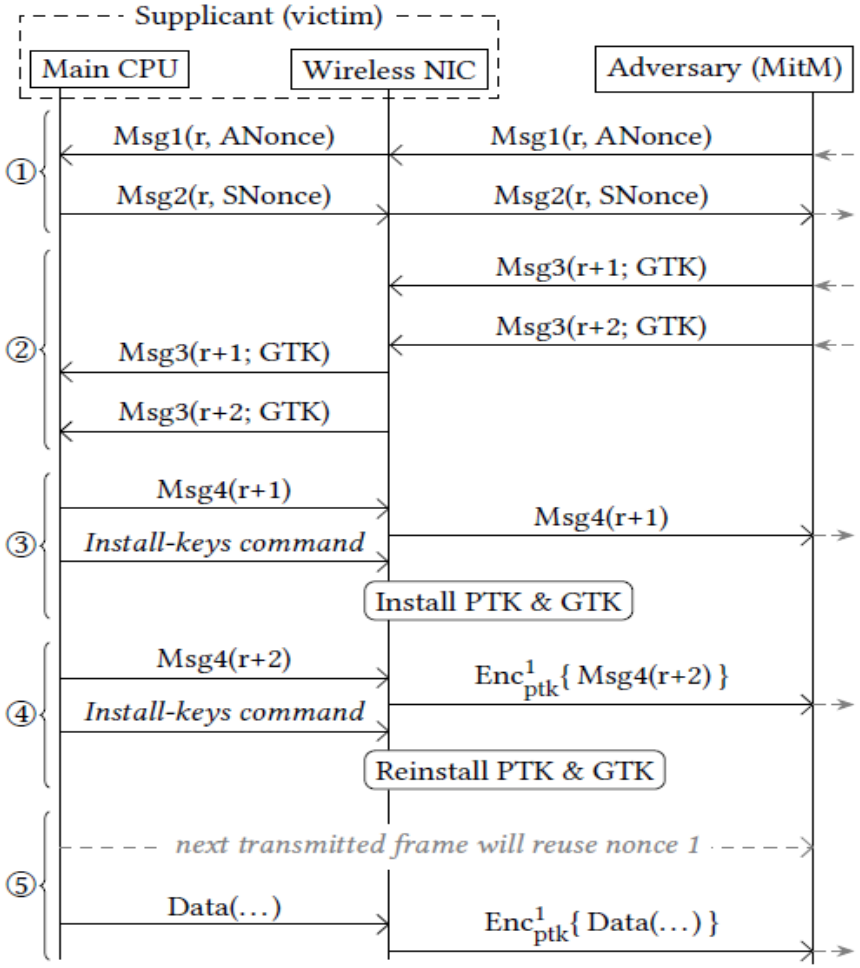
KRACK Attack

Key Reinstallation Attack – 4-Way-Handshake

La vittima accetta ritrasmissioni in chiaro del messaggio 3, dopo aver installato la PTK, solo se ricevute immediatamente una dopo l'altra. (Supplicant Android e Linux)

- Wireless NIC: implementa il protocollo di data-confidentiality.
- Main CPU: implementa il 4-way-handshake

Gli scambi tra attaccante e Authenticator sono gli stessi del caso precedente.



KRACK Attack

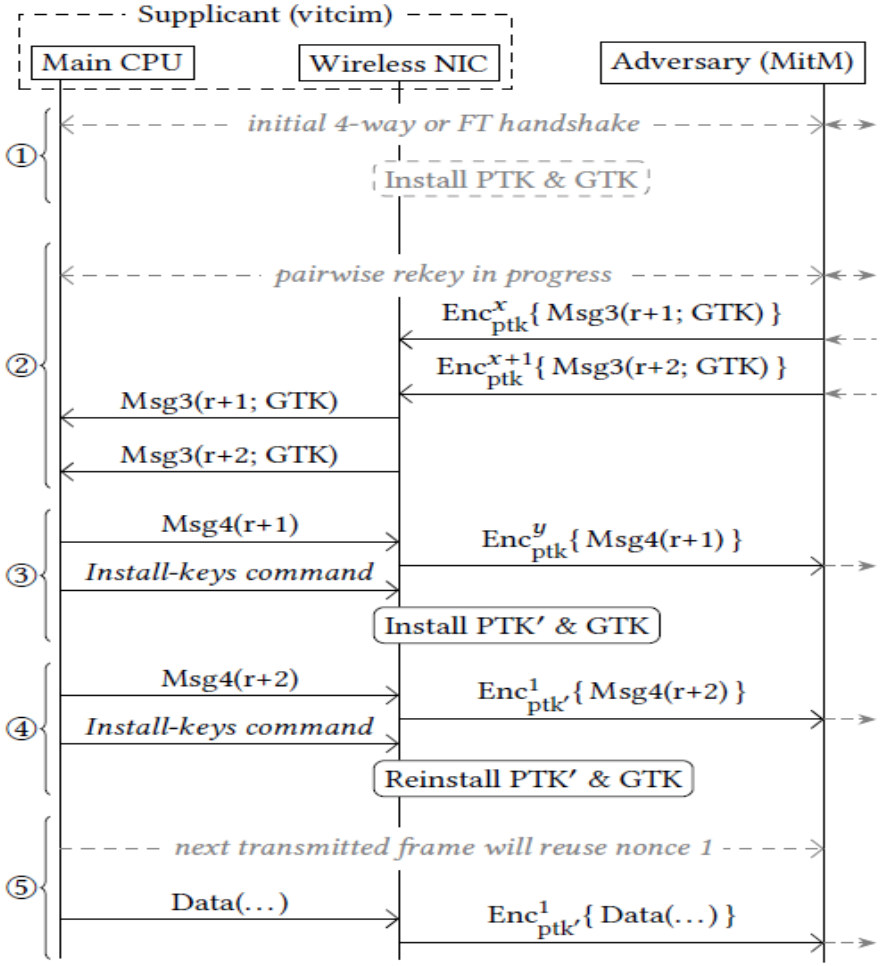
Key Reinstallation Attack – 4-Way-Handshake

La vittima accetta ritrasmissioni crittografate del messaggio 3, dopo aver installato la PTK. (OpenBSD, OS X, macOS)

- Wireless NIC: implementa il protocollo di data-confidentiality.
- Main CPU: implementa il 4-way-handshake

Gli scambi tra attaccante e Authenticator sono gli stessi del caso precedente.

L'attacco si fa in fase di rekey, che si può facilmente forzare.



Key Reinstallation Attack – Group Handshake

Requisiti:

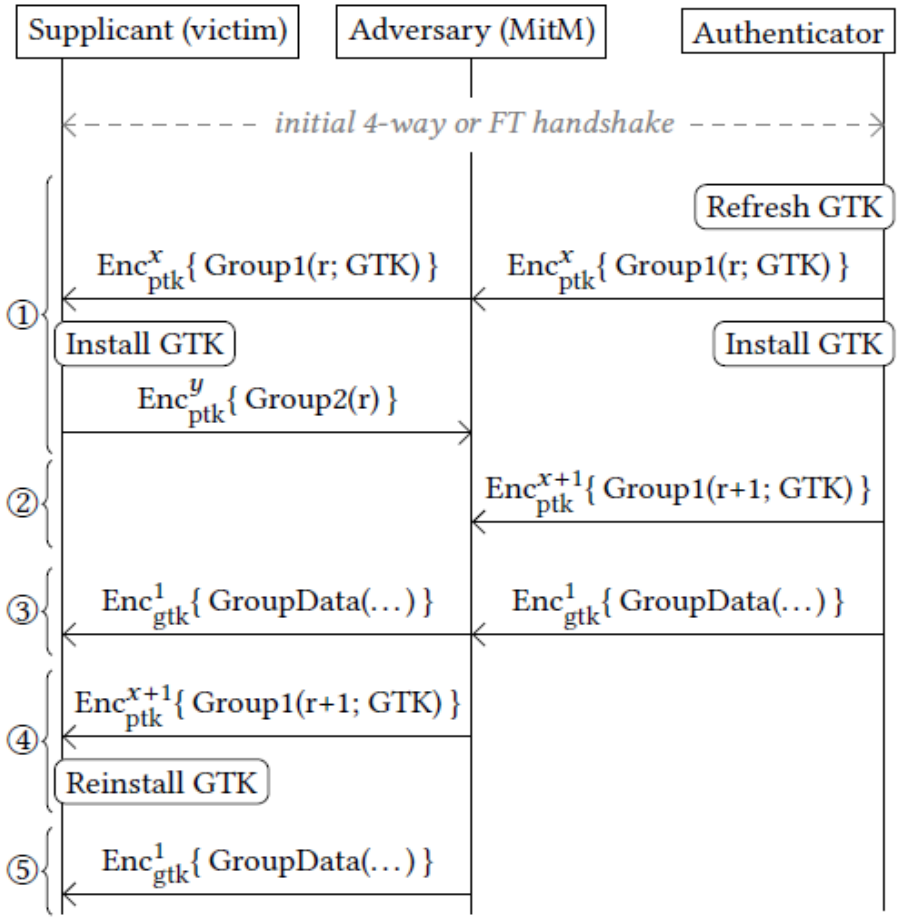
- L'attaccante deve essere fisicamente presente e in posizione di Man-in-the-Middle (MitM), sul canale, tra il Client e l'AP.
- La vittima deve re-inizializzare il replay counter durante l'installazione della GTK.
- L'attaccante deve riuscire a catturare il messaggio di gruppo 1, idoneo per il client e che contenga la chiave di gruppo già installata dall'AP.
- L'AP può installare la GTK:
  - subito dopo inviato il messaggio di gruppo 1
  - dopo aver ricevuto, la risposta dai client (complica un po' l'attacco)

L'attacco si può facilmente forzare

KRACK Attack

Key Reinstallation Attack – Group Handshake

L'AP installa la GTK subito dopo aver inviato il messaggio di gruppo 1.



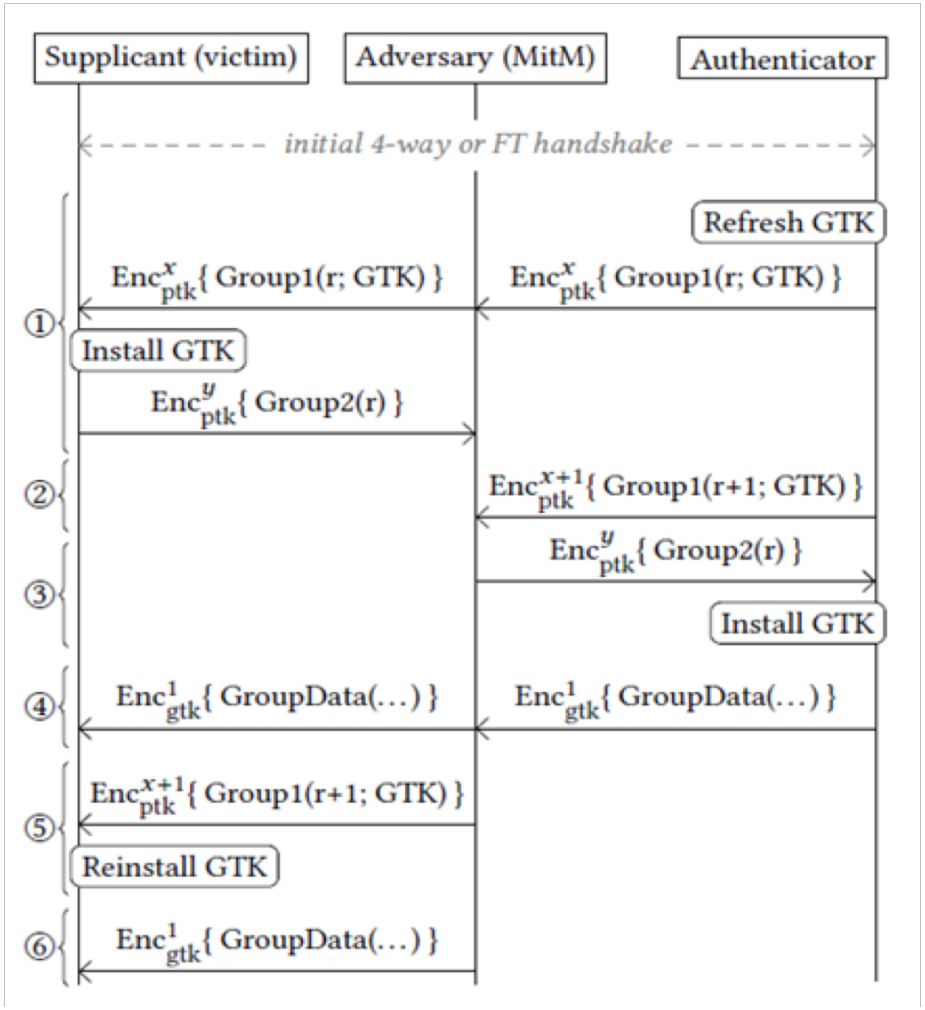
KRACK Attack

Key Reinstallation Attack – Group Handshake

L'AP installa la GTK in modalità ritardata, ovvero dopo aver ricevuto il messaggio di gruppo 2 dal client.

È necessario che l'AP accetti messaggi con replay counter antecedenti a quello corrente.

OpenBSD non è vulnerabile perché installa la GTK in modalità ritardata e accetta solo messaggi con replay counter corrente.



KRACK Attack

Key Reinstallation Attack – Fast Basic Service Set Transition Handshake

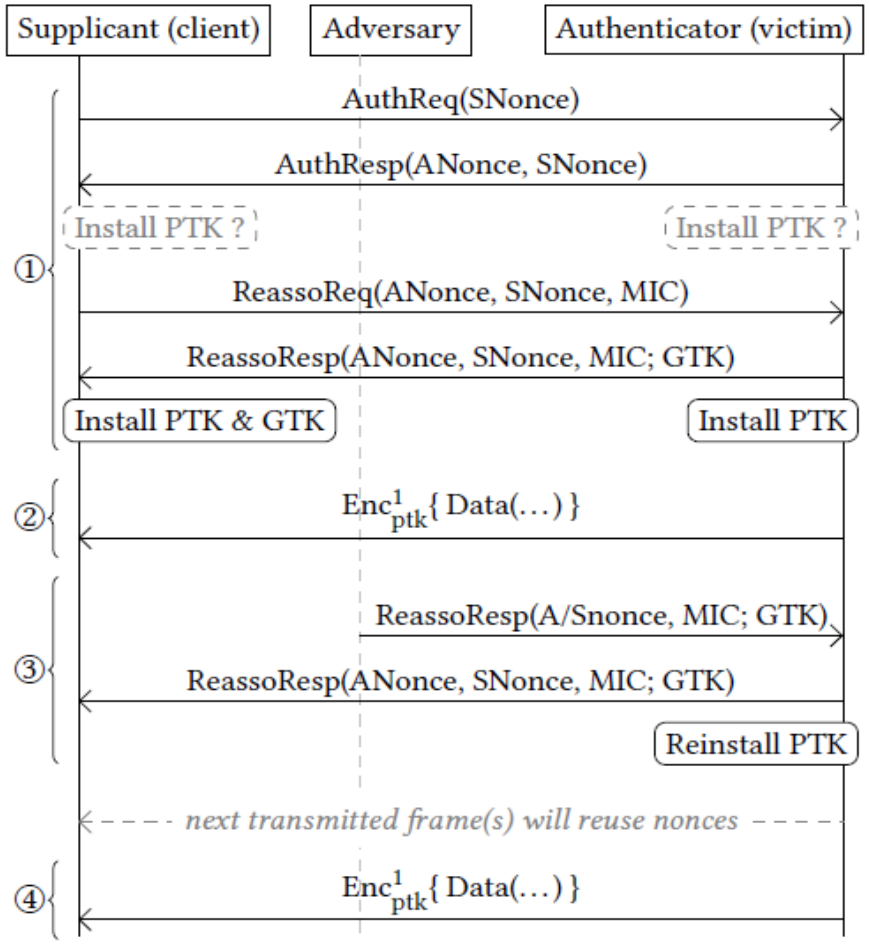
Definito in 802,11r, per ridurre il tempo di roaming del Client tra un AP e un altro sulla stessa rete protetta.

Nota:

La PTK dovrebbe essere installata dopo i messaggi di autenticazione, invece viene installata alla fine dell'handshake.

Attacco devastante: il messaggio di ri-associazione può essere ritrasmesso perché non c'è il replay counter.

Non è necessaria la posizione MitM



Key Reinstallation Attack – Impatto

- Il riutilizzo del nonce, implica il riutilizzo del keystream, che porta a decifrare le frame.
- La ripetizione del replay counter, permette attacchi di tipo replay.
- Se si usa TKIP è possibile recuperare il MIC, e di conseguenza forgiare frame nella direzione che parte dalla vittima :
  - il client, nel caso del 4-way-handshake
  - l'AP nel caso del FT handshake.
- Se si usa GCMP, (usato per Wireless Gigabit) si riesce a recuperare il MIC per entrambe le direzioni.
- In wpa-supplicant 2,4 e 2,5, l'attacco produce la reinstallazione di una chiave di crittografia con tutti zero.

Key Reinstallation Attack – Contromisure

- Il protocollo di data-confidentiality dovrebbe verificare se è incorso la reinstallazione di una PTK già in uso, e nel caso non reimpostare il nonce e/o il replay counter associato.
- Assicurarsi che la chiave sia installata una sola volta nella Wireless NIC, durante l'handshake.
- Essere più rigorosi nella descrizione e nell'implementazione degli standard.
- Installare sempre gli ultimi aggiornamenti proposti dai rispettivi produttori.

KRACK Attack

Test dispositivi

I dispositivi, gli applicativi e i sistemi operativi vulnerabili sono vari, anche se ognuno implementa lo standard in modo diverso.

Si sottopongono al test 3 dispositivi:

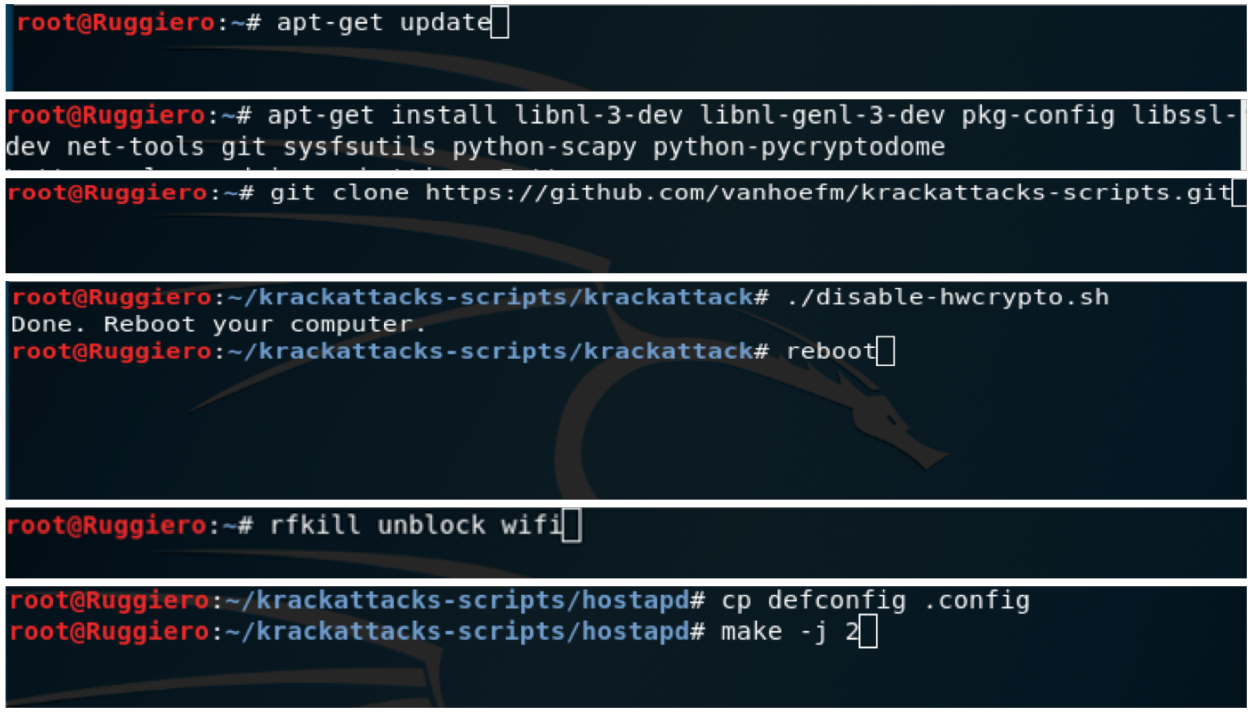
- Samsung Galaxy S4, GT-I9505-Versione Android 5.0.1
- OUKITEL, U11 Plus – Versione Android 7.0
- Iphone 4S, MD239B/A – Versione iOS 9.3.5 (13G36)

Il test che viene effettuato è il **./krack-test-client.py**, che testa la reinstallazione delle chiavi nel 4-way-handshake sia della PTK sia della GTK.

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.

Test dispositivi – Configurazione Kali Linux



Test dispositivi – Lancio dello script

```
root@Ruggiero:~/krackattacks-scripts/krackattack# ./krack-test-client.py
[12:16:22] Note: disable Wi-Fi in network manager & disable hardware encryption.
 Both may interfere with this script.
[12:16:22] Starting hostapd ...
Configuration file: /root/krackattacks-scripts/krackattack/hostapd.conf
Using interface wlan0 with hwaddr 48:5d:60:c4:db:69 and ssid "testnetwork-maggio
2018"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
[12:16:23] Ready. Connect to this Access Point to start the tests. Make sure the
 client requests an IP using DHCP!
[12:16:24] Reset PN for GTK
[12:16:26] Reset PN for GTK
[12:16:28] Reset PN for GTK
[12:16:31] Reset PN for GTK
```

Test dispositivi – Configurazione per il monitoraggio

```
root@Ruggiero:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k           Qualcomm Atheros AR9285 Wireless Network
 Adapter (PCI-Express) (rev 01)
phy1    wlan1           rtl8187         NetGear, Inc. WG111v3 54 Mbps Wireless [
realtek RTL8187B]
```

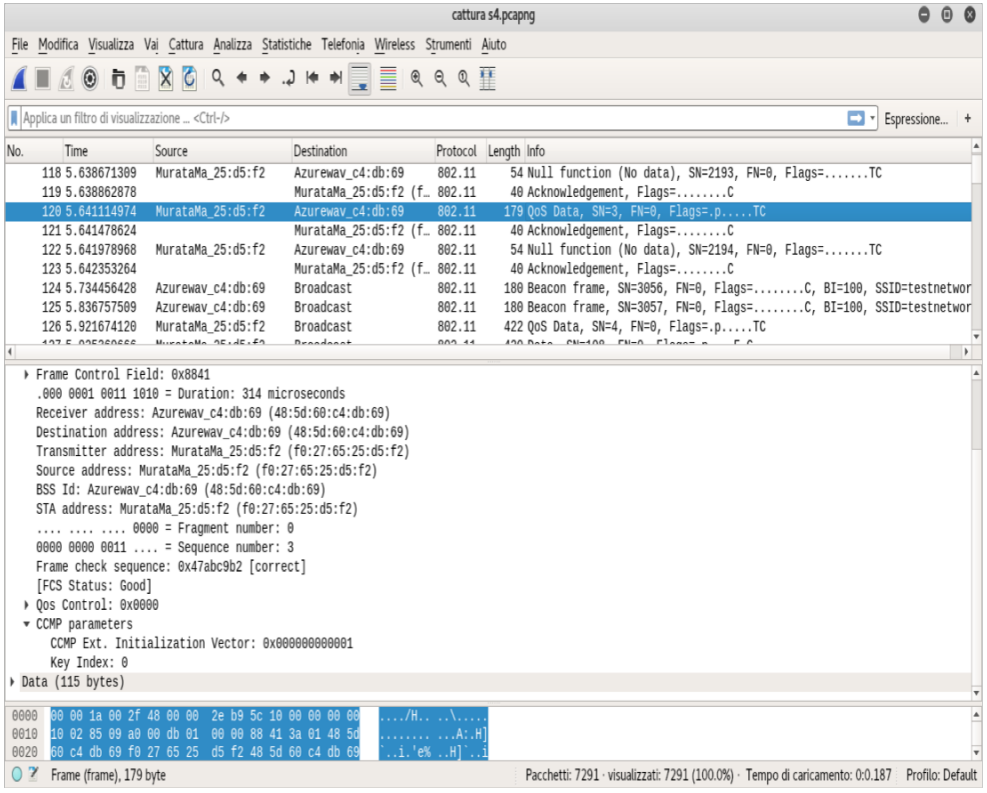
```
root@Ruggiero:~# airmon-ng check kill

Killing these processes:

  PID Name
  525 wpa_supplicant
```

```
root@Ruggiero:~# airmon-ng start wlan1
```

```
root@Ruggiero:~# iwconfig wlan1mon channel 6
root@Ruggiero:~# airodump-ng wlan1mon --channel 6
```

```
CH  6 ][ Elapsed: 6 s ][ 2018-05-30 19:06

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

48:5D:60:C4:DB:69  -16 100       69        0    0   6  54e  WPA2 CCMP   PSK  testnetwork-maggio2018

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   3C:CF:5B:AE:58:36  -65    0 - 1      1        4
```

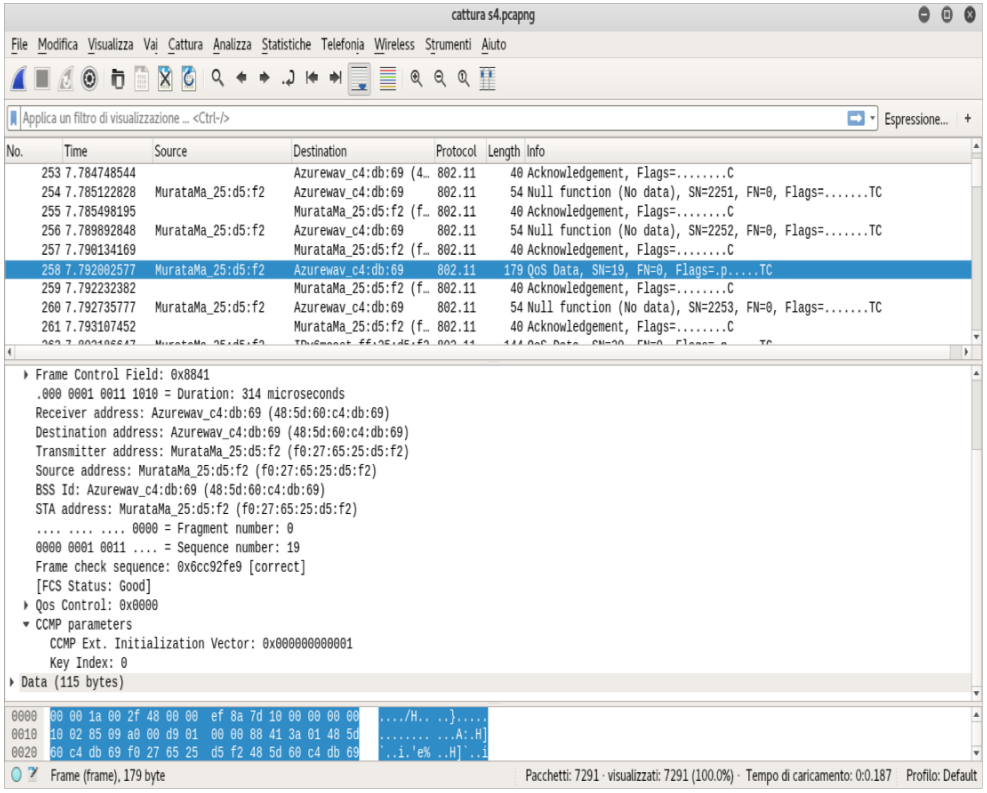
Test dispositivi – I° Dispositivo




```
[14:59:25] Reset PN for GTK
[14:59:25] f0:27:65:25:d5:f2: sending a new 4-way message 3 where the GTK has a zero RSC
[14:59:25] f0:27:65:25:d5:f2: DHCP reply 192.168.100.2 to f0:27:65:25:d5:f2
[14:59:27] Reset PN for GTK
[14:59:27] f0:27:65:25:d5:f2: sending a new 4-way message 3 where the GTK has a zero RSC
[14:59:27] f0:27:65:25:d5:f2: client has IP address -> now sending replayed broadcast ARP packets
[14:59:27] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 0 ARPs this interval)
[14:59:27] f0:27:65:25:d5:f2: IV reuse detected (IV=1, seq=19). Client reinstalls the pairwise key in the 4-way handshake (this is bad)
[14:59:29] Reset PN for GTK
[14:59:29] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 1 ARPs this interval)
[14:59:31] Reset PN for GTK
[14:59:31] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 2 ARPs this interval)
```

```
[15:00:22] Reset PN for GTK
[15:00:22] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 3 ARPs this interval)
[15:00:24] Reset PN for GTK
[15:00:24] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 4 ARPs this interval)
[15:00:26] Reset PN for GTK
[15:00:26] f0:27:65:25:d5:f2: Client DOESN'T reinstall the group key in the 4-way handshake (this is good)
[15:00:26] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 1 ARPs this interval)
[15:00:28] Reset PN for GTK
[15:00:28] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 2 ARPs this interval)
[15:00:30] Reset PN for GTK
```

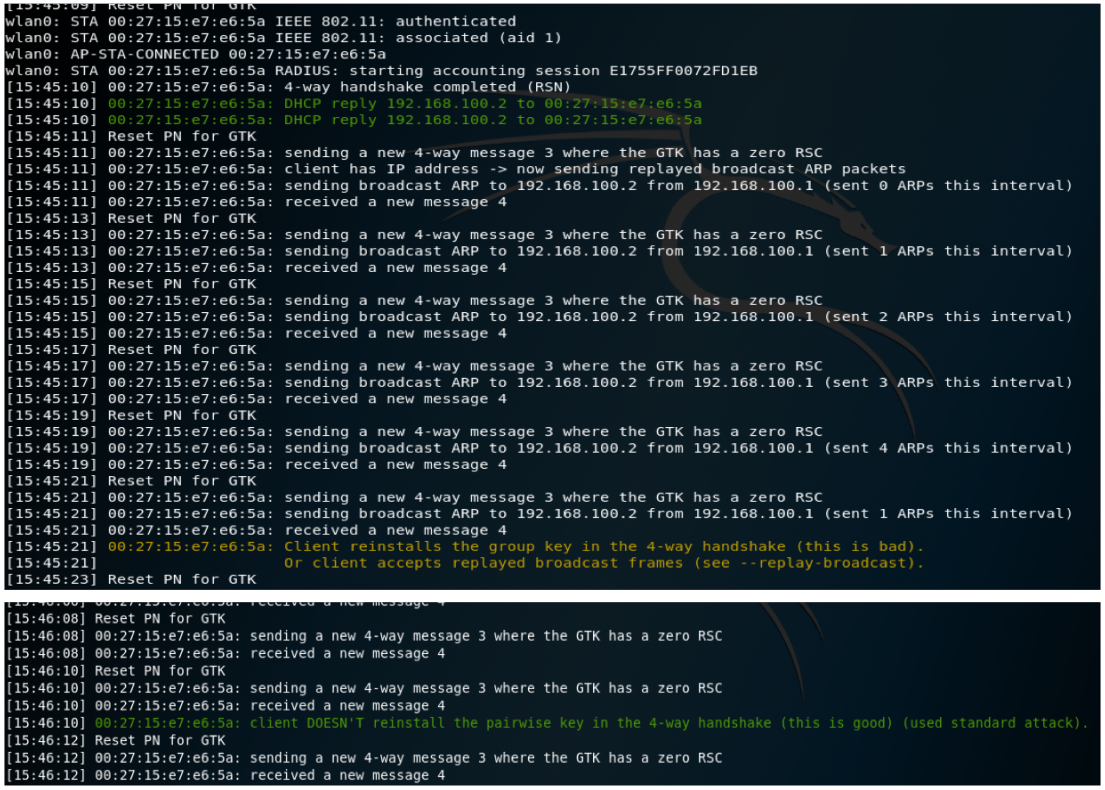
Test dispositivi – I° Dispositivo




```
[14:59:25] Reset PN for GTK
[14:59:25] f0:27:65:25:d5:f2: sending a new 4-way message 3 where the GTK has a zero RSC
[14:59:25] f0:27:65:25:d5:f2: DHCP reply 192.168.100.2 to f0:27:65:25:d5:f2
[14:59:27] Reset PN for GTK
[14:59:27] f0:27:65:25:d5:f2: sending a new 4-way message 3 where the GTK has a zero RSC
[14:59:27] f0:27:65:25:d5:f2: client has IP address -> now sending replayed broadcast ARP packets
[14:59:27] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 0 ARPs this interval)
[14:59:27] f0:27:65:25:d5:f2: IV reuse detected (IV=1, seq=19). Client reinstalls the pairwise key in the 4-way handshake (this is bad)
[14:59:29] Reset PN for GTK
[14:59:29] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 1 ARPs this interval)
[14:59:31] Reset PN for GTK
[14:59:31] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 2 ARPs this interval)
```

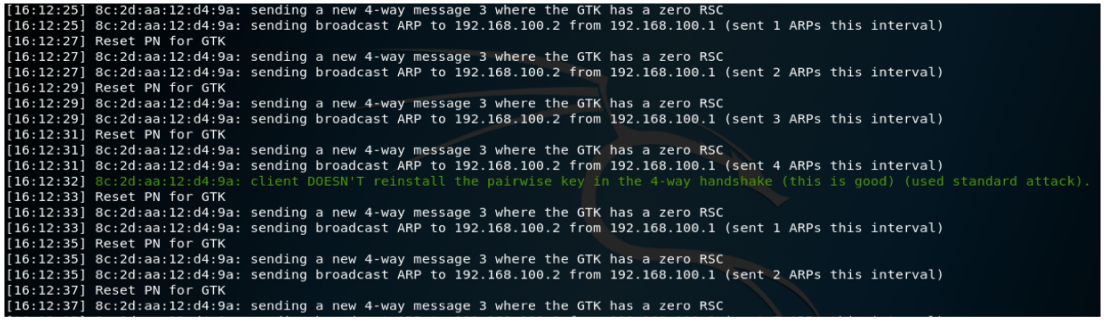
```
[15:00:22] Reset PN for GTK
[15:00:22] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 3 ARPs this interval)
[15:00:24] Reset PN for GTK
[15:00:24] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 4 ARPs this interval)
[15:00:26] Reset PN for GTK
[15:00:26] f0:27:65:25:d5:f2: Client DOESN'T reinstall the group key in the 4-way handshake (this is good)
[15:00:26] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 1 ARPs this interval)
[15:00:28] Reset PN for GTK
[15:00:28] f0:27:65:25:d5:f2: sending broadcast ARP to 192.168.100.2 from 192.168.100.1 (sent 2 ARPs this interval)
[15:00:30] Reset PN for GTK
```

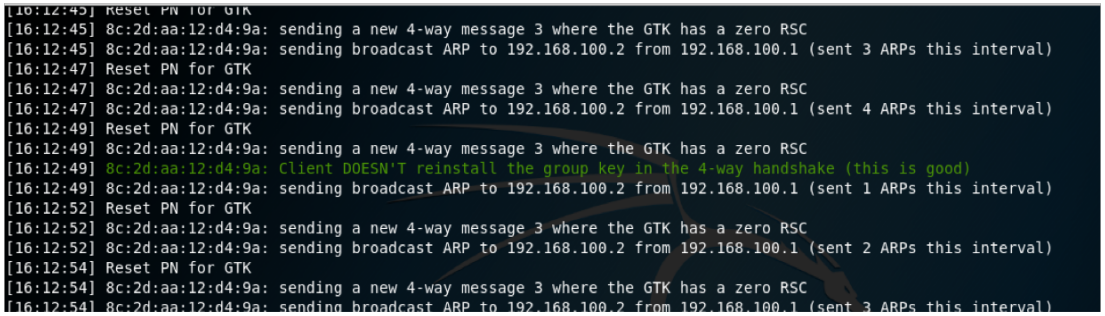
Test dispositivi – II° Dispositivo



Test dispositivi – III° Dispositivo

Non presenta vulnerabilità relative alla reinstallazione della chiave di sessione PTK, ne GTK





Conclusioni

Attacco abbastanza grave, ma comunque limitato all'area intorno al target.

Buona norma avvalersi:

- di protocolli sicuri come HTTPS, SSL/TLS, SSH
- delle reti VPN

Unico modo per proteggersi è aggiornare i sistemi con le ultime patch messe a disposizione.

Cambiare password e renderle più complesse non serve a mitigare l'attacco.

Sviluppi futuri

- Testare più dispositivi
- Utilizzare gli altri script messi a disposizione da Mathy Vanhoef
- Approfondire l'analisi dei pacchetti su WireShark

Scuola Politecnica e
delle Scienze di Base
Università degli Studi di Napoli Federico II

Facoltà di Ingegneria delle Telecomunicazioni

FINE