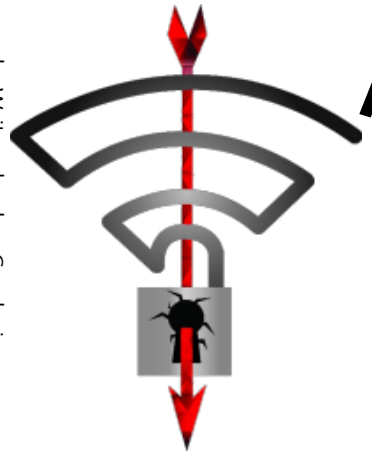
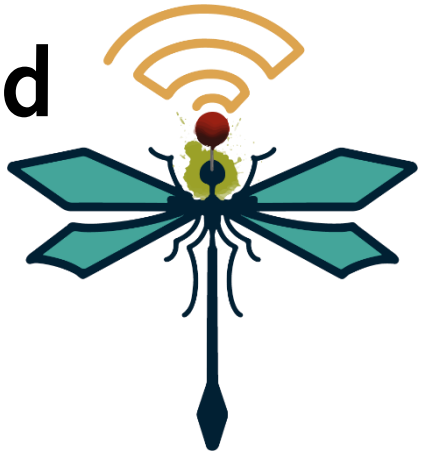
it.sec
security for your information

A handshake for vulnerabilities

-

A short dive into Krack and Dragonblood





it.sec GmbH

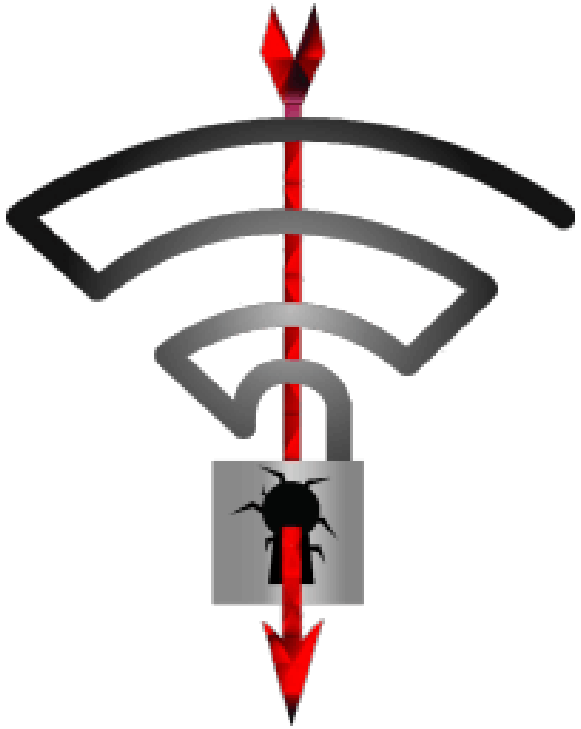
Who are we?

it.sec
security for your information

- Philip Madelmayer
  - Bachelor – IT Security – FH STP
  - Development/Pentesting
- Christoph Rottermanner
  - Bachelor – IT Security – FH STP
  - Master – Information Security – FH STP
  - Pentesting
  - @pycycle https://pycycle.info

KRACK

- **K**ey **R**einstall **A**tta**CK**
- Attacks 4-way-handshake

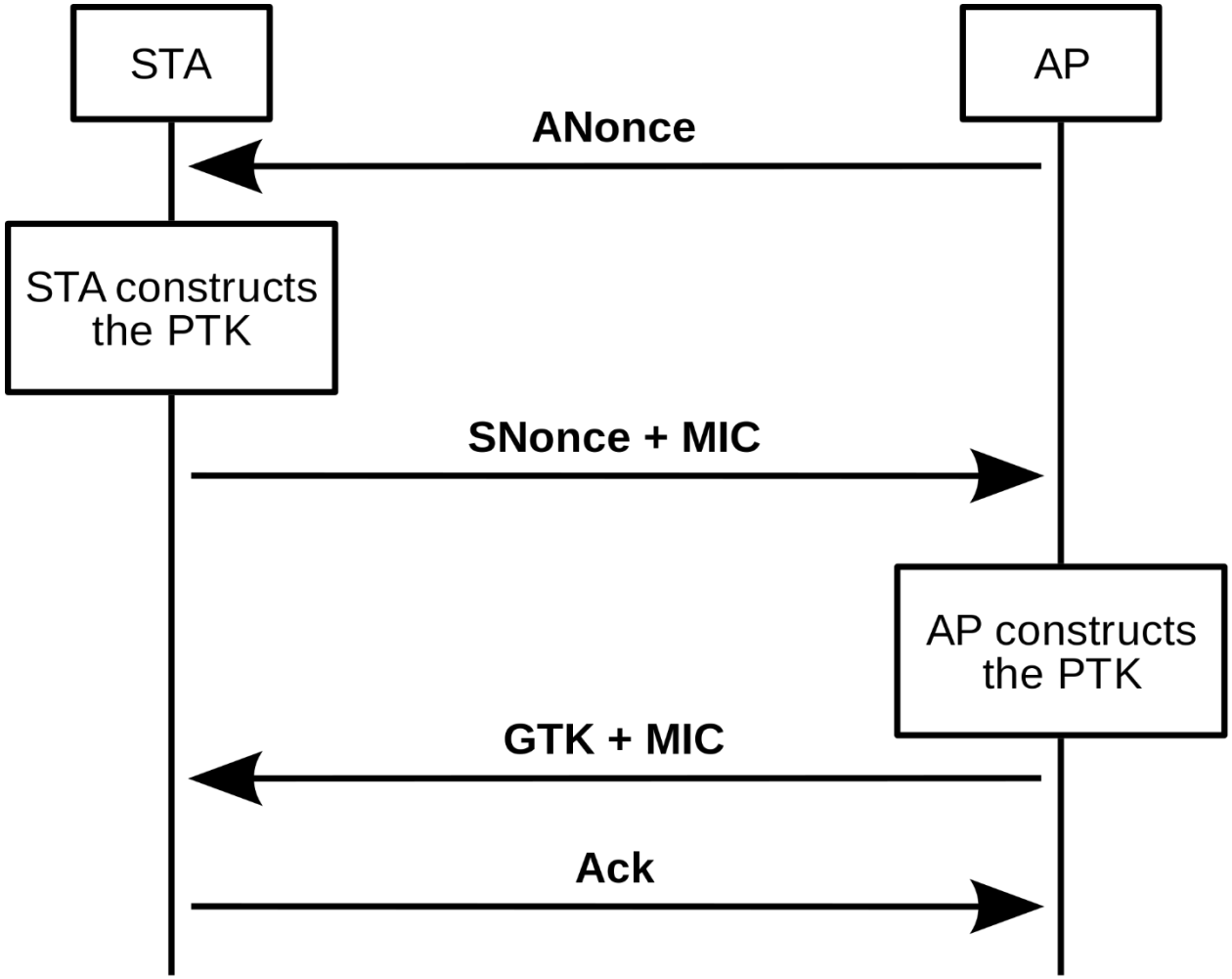


- https://www.krackattacks.com/

4-way-handshake WPA2

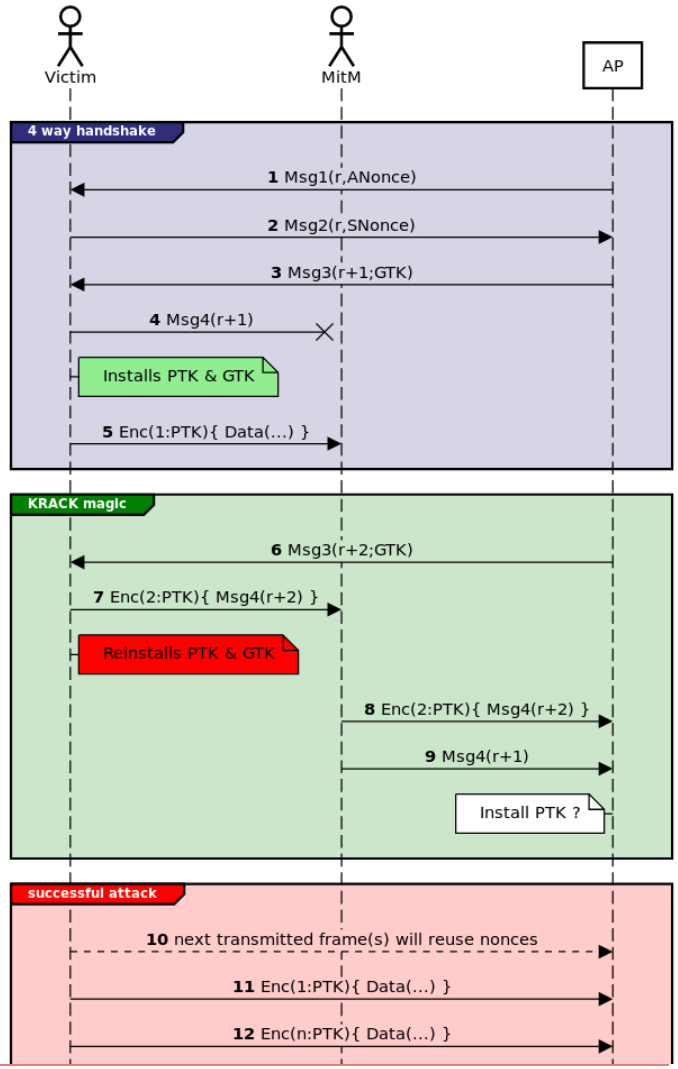
- Station ← Nonce-Token – AccessPoint
- Station – signed Nonce → AccessPoint
- Station ← signed key – AccessPoint
- Station – confirm key → AccessPoint

4-way-handshake WPA2



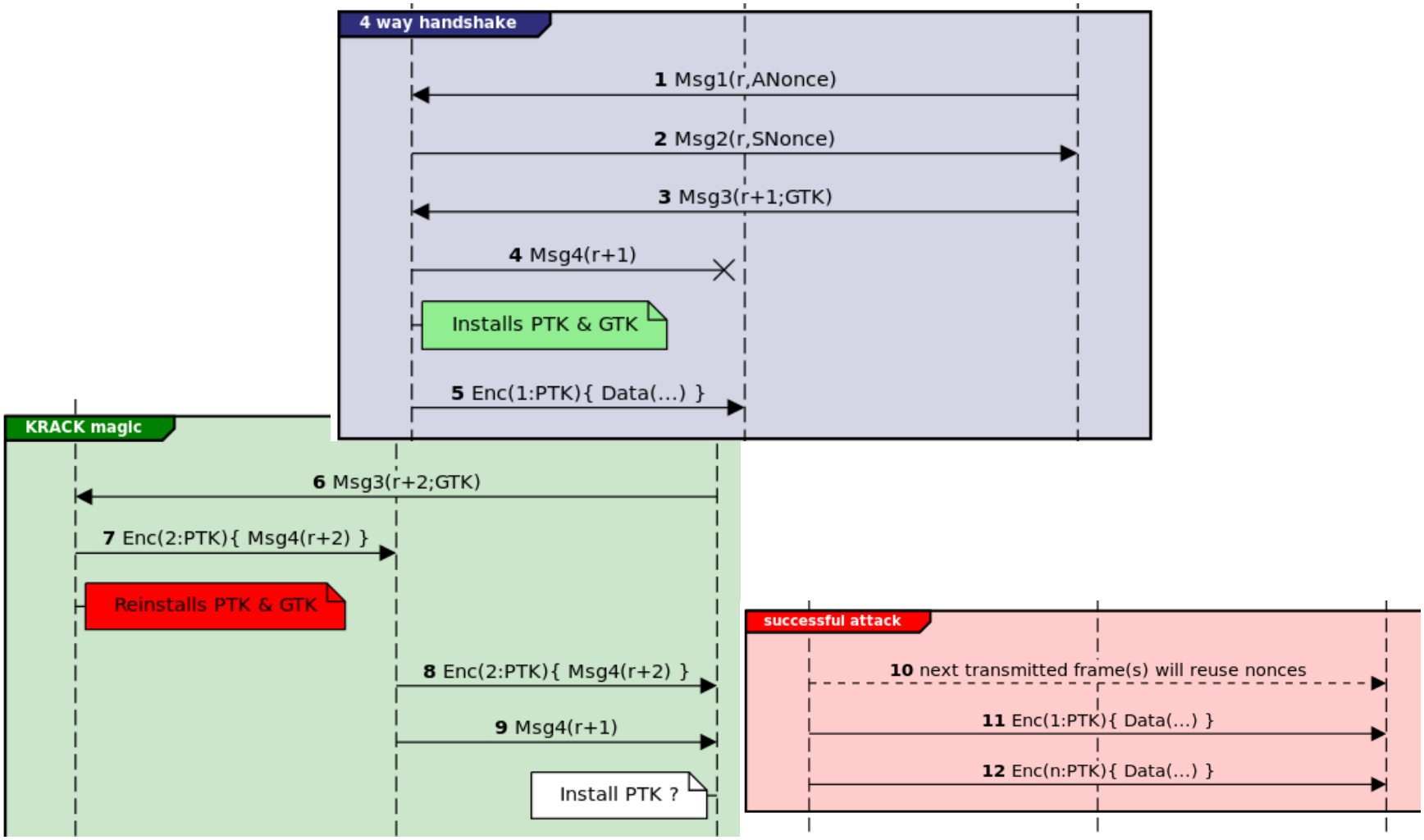
What happens?

- Blocks transmission of msg 4
  - → resends msg 3
- Enforces Nonce reuse
  - With the same encryption key
- Resets Nonce and Replay-Counter



4-way-handshake KRACK

it.sec
security for your information



Consequences

- Allows the adversary to … packages
  - Forward
  - Decrypt (same key)
  - Modify

Affected systems

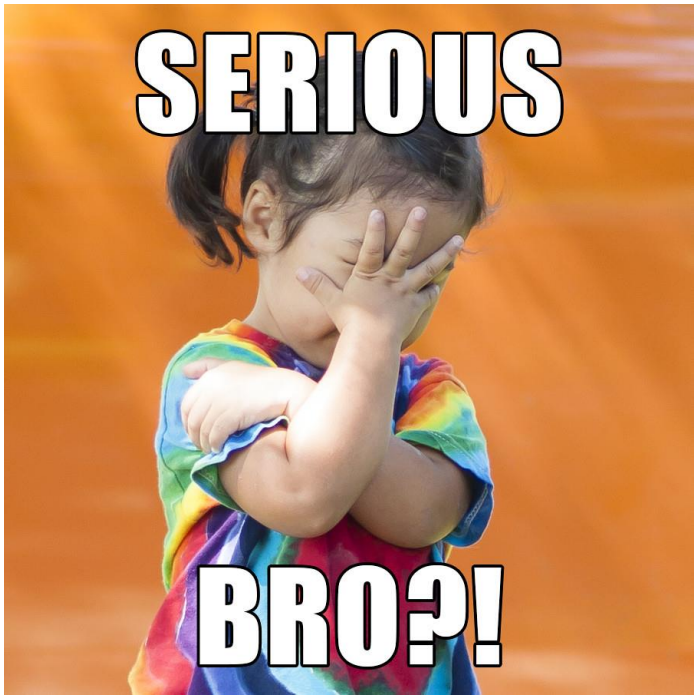
- Windows & Apple
  - Only Groupkey
  - No retransmission of msg 3
- Linux & Android
  - wpa_supplicant <= 2.6
- Router
  - 802.11r(Roaming)
  - WDS (Wireless Distribution System)

Linux and Android problem

- wpa_supplicant 2.4 - 2.6
- Msg 3 is received again
- Installs null-cipher-key
  - Removes old key and takes it afterwards

Fun fact: Broadcom-Router

- EAPOL-Frame from Client
- Request and Pairwise bits
  - Rekey without check



Countermeasure

- Check if key already in use
  - Was already implemented
    - Bypass with WNM-Sleep Frame
    - Installs new key → uses old key
- Only increase Replay-Counter
- Install key only once

Testing

- Krackattack scripts (Access to the Client)
- Krackattack POC (wpa_supplicant 2.4 - 2.6)
  - Demo
- Hostapd (manual guide)

- https://github.com/vanhoefm/krackattacks-scripts#testing-clients
- https://github.com/vanhoefm/krackattacks-poc-zerokey
- https://w1.fi/cgit/hostap/tree/tests/cipher-and-key-mgmt-testing.txt

DEMOTIME

it.sec
security for your information

Dragonblood – WPA3

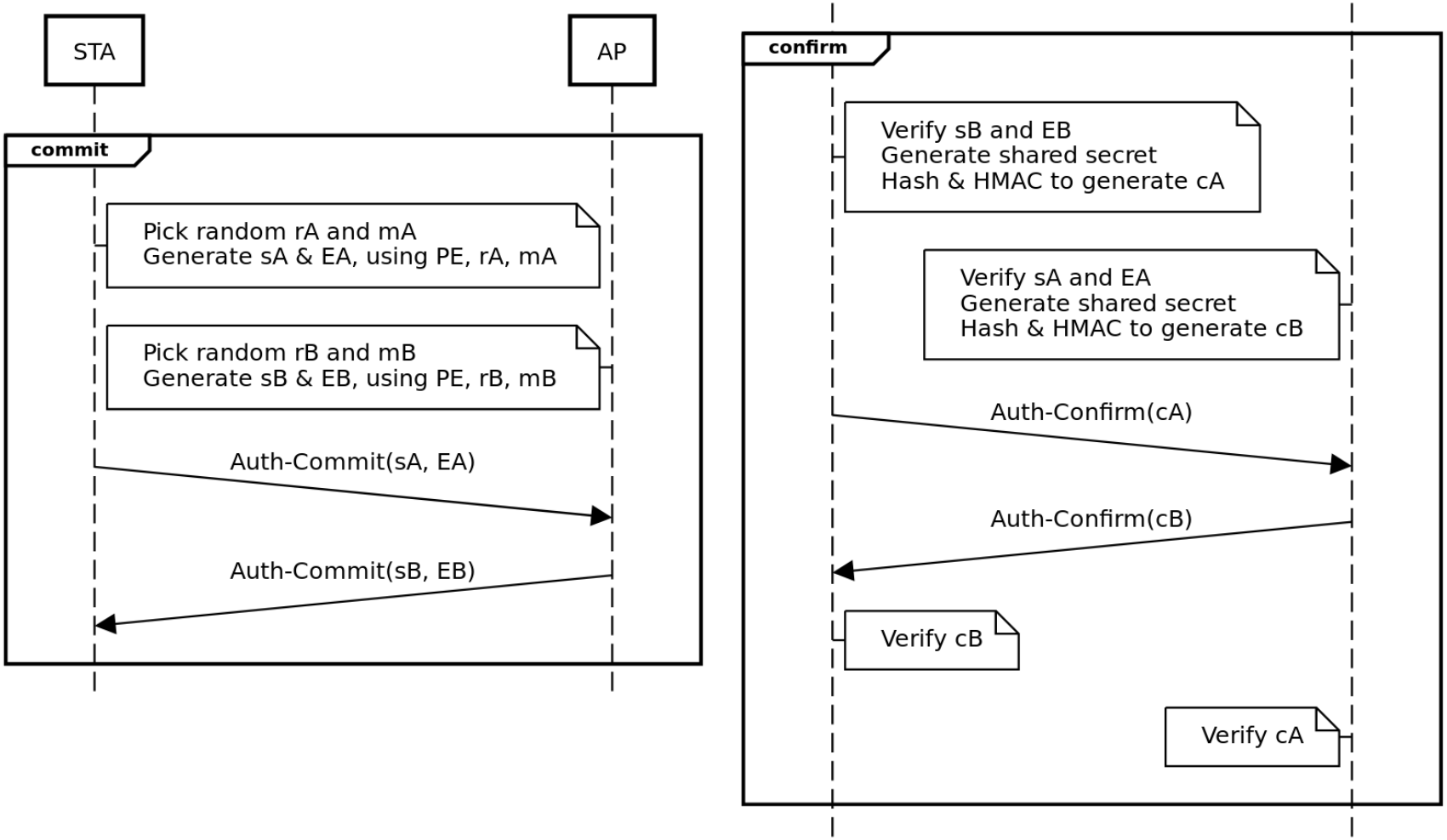
Changes in WPA3

- WPA3-Personal
  - Minimum encryption CCMP-128 (AES-128 in CCM mode)
- WPA3-Enterprise
  - Equivalent 192-bit cryptographic strength (AES-256 in GCM mode with SHA-384 as HMAC)
- Pre-Shared Key exchange replaced with SAE
  - Protection against offline brute-force attacks

Changes in WPA3

- Protection of management frames enforced
- Forward Secrecy
- Privacy on public Wi-Fi networks

Dragonfly handshake WPA3



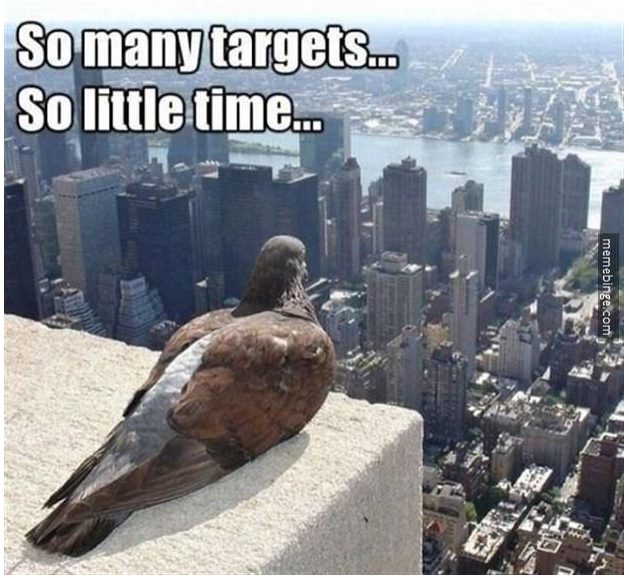
Dragonblood

- Authentication protocol Simultaneous Authentication of Equals (SAE), also known as Dragonfly
- Hash-to-element algorithms

- https://wpa3.mathyvanhoef.com/

Kind of attacks

- Downgrade & Dictionary Attack Against WPA3-Transition
- Security Group Downgrade Attack
- Denial-of-Service Attack
- Timing-Based Side-Channel Attack
- (Cache-Based Side-Channel Attack)
- (Invalid curve & reflection)

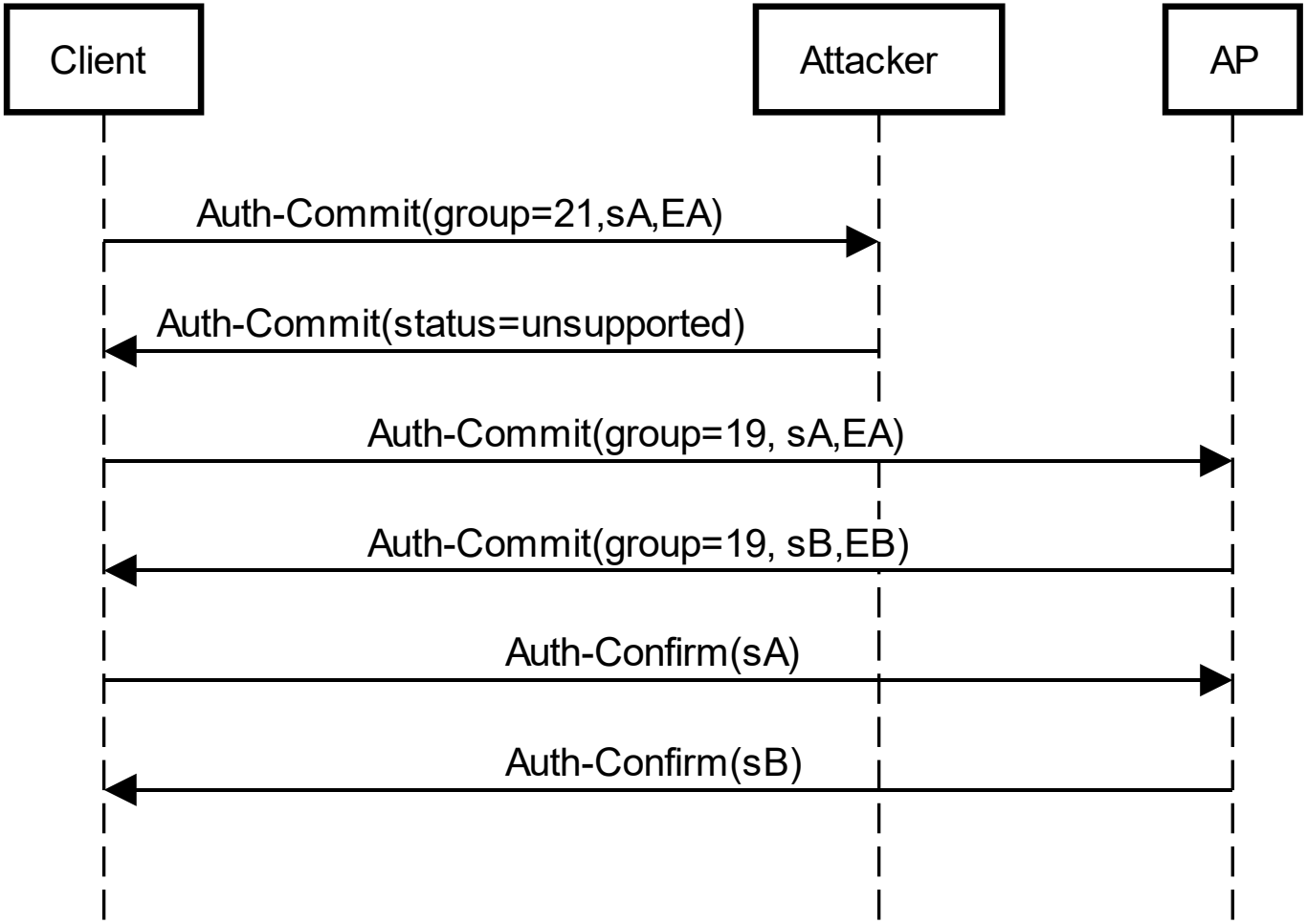


Attacking WPA3-Transition

it.sec
security for your information

- Verification of RSNE frame should prohibit downgrade attacks
- But ….
  - Forge the first message of the 4-way handshake
  - Victim transmits message 2 of the 4-way handshake, which is authenticated→ Profit
  - Client detects downgrade

Security Group Downgrade



DoS Attack

- Dragonfly handshake causes high load
- DoS prevention → secret cookies have to be reflected by the client
  - Secret cookie per MAC address
- Easy to spoof MAC address
- 70 commit exchanges/second (curve P-256) enough to overload AP by a Raspberry Pi B+

Hash-to-group

for counter in range(1, 256):

value = Hash(password, addr1, addr2, counter)

if value >= p: continue

$P = value^{(p-1)/q}$

return P

Time-based Attack

it.sec
security for your information

- Processing time for generating the password hash depends on the password
- Depends on used security group
- MAC address of client and AP used to build password hash

Time-based Attack

- Measure the time it takes for the AP to calculate the password element
- Perform offline calculation for several passwords on the client and also measure the time
- Compare the measurement results

Consequences

- Allows the adversary to
  - Recover the password
  - Steal sensitive information
    - Credit cards
    - Password
    - Emails

Affected … ?

- WPA3 devices
- Tested implementations
  - FreeRADIUS
  - Radiator
  - Aruba's EAP-pwd for Windows
  - iNet Wireless Daemon
  - Hostapd and wpa_supplicant

Countermeasure

- Password and MAC address shouldn't influence processing time of password hash
- Use only certain security groups
  - Approach of Microsoft is to support only cryptographic group 19

Testing

- Dragondrain / Dragontime
  - Denial-of-service attacks against SAE handshake.
  - Performs timing attacks against the SAE handshake.
- Dragonforce
  - Timing or cache-based attacks to perform a password partitioning attack.
- Dragonslayer
  - Performs invalid curve attacks against EAP-pwd

- https://github.com/vanhoefm/

Should we be concerned?

it.sec
security for your information

- KRACK
  - Need to be in physical range
  - Can not break HTTPs or VPN traffic

- Dragonblood
  - Physical range again
  - Not common yet
  - Hopefully patched before
  - Not trivial to exploit

Where it.sec is „hiding“ their Hackers?

it.sec
security for your information

Head Ulm/Donau	Branch Berlin
it.sec GmbH	it.sec GmbH
Einsteinstr. 55 89077 Ulm/Donau Deutschland	Reinhardtstr. 47 10117 Berlin Deutschland
Tel: +49 731 20 589-0 Fax: +49 731 20 589-29	Tel: +49 30 20 96 759-0 Fax: +49 30 20 96 759-29
info@it-sec.de www.it-sec.de	info@it-sec.de www.it-sec.de

Branch Wien	Branch St. Pölten
it.sec GmbH	it.sec GmbH
Gußhausstraße 22/4 1040 Wien Österreich	Heinrich-Schneidmadl-Str. 15 3100 St. Pölten Österreich
Tel: +43 1 37 50 247-0 Fax: +43 1 37 50 247-29	Tel: +43 1 37 50 247-0 Fax: +43 1 37 50 247-29
info@it-sec.de www.it-sec.de	info@it-sec.de www.it-sec.de