

# KRACK attack (802.11i four-way handshake attack)

Vadim Davydov

19/03/2018



# Presentation agenda

- History of 802.11 security protocols
- 802.11i protocol
- 4-way handshake
- Techniques for confidentiality over 802.11i: TKIP, AES CCMP, AES GCMP
- Key re-installation attack on 4 way handshake
- Group key handshake
- Group key handshake break
- Countermeasures

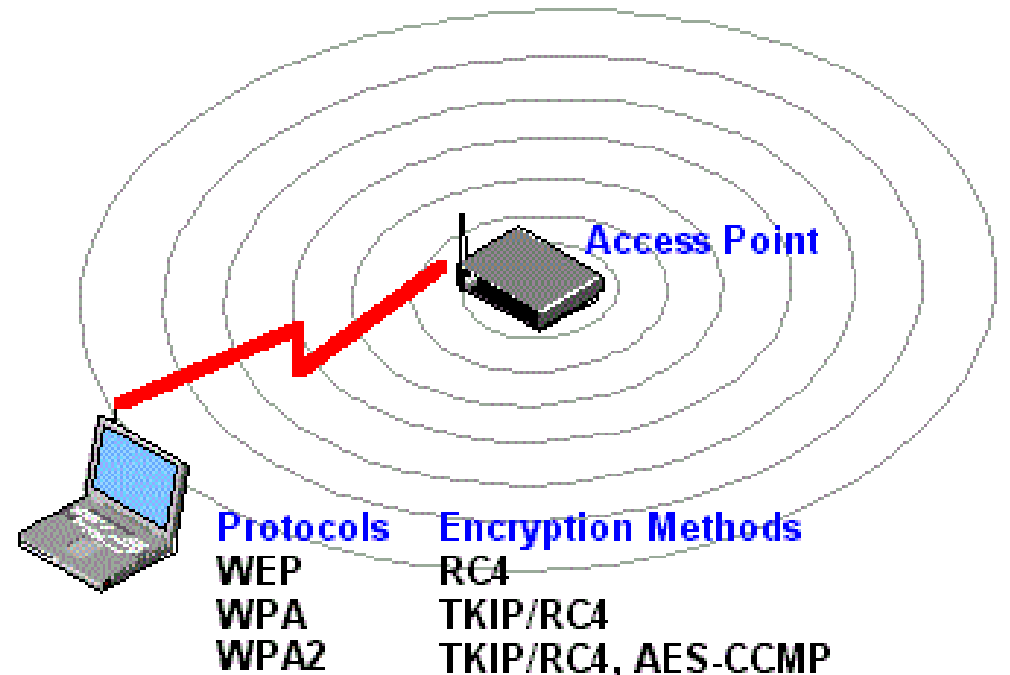
# History of 802.11 security protocols family

IEEE 802.11 is the set of standards that define communication for wireless local area networks (WLANs). The technology behind 802.11 is branded to consumers as Wi-Fi.



# History of 802.11 security protocols

- WEP (Wired Equivalent Privacy) is the first standard for Wi-Fi protection
- WPA (Wi-Fi Protected Access)
- WPA2



# Wireless security

Encryption standard	Fast facts	How it works
WEP	First standard for Wi-Fi protection. Can be easily hacked due to its 24-bit initialization vector and weak authentication	It uses RC4 stream cipher and 64- or 128-bit keys. Static master key must be manually entered into each device
WPA	Security protocol developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in WEP	Also uses RC4 but longer IVs and 256-bit keys are added. Each client gets new keys with TKIP
WPA2	WPA2 replaced WPA. It implements the mandatory elements of IEEE 802.11i. In particular, it includes mandatory support for CCMP, an AES-based encryption mode with strong security	Replaces RC4 and TKIP with CCMP and AES algorithm for stronger authentication and encryption

# 802.11i Protocol



# Used keys

```
graph TD; UK[Used keys] --> PMK[PMK (Pairwise Master Key)]; UK --> PTK[PTK (Pairwise Transient Key)]; UK --> GTK[GTK (Group Temporal Key)]; PTK --> KCK[KCK (Key Confirmation Key)]; PTK --> KEK[KEK (Key Encryption Key)]; PTK --> TK[TK (Temporal Key)];
```

## **PMK** (Pairwise Master Key)

- Derived from a pre-shared password in a personal network

## **PTK** (Pairwise Transient Key)

- Derived from PMK, ANonce, SNonce, MAC addresses of both

## **GTK** (Group Temporal Key)

- Generated by the Authenticator

## **KCK** (Key Confirmation Key)

– bits 0-127 of the PTK

- To protect handshake messages

## **KEK** (Key Encryption Key)

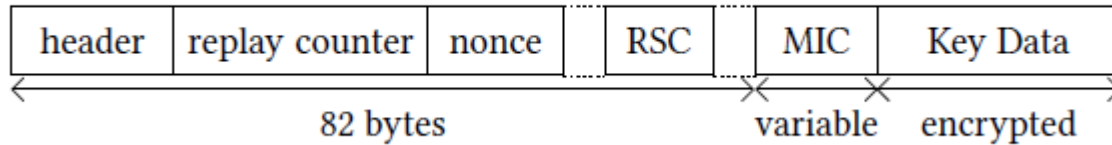
– bits 128-255 of the PTK

- To protect handshake messages

## **TK** (Temporal Key) – bits 256-383 of the PTK

- To protect normal data frames with a data-confidentiality protocol

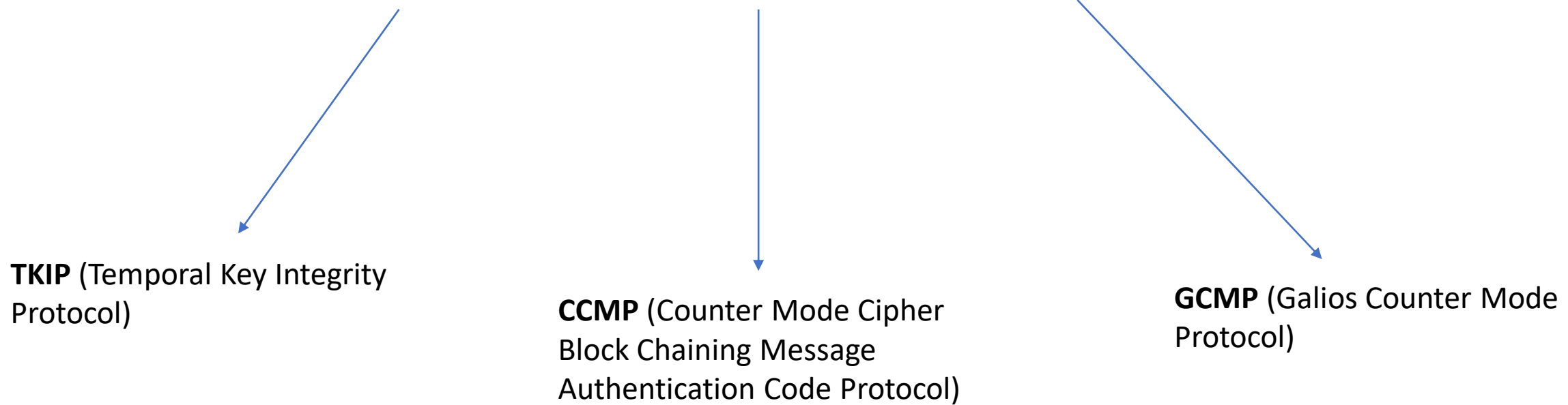
# EAPOL



- Header: which message in the handshake a particular EAPOL frame represents
- Replay Counter: to detect replayed frames
- Nonce: to transport random nonces to derive a fresh session key
- RSC (Receive Sequence Counter): contains the starting packet number of group key
- MIC (Message Integrity Check): the authenticity of the frame is protected using the KCK with a MIC
- Key Data: has the group key itself, which is encrypted using KEK



# 802.11i. Confidentiality and Integrity Protocols



```
graph TD; A[802.11i. Confidentiality and Integrity Protocols] --> B[TKIP (Temporal Key Integrity Protocol)]; A --> C[CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol)]; A --> D[GCMP (Galios Counter Mode Protocol)];
```

**TKIP** (Temporal Key Integrity Protocol)

**CCMP** (Counter Mode Cipher  
Block Chaining Message  
Authentication Code Protocol)

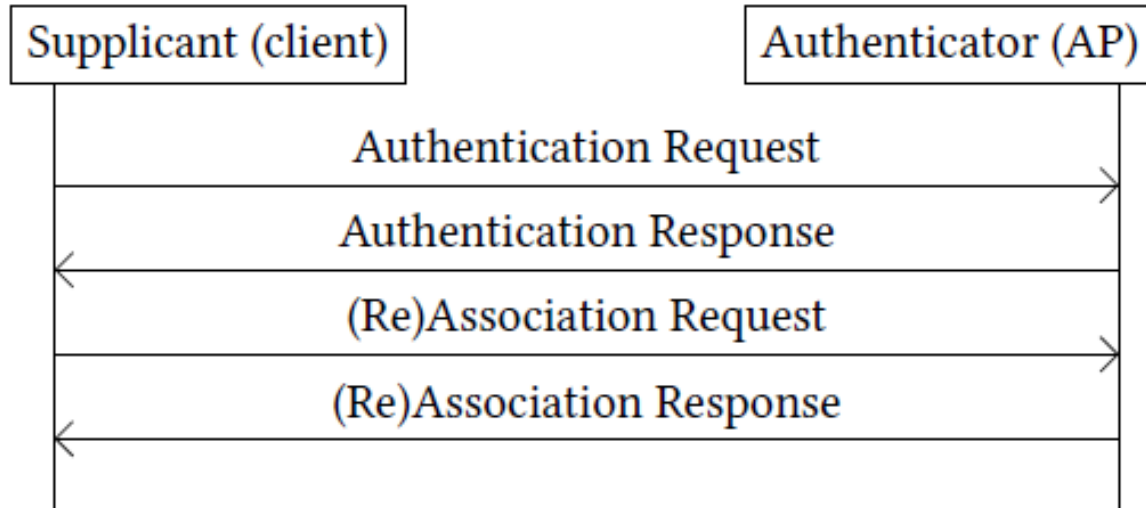
**GCMP** (Galios Counter Mode  
Protocol)

# 802.11i. Confidentiality and Integrity Protocols



\* The difference between WPA-CCMP and WPA-GCMP is that the second one also adds support for short-range communications in the 60 GHz band

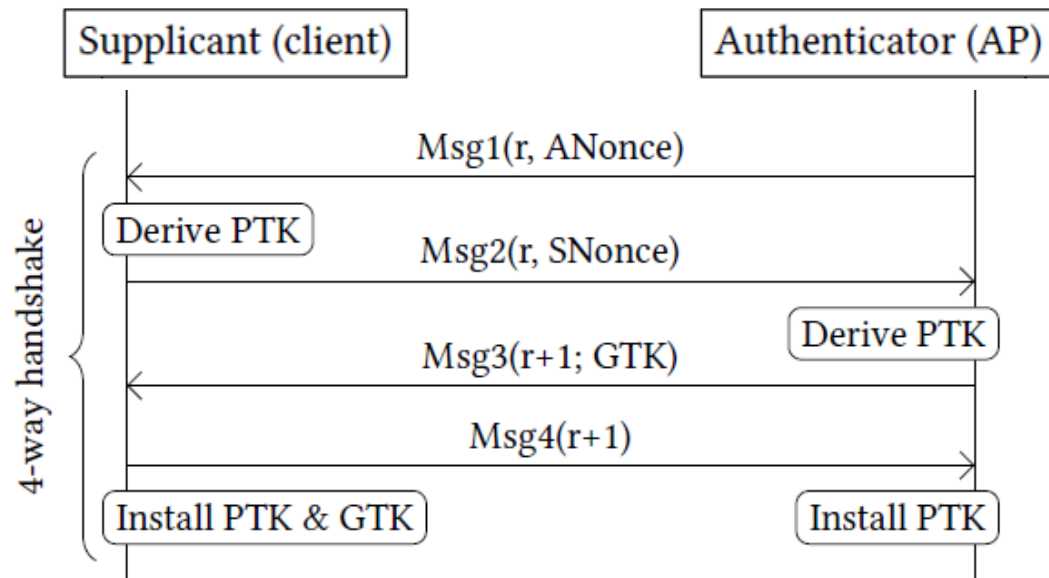
# 802.11i. Authentication



- Authenticating the client as valid and having permission to access the network
- Allows any client to authenticate
- After this step, the client associates with the network

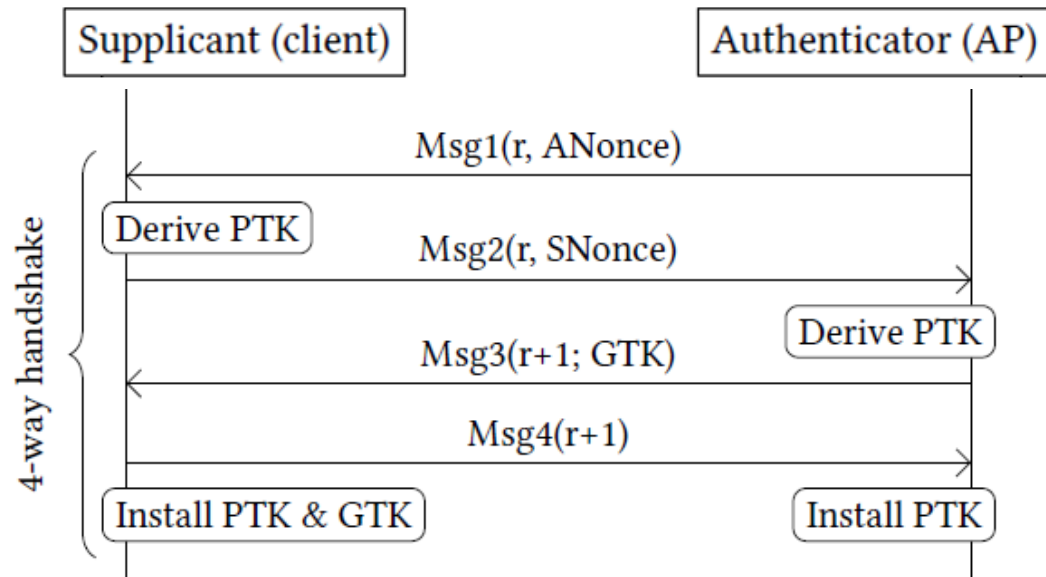


# 802.11i. 4-way Handshake



- At the starting state, no keys are known, the MIC cannot be computed
- **Msg1**: the authenticator uses this message only to send its value of ANonce to the supplicant
- **Msg2**: After successful delivery of the first message, the supplicant generates its own value of SNonce

# 802.11i. 4-way Handshake

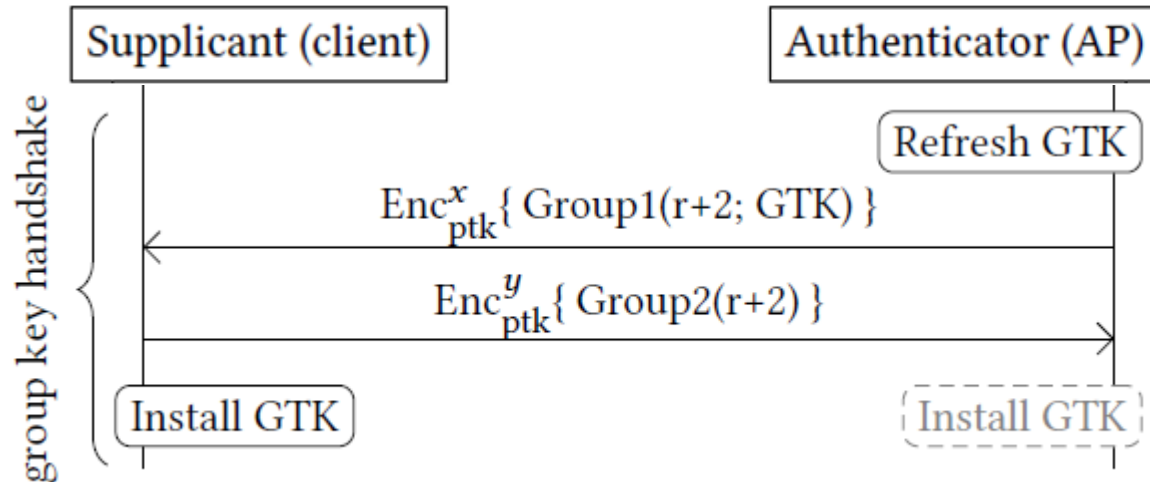


- **Msg3:**

- verifies to the supplicant that the authenticator knows the PMK and is thus a trusted party
- it tells the supplicant that the authenticator is ready to install and start using the data encryption keys
- it gives the supplicant the group key

- **Msg4:** verifies to the authenticator that the keys are about to be installed

# The Group Key Handshake



- Authenticator periodically refreshes GTK and initiates the handshake by sending the message to all clients in the group
- Depending on the implementation, GTK can be installed after sending message 1 or after receiving responses from all clients
- Since a PTK is installed, the complete EAPOL frame is protected using a data-confidentiality protocol



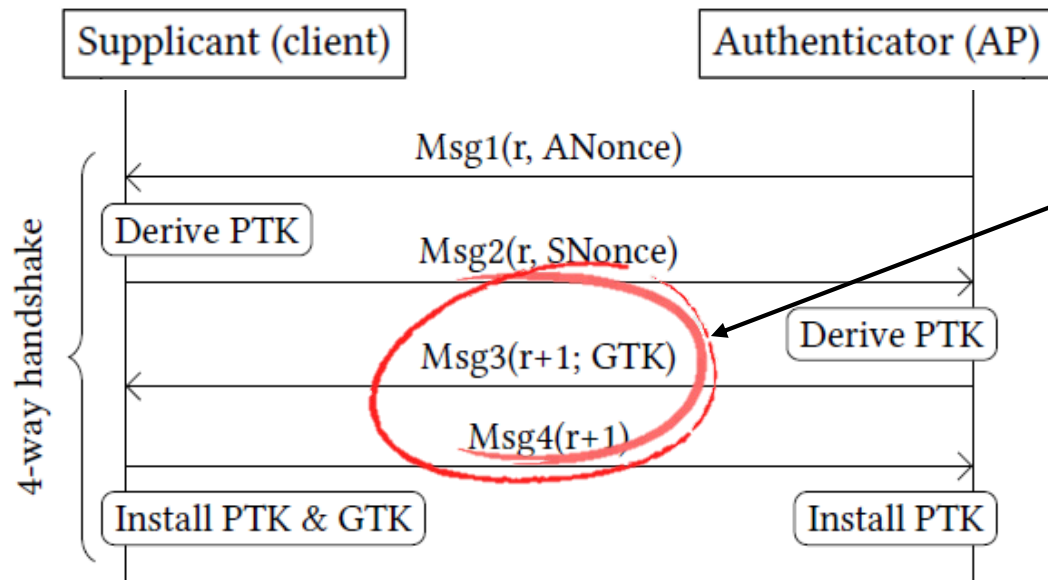
# Key Reinstallation Attacks

Breaking WPA2 by forcing nonce reuse



# Problem

## 4-way handshake



Can be retransmitted if the AP didn't receive a reply



# Why is it a critical moment?

**“If the Authenticator does not receive a reply to its messages, it shall attempt to transmit the message, plus a final timeout.”**

IEEE Std 802.11i. 2004. Amendment 6: Medium Access Control (MAC) Security Enhancements,

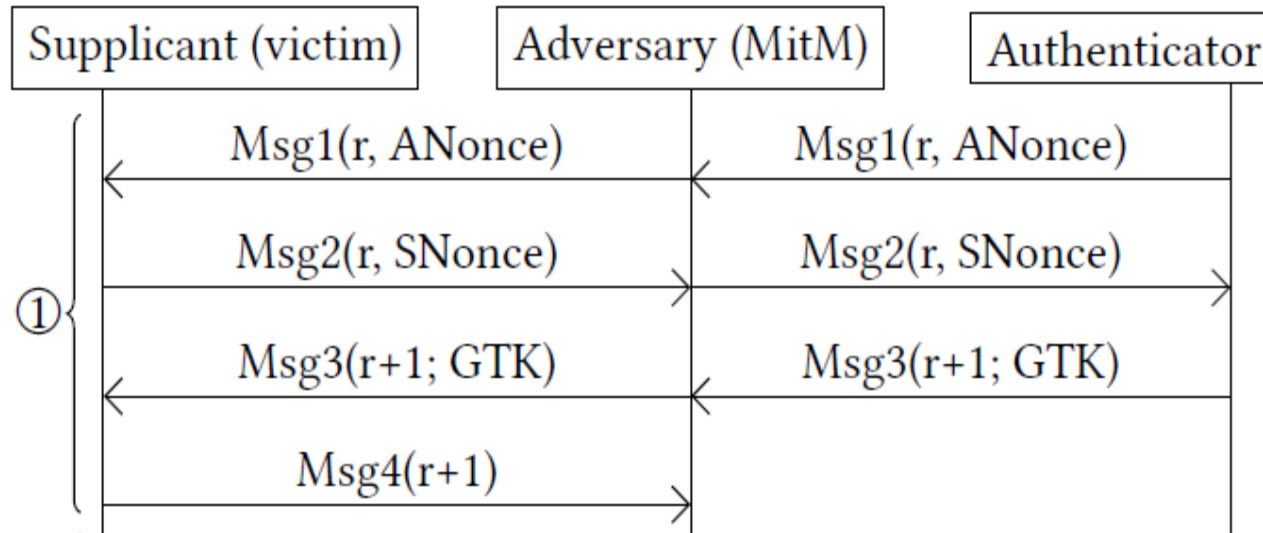
§ 8.5.3.5 4-Way Handshake implementation considerations

# Why is it a critical moment?

Retransmitting the message → PTK will be reinstalled → Nonce will be reused

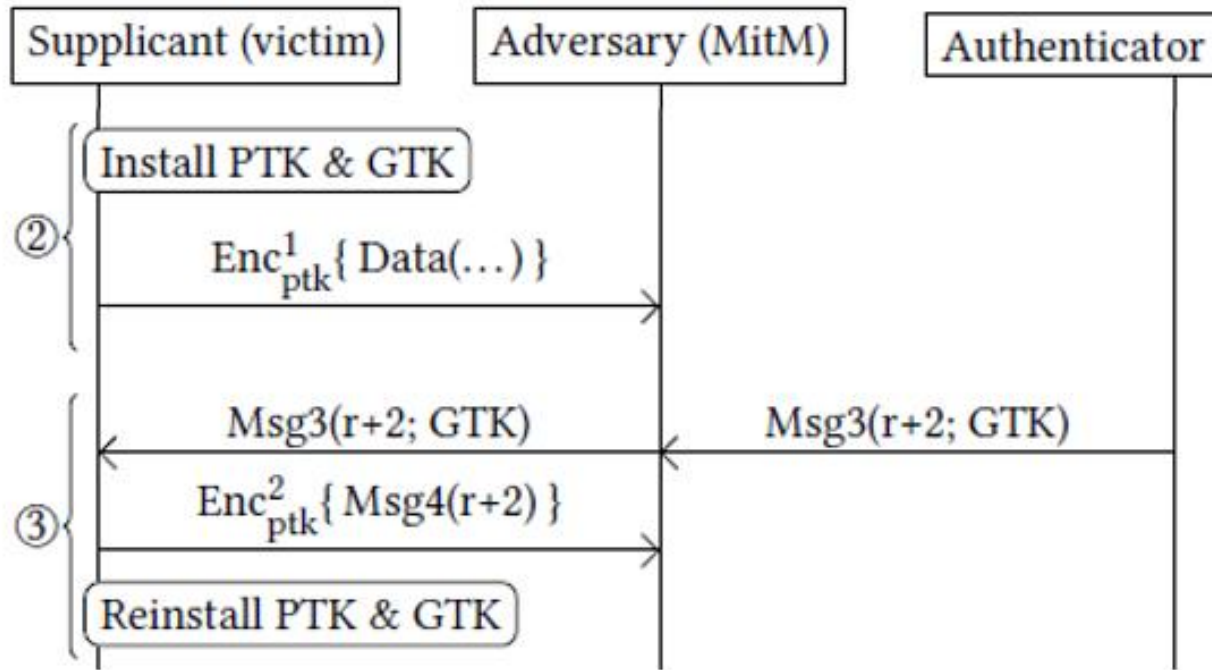
Due to the properties of the stream ciphers used in data-confidentiality protocols, reusing nonces leads to the ability of decryption

# Plaintext retransmission attack



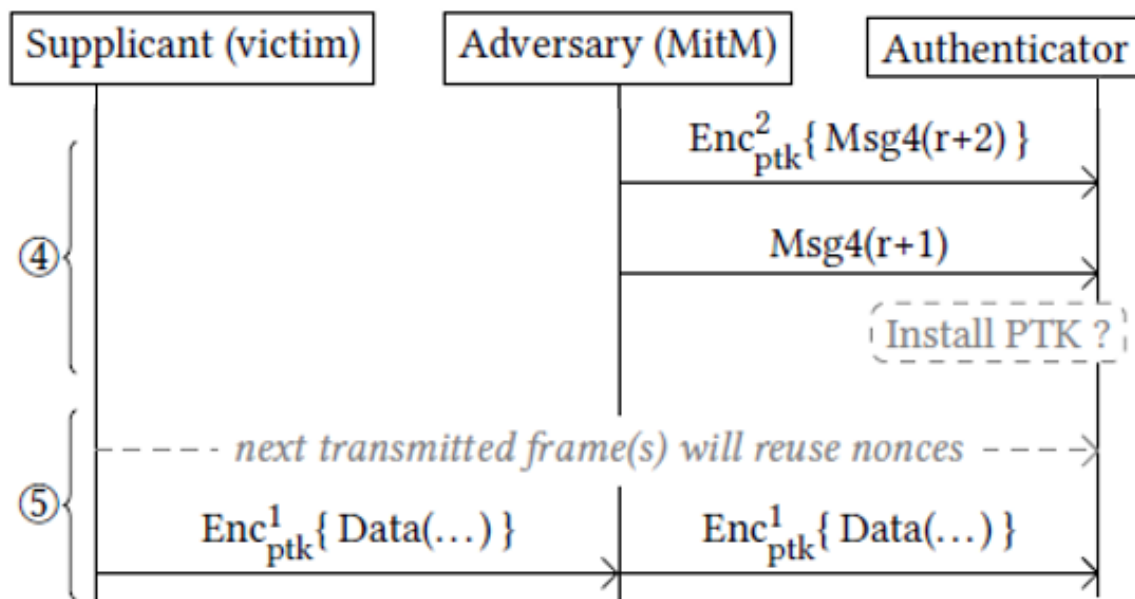
- Using Man-in-the-middle attack to manipulate messages
  - Blocking message 4 from arriving at the authenticator
- ↓
- The authenticator retransmits  $\text{Msg3}$  due to he didn't receive  $\text{Msg4}$

# Plaintext retransmission attack



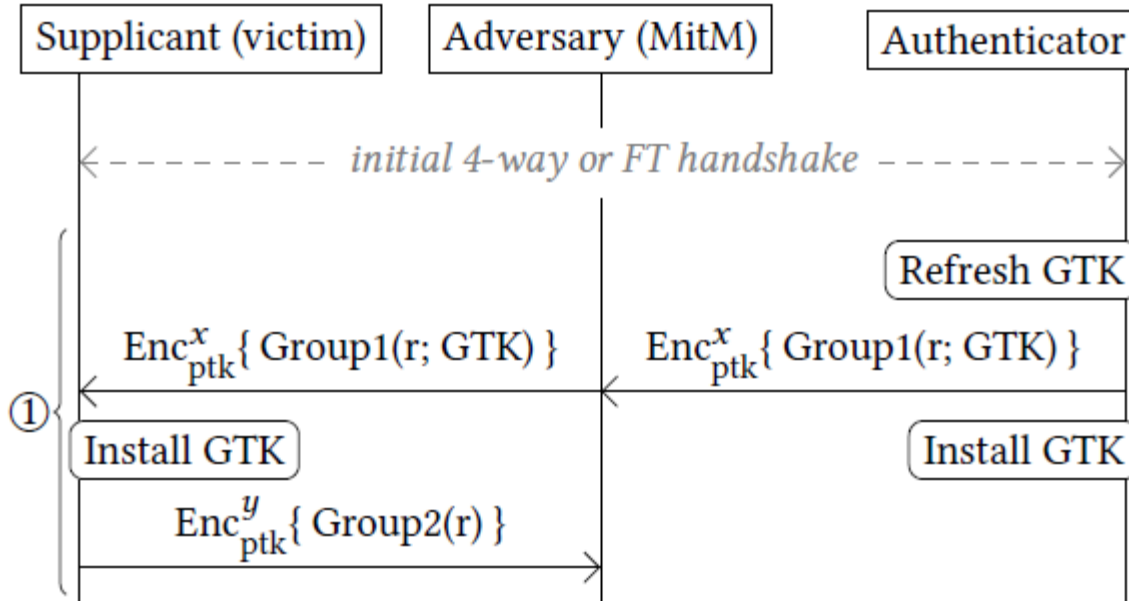
- Suppliant installs PTK & GTK
- Authenticator sends Msg3 again which the adversary doesn't block, and the suppliant reinstalls PTK & GTK
- As a result, it resets the nonce and replay counter used by the data-confidentiality protocol

# Plaintext retransmission attack



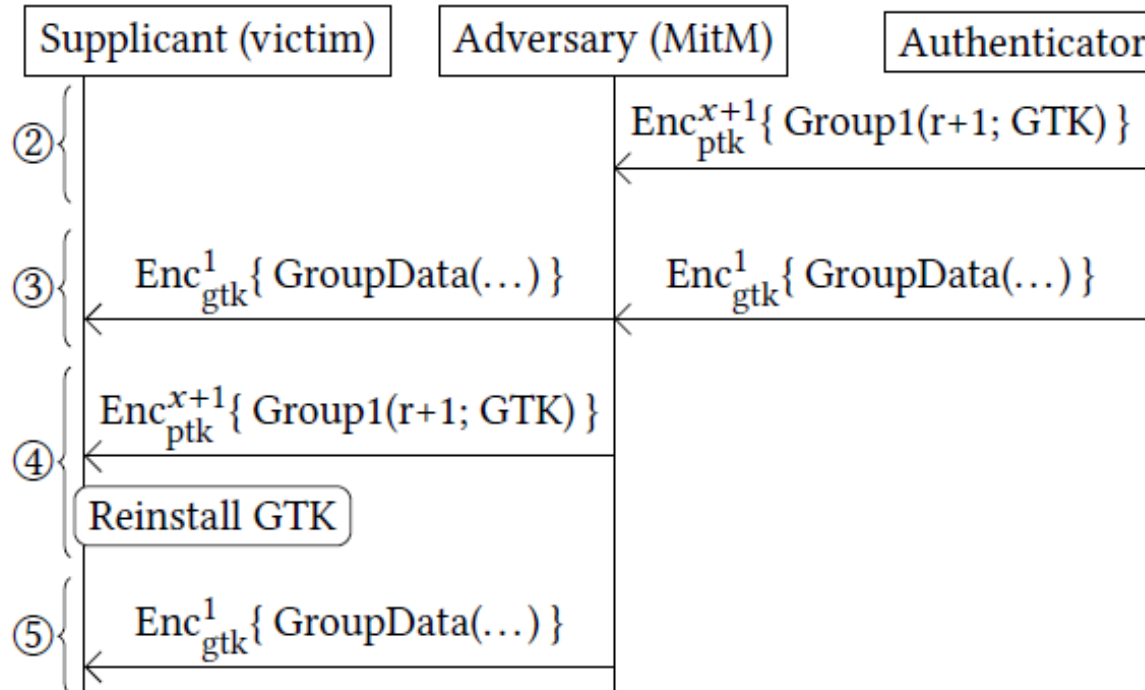
- Since the authenticator did not yet install the PTK, it will normally reject the encrypted  $\text{Msg4}$
- BUT the authenticator may accept any replay counter that was used in the 4-way handshake
- When the victim transmits its next data frame, the data-confidentiality protocol reuses nonces

# Group Key Handshake Break (Immediate Key installation)



- The adversary blocks the response (group Msg2) from arriving at the AP

# Group Key Handshake Break



- Authenticator retransmits a new group message 1
- Waiting until data frame is transmitted and forward a new group message to the supplicant



- The group key is reinstalled

# Other attacks

There are several attacks which depend on the using system and how the protocol 802.11i is implemented:

- Attacking 4-way handshake when the victim only accepts encrypted message 3 retransmission
- Attacking the Group Key Handshake with a delayed key installation



# Countermeasures

- Check if the new key has already been installed and avoid repetition of the replay counters
- Changing the data-confidentiality protocols

# References

- Key reinstallation attacks. <https://www.krackattacks.com/>
- I. W. Group et al. 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: Wireless access in vehicular environments. IEEE Std, 802(11), 2010.
- M. Vanhoef and F. Piessens. Key reinstallation attacks: Forcing nonce reuse in wpa2. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pages 1313–1328. ACM, 2017.

Q&A