Release the KRACK-en!!

WPA2 is dead. Welcome WPA2

TheZero - `https://files.thezero.org/kracken.pdf`

@ToHack - 12/2017

TOHack

Cos’è WPA2

Cos'è WPA2

- Attuale standard Wi-Fi protetto [IEEE 802.11i-2004]
- Versione rinnovata di WPA [draft IEEE 802.11i-2003]
- Successore dell'ormai defunto WEP (R.I.P. 2010)

TOHack

YEEE

IEEE

IEEE STANDARDS STORE
In Partnership with Techstreet

SEARCH | IEEE Standards | GO

Standards Store Home | About IEEE-SA | Contact Us | Sign In | My Account | View Basket

IEEE 802.11i-2004

Most Recent

Track It

IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security

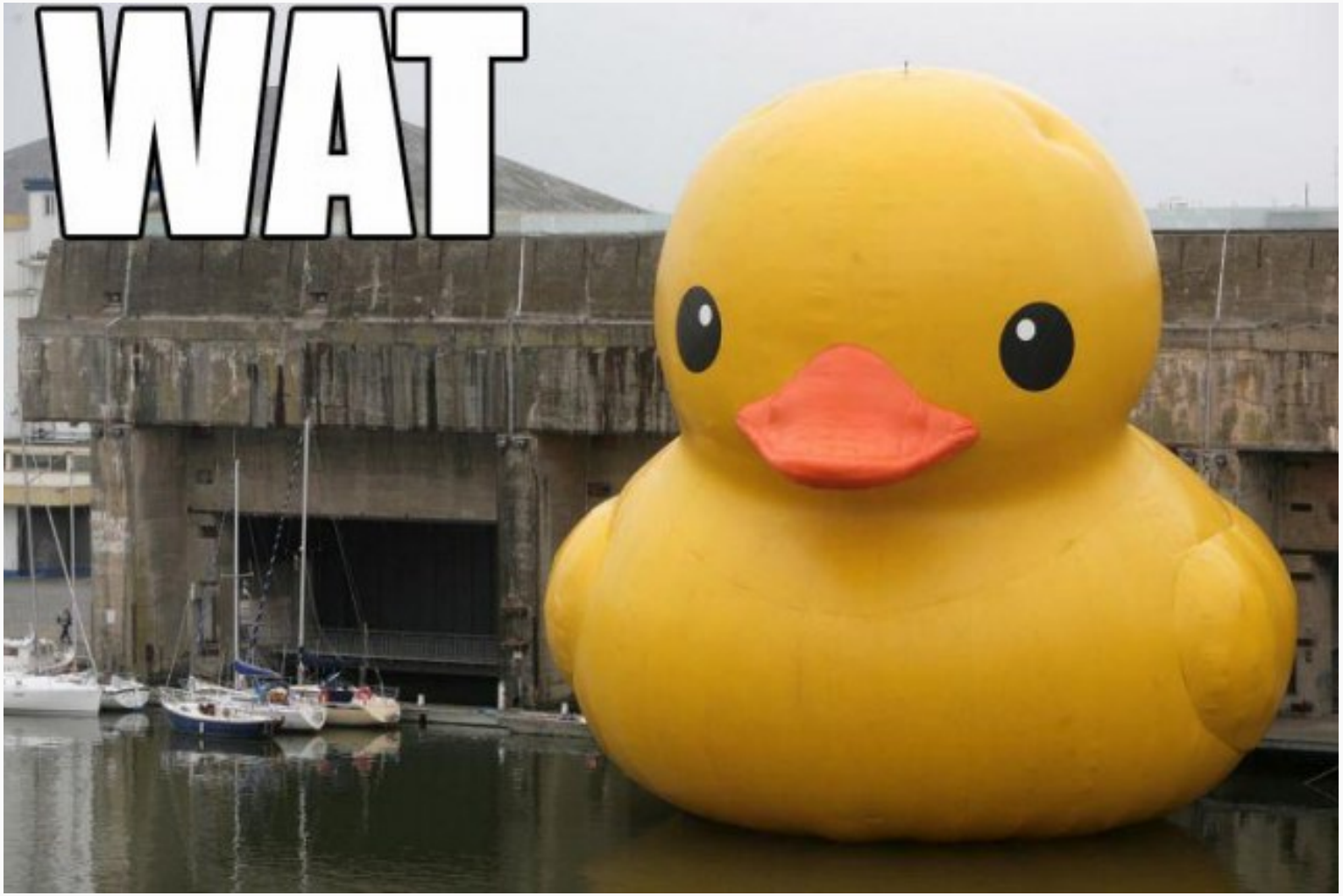
STANDARD by IEEE, 07/24/2004

View all product details

Language: English

Available Formats	Options	Availability	Priced From (in USD)	
PDF		Immediate download	**$170.00** Members pay $136.00	Add to Cart

Paywall WAT



TOHack

Protocollo

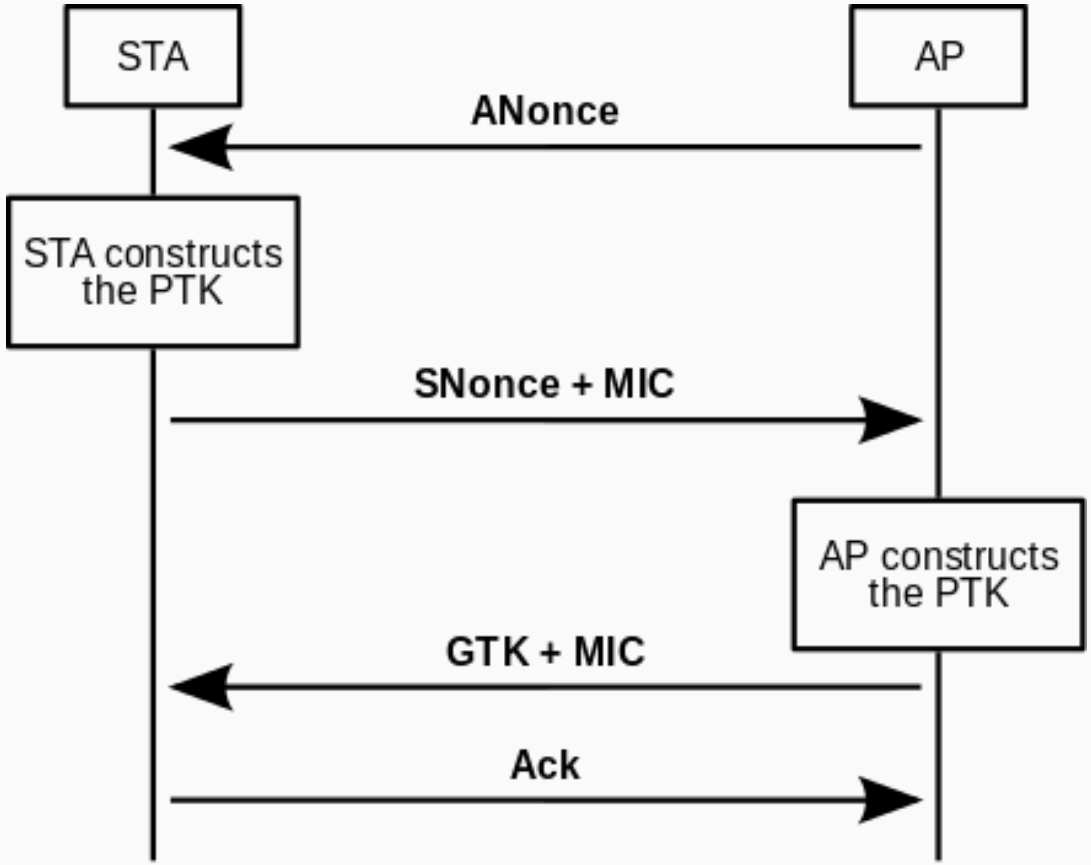
4-way Handshake

- "Verifica" tra un Supplicant (client) e Authenticator (AP)
- Avviene trasmettendo 4 messaggi
- *Milionari socialisti*
- Costruire la `PTK` (Pairwise Transient Key)
- Cifrato tramite `PMK` (Pairwise Master Key)
- `MIC` Message Integrity Check con `PTK`
- Key-Secrecy e Mutua autenticazione **verificati formalmente** da terze parti

```
PTK = PMK + ANonce + SNonce + AMAC + SMAC
```

TOHack

4-way Handshake

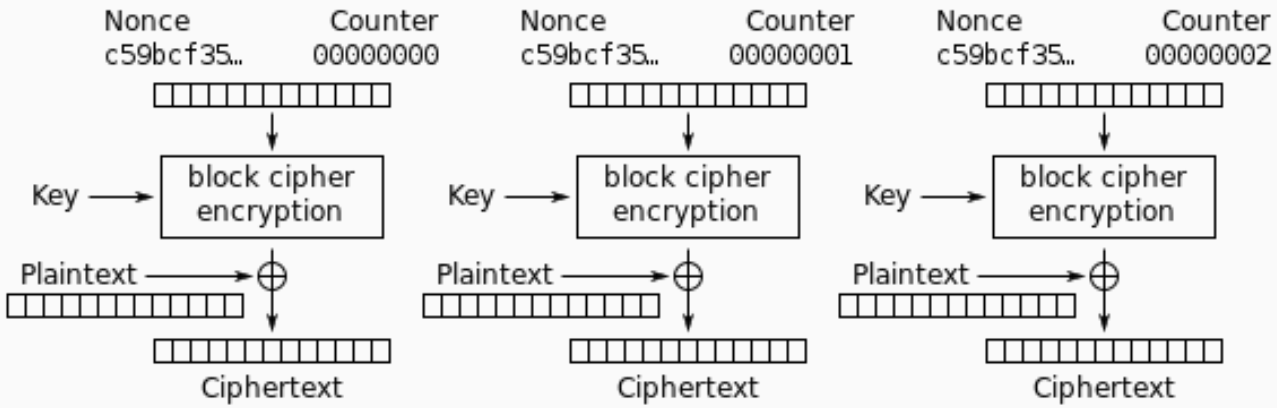


TOHack

Crypto

CCMP

- Usa `CCM = CTR + CBC-MAC`
- Authenticate-then-Encrypt *double-pass*
- **Proof-of-Security** finché l'algoritmo usato è sicuro (*AES*) e non vi è **nonce reuse** (KPA)

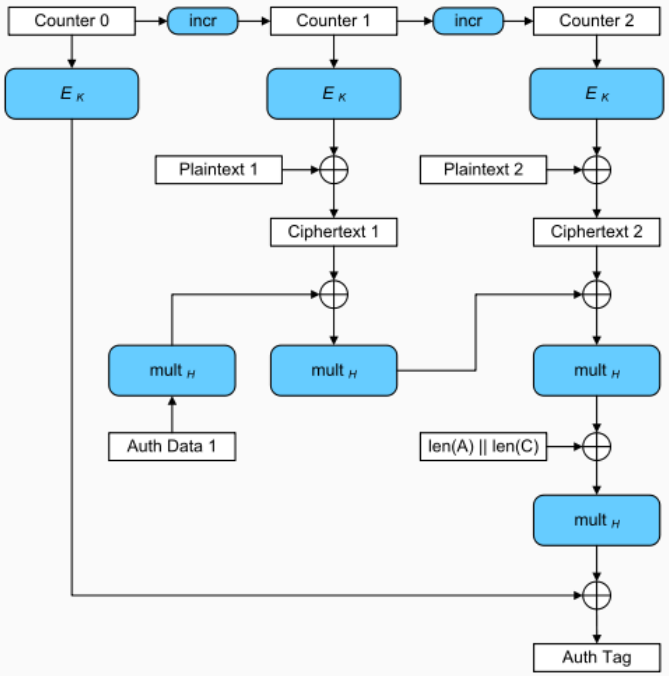


Counter (CTR) mode encryption

TOHack

GCMP

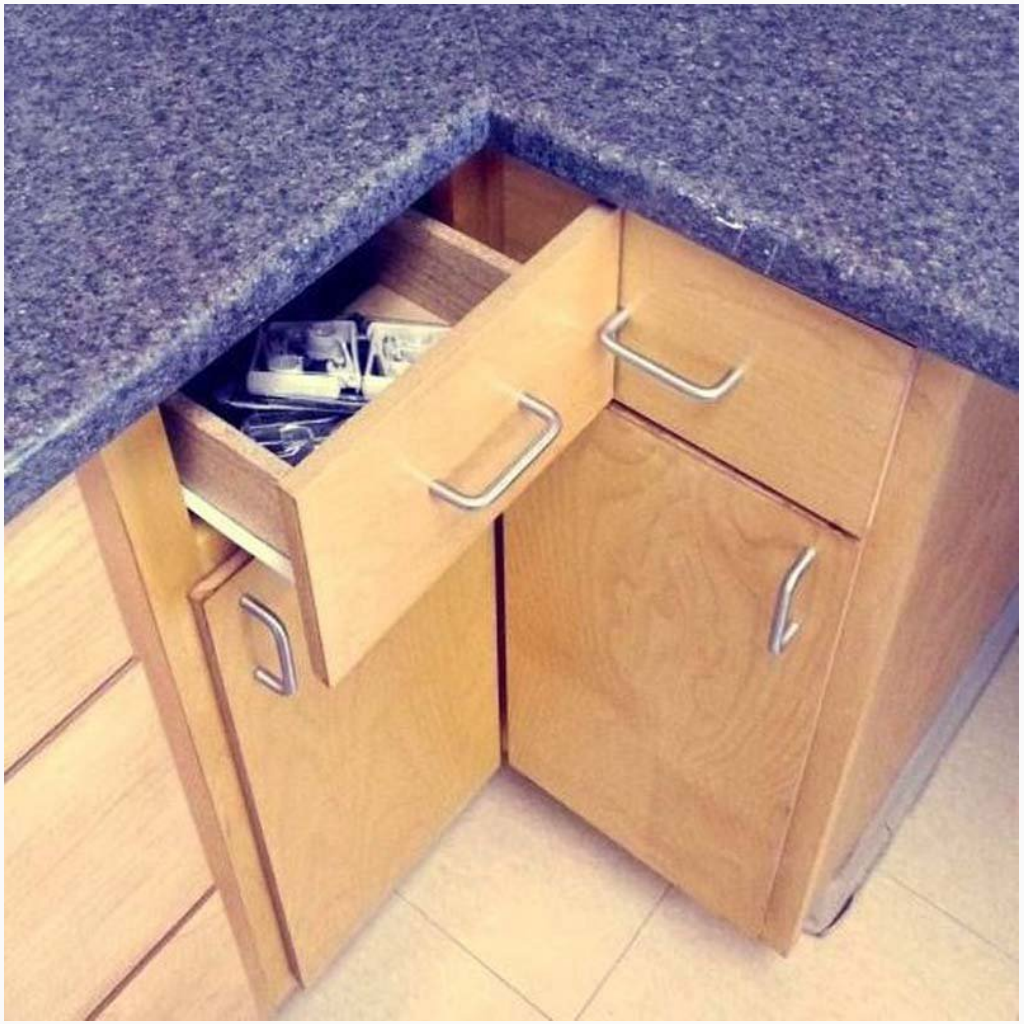
- Usa `GCM`
- `GCM` è basato su `CTR`
- Authenticated Encryption *single-pass*
- **Proof-of-Security** finché l'algoritmo usato è sicuro (*AES*) e non vi è **nonce reuse** (KPA)



TOHack

KRACK

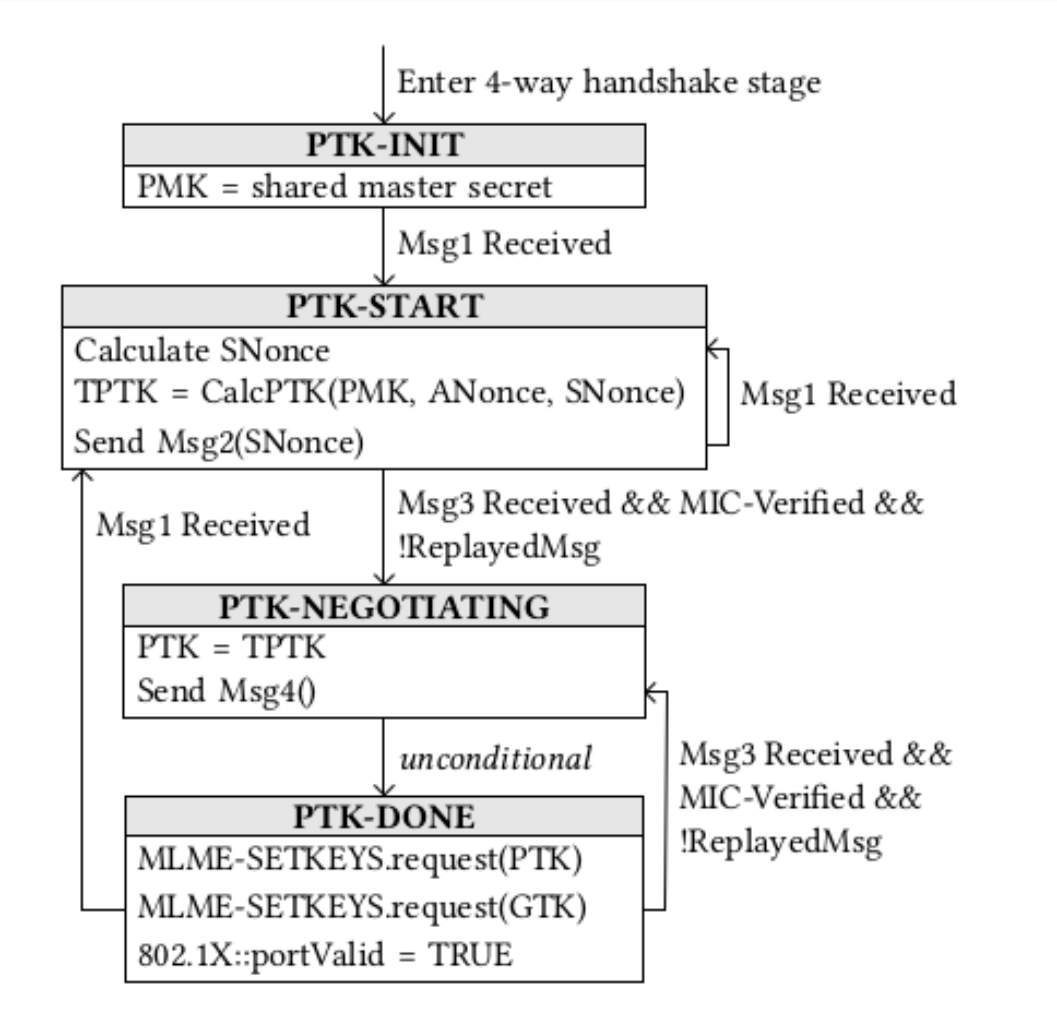
2 Unit test, 0 Integration test



TOHack

4-way HS State Machine

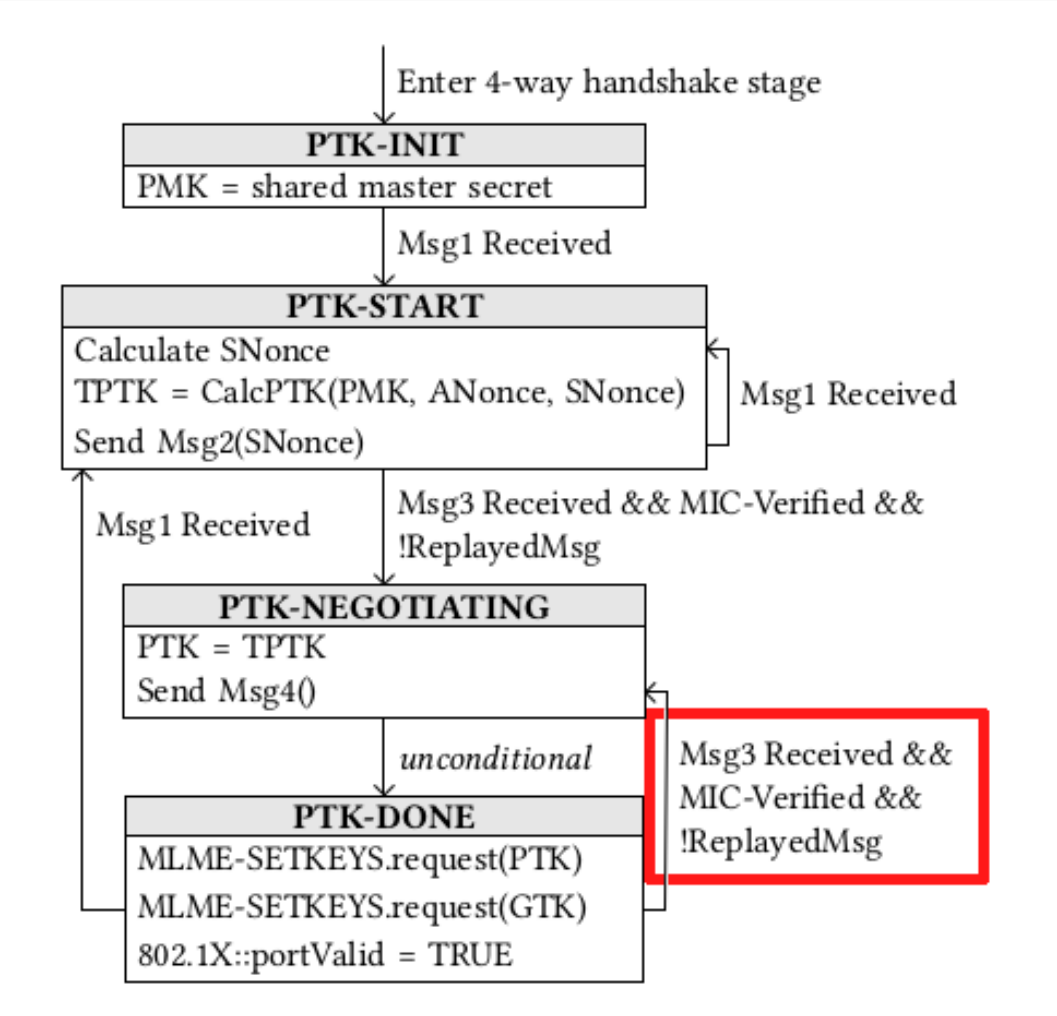
Supplicant State Machine



TOHack

4-way HS State Machine

Supplicant State Machine



TOHack

Cosa ha fatto KRACK?

Lo standard 802.11i indica esplicitamente che:

- L'AP deve ritrasmettere i messaggi 1 o 3 se non riceve risposta valida.
  Il client dovrà quindi gestire un'eventuale ritrasmissione.
- Il client deve installare la `PTK` subito dopo aver processato il messaggio 3
- È buona norma cancellare la chiave di cifratura una volta installata (*PTK? PMK? TK? TPTK?*)

TOHack

La cometa di Halley

TOHack

L’attacco

È necessaria una posizione di **channel-based MitM**

- Fake AP su un canale diverso dal AP
- Jamming del client sul canale del AP reale
- Spoof di entrambi i MAC address
- Hardware dedicato o Driver dedicato

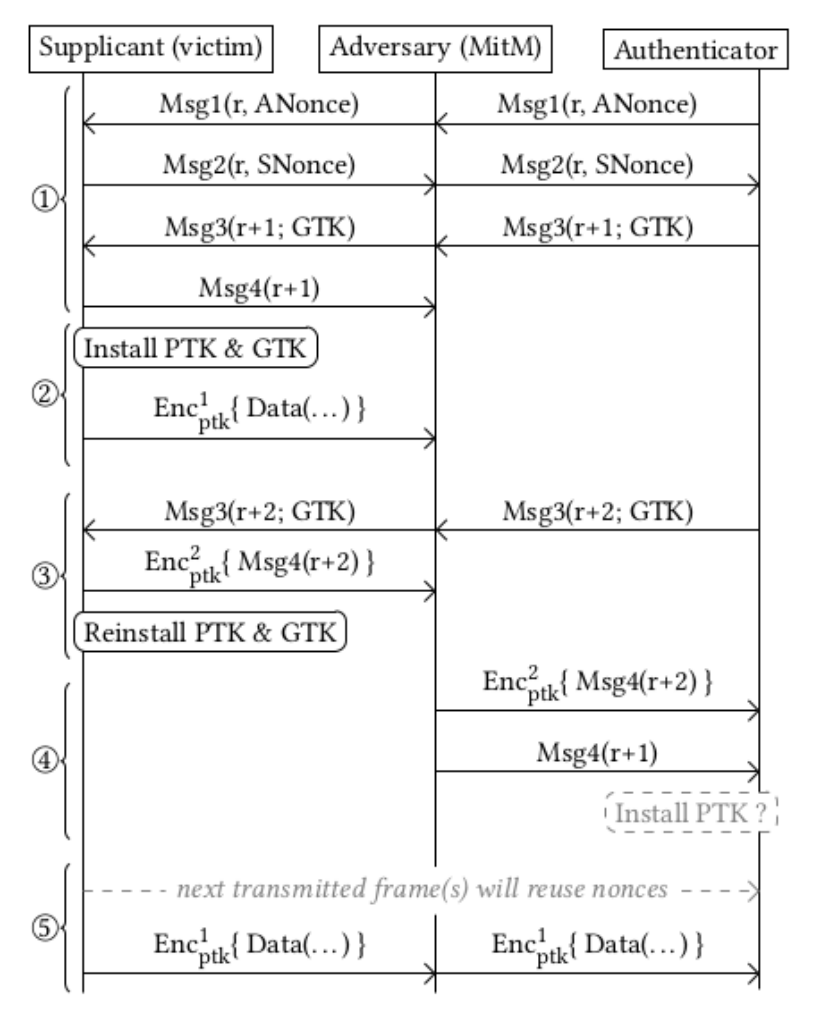
TOHack

L’attacco

- Si forwardano tutti i frame bloccando il messaggio 4 dell handshake
- L’AP ritrasmetterà il messaggio 3 forzando il client a reinstallare la `PTK` e **azzerare i propri nonce**
- **Known-Plaintext-Attack**: è possibile ricavare il keystream e decifrare ogni blocco con stesso nonce
- In `CCM` un attaccante può decifrare, in `GCM` può decifrare **e** forgiare!

TOHack

L’attacco



TOHack

L’attacco

TOHack

Vulnerabilità

Windows/iOS

Windows e iOS non accettano la ritrasmissione del messaggio 3.
Questo viola lo standard IEEE 802.11.
Per questo motivo queste due piattaforme non sono vulnerabili a questo tipo di attacco.

TOHack

Linux/Android: wpa_supplicant

Seguendo (?) il consiglio dello standard, `wpa_supplicant` cancella la `TPTK` appena viene installata come `PTK`.
Alla ricezione del messaggio 3 tenterà di reinstallare la `TPTK` e finirà con l'usare una chiave settata a `0`.

TOHack

Vulnerabilità in KRACK

Un attaccante può:

- Decifrare pacchetti arbitrari
  - Quindi prendere numeri di sequenza TCP e fare MitM
- Replay di frame broadcast e multicast
- Decifrare e iniettare pacchetti arbitrari (solo `GCMP`)
- Forzare il client ad usare chiavi prevedibili settate a `0` (Android 6.0+ e Linux)

Un attaccante **NON** può:

- Risalire alla password WPA2 del AP
- Iniettare pacchetti (solo `CCMP`)

TOHack

Soluzioni

Soluzioni

k

Soluzioni

[Original cartoon by Allie Bosh]

TOHack

Soluzioni

Evitare di reinstallare una `PTK` già in uso (senza ricominciare l'handshake)

Evitare channel-based MitM inserendo il canale nella `PTK`

TOHack

Domande?

Domande

TOHack

Riferimenti bibliografici

Riferimenti bibliografici

- https://www.krackattacks.com/ - Sito ufficiale KRACK
- https://papers.mathyvanhoef.com/ccs2017.pdf - Paper ufficiale di Mathy Vanhoef
- https://en.wikipedia.org/wiki/CCMP_(cryptography) - CCMP su wikipedia
- https://en.wikipedia.org/wiki/Galois/Counter_Mode - GCM su wikipedia
- https://en.wikipedia.org/wiki/Socialist_millionaires- Milionari socialisti su wikipedia

TOHack