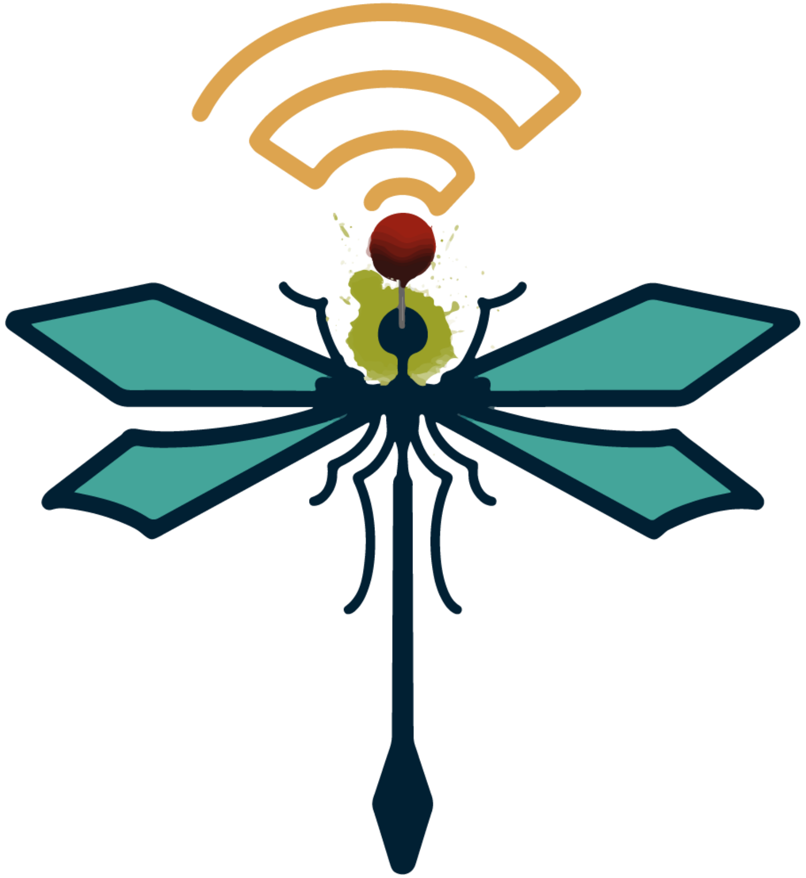
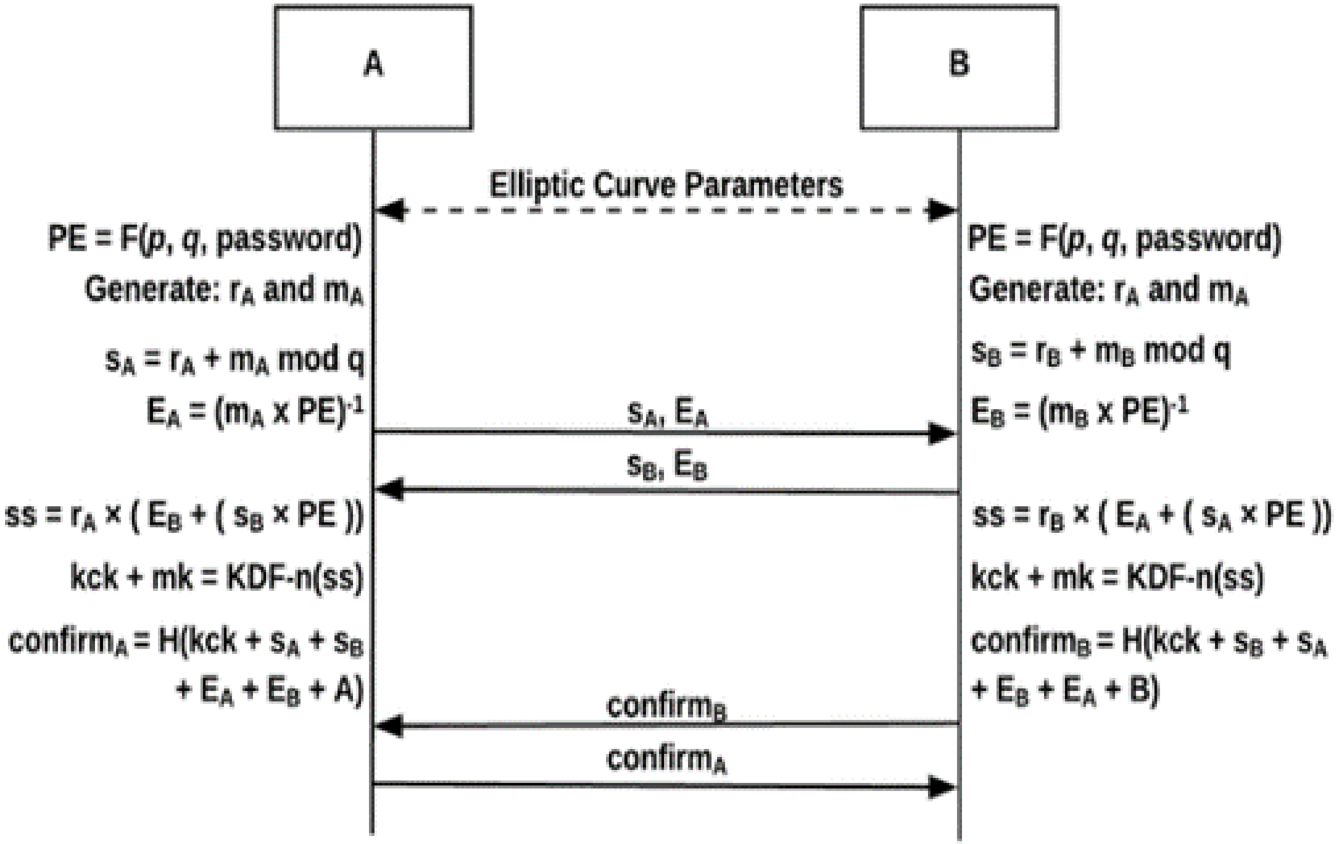
WPA3 - DragonBlood

- Killian MARTY
- Aurélien POUILLES
- Baptiste REBILLARD
- Leandro RODRIGUEZ



How does WPA3 works ?


A
B
Elliptic Curve Parameters
$PE = F(p, q, \text{password})$
Generate: r_A and m_A
$s_A = r_A + m_A \bmod q$
$E_A = (m_A \times PE)^{-1}$
$PE = F(p, q, \text{password})$
Generate: r_A and m_A
$s_B = r_B + m_B \bmod q$
$E_B = (m_B \times PE)^{-1}$
s_A, E_A
s_B, E_B
$ss = r_A \times (E_B + (s_B \times PE))$
$ss = r_B \times (E_A + (s_A \times PE))$
$kck + mk = KDF\text{-}n(ss)$
$kck + mk = KDF\text{-}n(ss)$
$confirm_A = H(kck + s_A + s_B + E_A + E_B + A)$
$confirm_B = H(kck + s_B + s_A + E_B + E_A + B)$
$confirm_B$
$confirm_A$

Dragonfly (SAE)

Simultaneous Authentication of Equals

Resistant to offline attacks, as WPA3's handshake uses fresh random values each time.

Preventing password guessing without real-time interaction.

Also introduces :

- Forward Secrecy
- FMP (Frame Management Protection)
- Stronger encryption

DragonBlood

Mathy Vanhoef and Eyal Ronen, 2019

1. Timing attack
2. Cache attack
3. Downgrade attack

Timing attack

Exploits **timing** differences in **SAE**’s *hash-to-group* to partition the password candidate space and accelerate guessing.

The method to retrieve a password is :

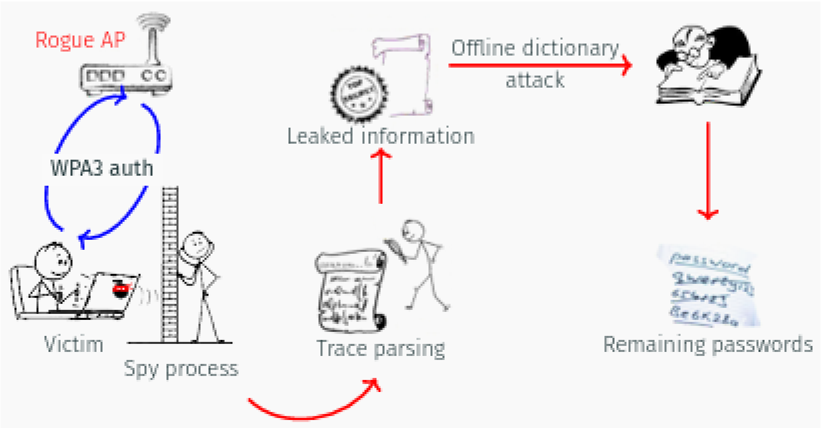
- Trigger or observe SAE commit and **measure response time**.
- Assign each timing observation to a group corresponding to the **iteration count.**
- Keep candidates whose simulated timing matches the group, discard incompatible groups.
- Repeat until the candidate set is small enough for cracking.

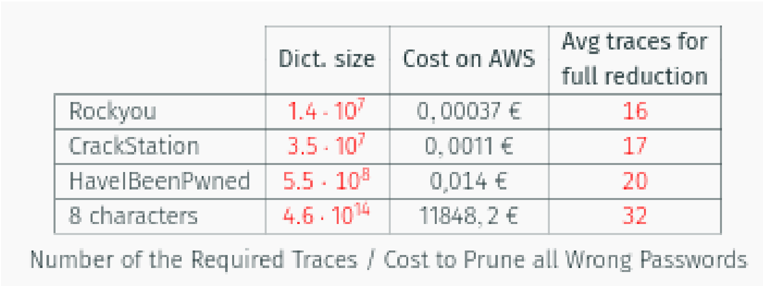
Cache attack

WPA3 use the Dragonfly handshake to **derive keys** from the password.

This process can leak information through CPU cache behavior:

- Secret-dependent operations cause different **cache access time**.
- An attacker observe the **cache** access delays (ex: local browser/JS)
- The attacker can then **infer partial information** about the password and **reduce** the search space.
- **Crack the password** faster.





	Dict. size	Cost on AWS	Avg traces for full reduction
Rockyou	$1.4 \cdot 10^7$	0, 00037 €	16
CrackStation	$3.5 \cdot 10^7$	0, 0011 €	17
HaveIBeenPwned	$5.5 \cdot 10^8$	0,014 €	20
8 characters	$4.6 \cdot 10^{14}$	11848, 2 €	32

Number of the Required Traces / Cost to Prune all Wrong Passwords

Source : https://people.irisa.fr/Mohamed.Sabt/assets/publications/2020_acsac_dragonblood_still_leaking_slides.pdf

Downgrade attack

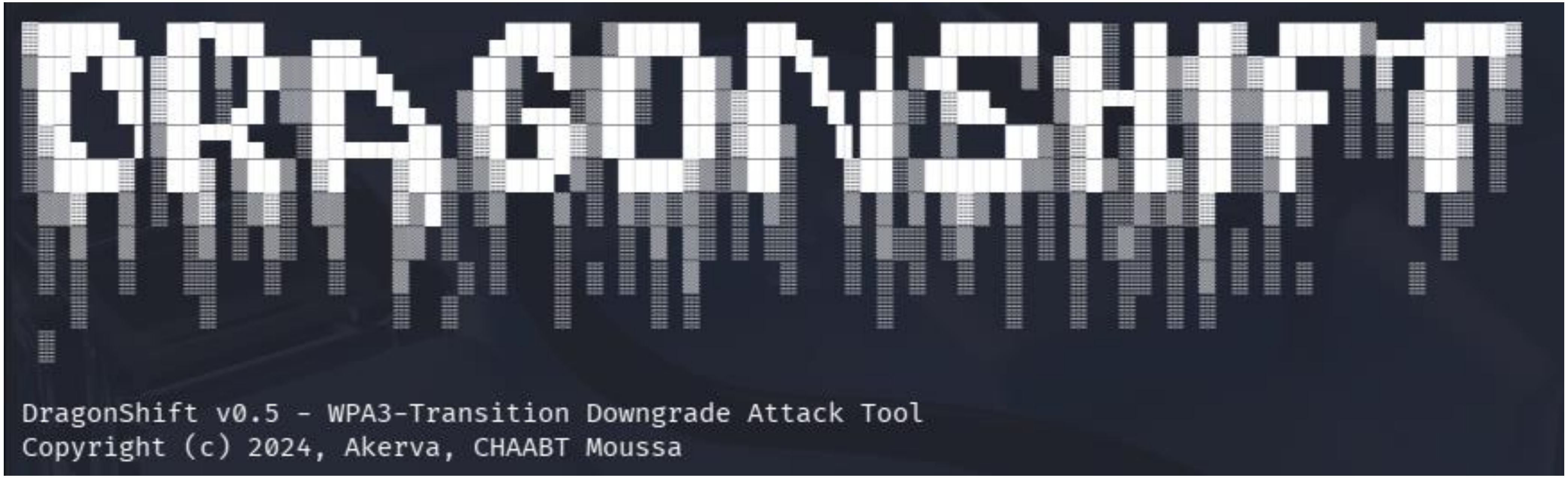
Some access points are in **WPA2/WPA3** transition mode to allow not WPA3 compatible devices to use the access point.

It causes a **downgrade** vulnerability:

- Create a fake AP using same SSID in WPA2.
- Send DeAuth messages to target client.
- The client could connect to the rogue AP and we can collect the WPA2 4-way handshake.
- Crack the password offline.

Note: FMP need to be disabled.

Demo



```
DragonShift v0.5 - WPA3-Transition Downgrade Attack Tool
Copyright (c) 2024, Akerva, CHAABT Moussa
```