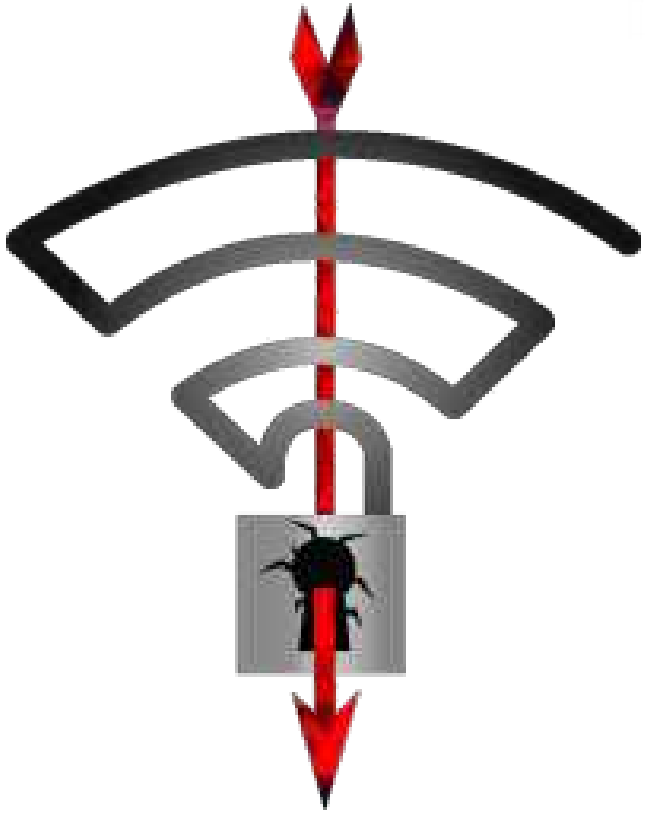
WiFi WPA/WPA2 KrackAttack



Paolo Giardini
STUDIO GIARDINI
Eucip Certified Informatics Professional
Consulente per la sicurezza delle Informazioni

Chiù WiFi pe' tutti!

Hotel, ristoranti, uffici, ospedali,… dapperttutto un fiorire di WiFi libere.

La domanda è: sono sicure? Se l'access point non è messo in sicurezza qualcuno potrebbe "ascoltare" le nostre comunicazioni, rubare password, ….

WPA2: la panacea di tutti i mali

Per proteggere le WiFI dagli attacchi e per impedire l'accesso non autorizzato, sono state implementate alcune misure di sicurezza.

Dapprima WEP (Wired Equivalent Privacy) che si è dimostrata non all'altezza del compito. Successivamente WPA (WiFi Protected Access) e quindi WPA2 nelle varie versioni (enterpirse).

Nel protocollo WPA il vettore di inizializzazione (IV) è più lungo di quello di WEP e viene utilizzato un altro metodo di cifratura delle informazioni utilizzando la cifratura RC4 ed un protocollo di integrità denominato TKIP (Temporal Key Integrity Protocol).

Le comunicazioni Wireless sono salve, basta ricordarsi poche semplici regole: sostituire le password di default, usare password complesse e cambiale spesso.

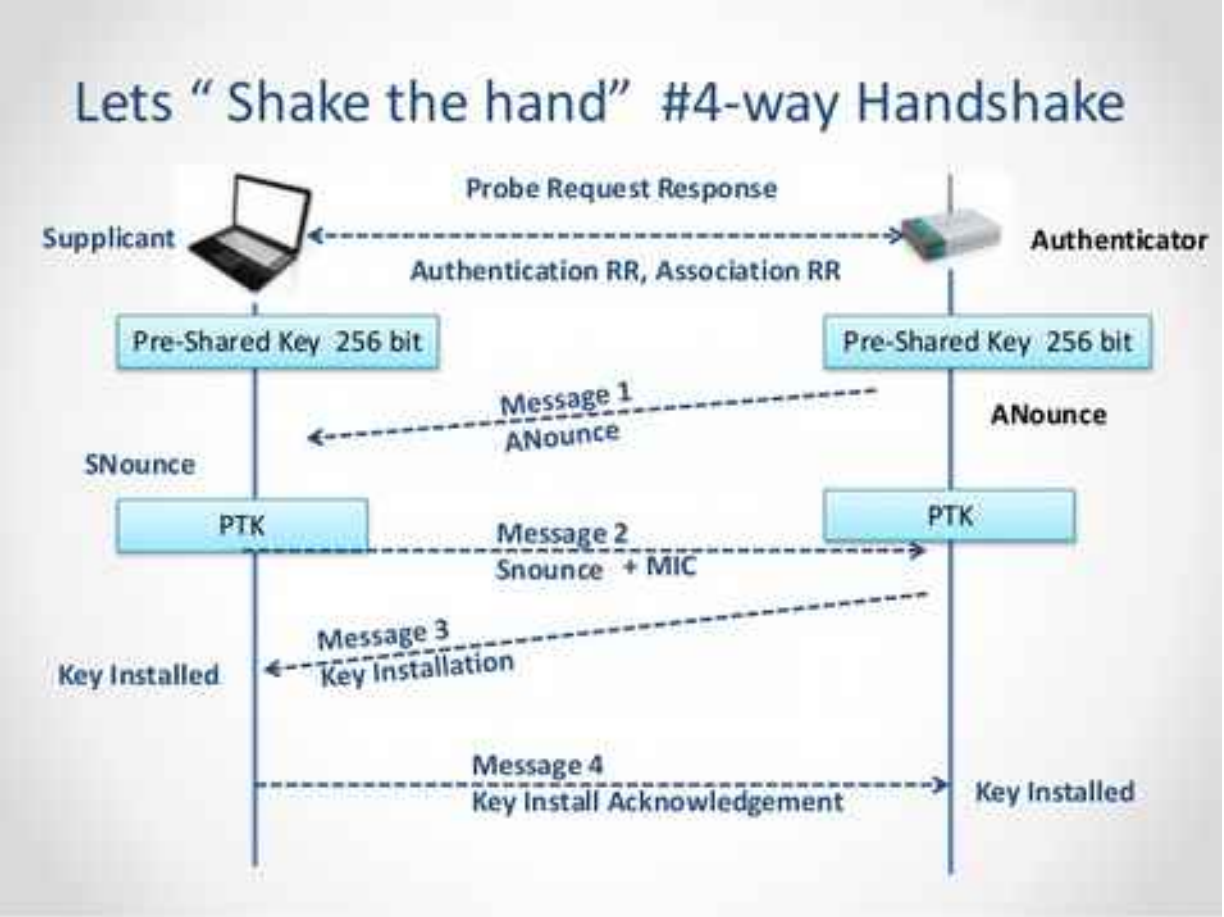
Come funziona WPA2

Ogni pacchetto trasmesso usando TKIP ha un serial number a 48 bit incrementato ogni volta che viene trasmesso un nuovo pacchetto e utilizzato sia come Vettore di Inizializzazione (IV) che come parte della chiave.

Inserire un numero di sequenza nella chiave assicura che la chiave sia diversa per ogni pacchetto.

PTK: Pairwise Transient Key

https://en.wikipedia.org/wiki/IEEE_802.11i-2004



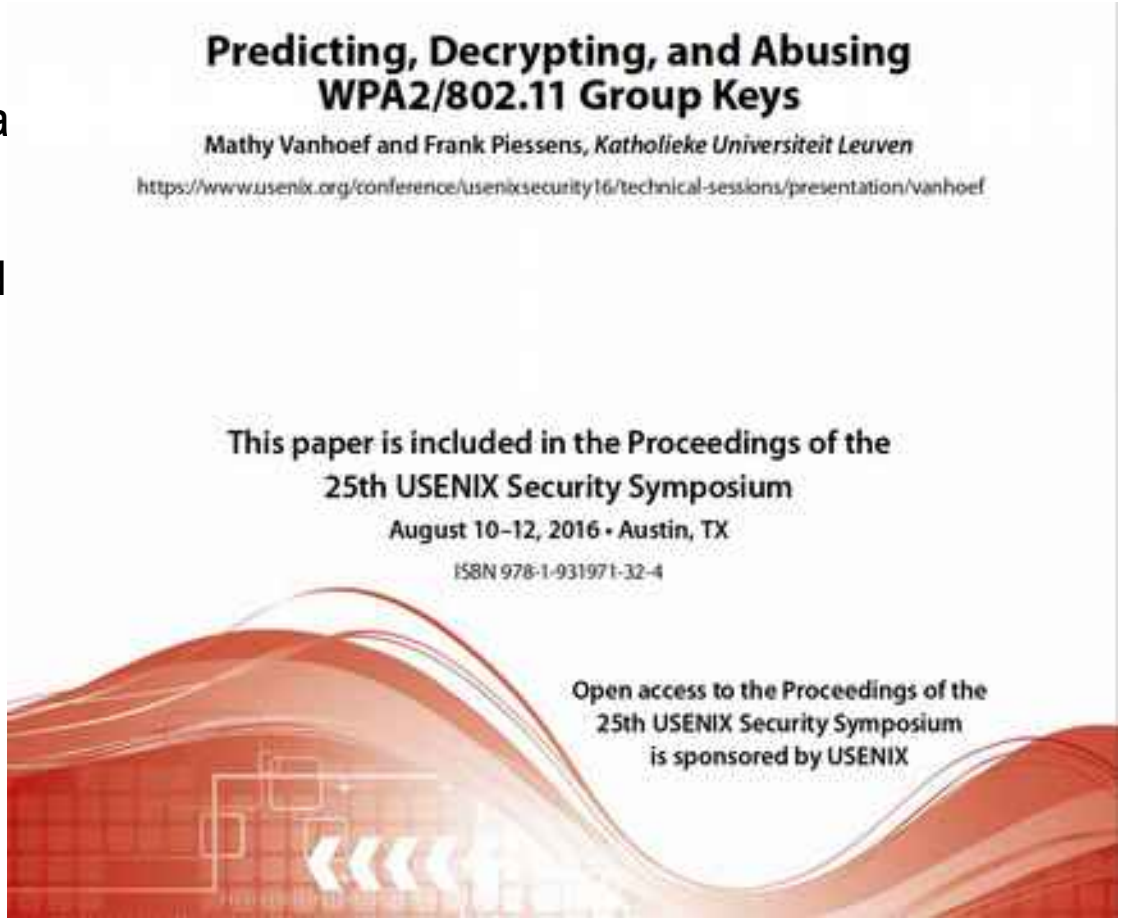
Fine di una favola

Già dallo scorso agosto un ricercatore ha evidenziato come i generatori di numeri casuali utilizzati per creare le PSK nel protocollo WPA non sono così casuali ed in qualche misura sono prevedibili.

Queste ricerche sono sfociate nel recente annuncio del KRACK ATTACK contro la WPA/WPA2.

La ricerca sarà presentata il 1 novembre 2017 ad ACM Conference on Computer and Communications Security a Dallas

https://www.krackattacks.com/

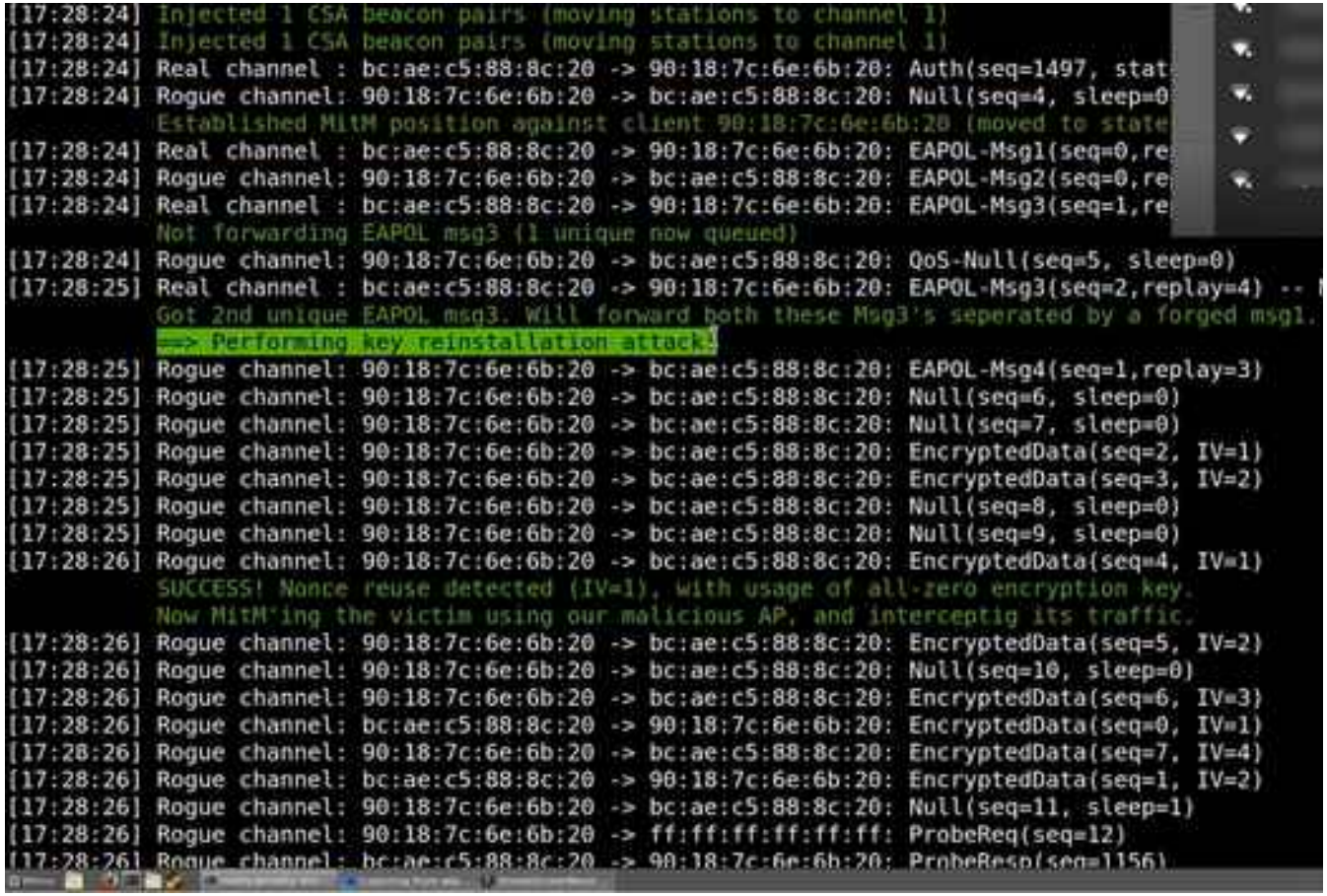


Krack Attack

L'attacco KRACK viene eseguito contro il **4-ways handshake** che viene eseguito quando un client tenta di collegarsi ad un access point.

Durante il **4-ways handshake** viene generata una nuova chiave di crittografia che verrà utilizzata per crittografare i dati scambiati tra stazione e client.

Questa chiave verrà installata dal client quando riceve il terzo pacchetto del **4-ways handshake.**



KRAck in teoria

Se il messaggio 3 (key installation) non viene ricevuto dal client, questi non invierà la conferma alla stazione.
Se la stazione non riceve la conferma, invierà di nuovo il messaggio 3 al client.
Ciò significa che il client può ricevere il messaggio 3 più volte.

Ogni volta che il client riceve il messaggio 3, reinstalla nuovamente la chiave resettando l'incremental transmit packet number (nonce) ed il receuive packet number al valore iniziale.

Nel Key Reinstallation Attack (KRAck) l'attaccante raccoglie e invia il messaggio 3 della 4-way handshake per forzare questi reset del pacchetto nonce, con conseguente decrittazione dei pacchetti, replay attack e man-in-the-middle.

Rischi e contromisure

Praticamente tutti gli apparati che usano WiFi sono vulnerabili, sia che usino WPA, WPA2, WPA Enterprise, AES…

Gli attacchi più gravi sono contro i client

Pensiamo a IoT (brrrr….!)

Non esistono contromisure. Ironicamente, alcuni apparati che non seguono gli standard potrebbero non essere vulnerabili...

Cosa fare

- Cambiare le password non serve a nulla
- Installare le patch sui client prima possibile, nel frattempo usare una VPN
- Aggiornare i kernel degli access point
- Verificare se possibile disabilitare ritrasmissione msg handshake sugli AP
- Non tutti gli apparati sono aggiornabili: **SOSTITUIRLI!**

Tools

- Test vulnerabilità access point

  https://github.com/vanhoefm/krackattacks-test-ap-ft
- Detect KRAck Attack

  https://github.com/kismetwireless/kismet

Grazie per l'attenzione

Paolo Giardini

Consulente per la protezione delle informazioni

paolo.giardini@solution.it

http://www.solution.it

http://blog.solution.it

http://www.accordance.it