WPA3

Network Security - Lecture 5

Ruxandra F. Olimid

Faculty of Mathematics and Computer Science, University of Bucharest

Outline

- SAE
- Dragonfly Handshake
- Attacks / Vulnerabilities

Changes

- Introduces Simultaneous Authentication of Equals (SAE) to replace the pre-shared key exchange
- SAE is a variant of the Dragonfly Handshake
- Enterprise: must offer at least 192 bits of security (e.g., 384-bit EC)
- Enforces 802.11w – security of management frames (e.g., radio management, QoS)

The Dragonfly Handshake

- Is a Password Authenticated Key Exchange (PAKE)
- Starts with a password and generates a higher entropy key
- Supports Elliptic Curve Cryptography (ECC)
- Has 2 phases:
  - *Commit*
  - *Confirm*

WPA3 – SAE Handshake

[Source: Vanhoef, M. and Ronen, E., 2020, May. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 517-533). IEEE.]

P: Password
k: the final / negotiated key

(k is further used in the 4WH, as in WPA2; i.e. *k* is like the PMK)

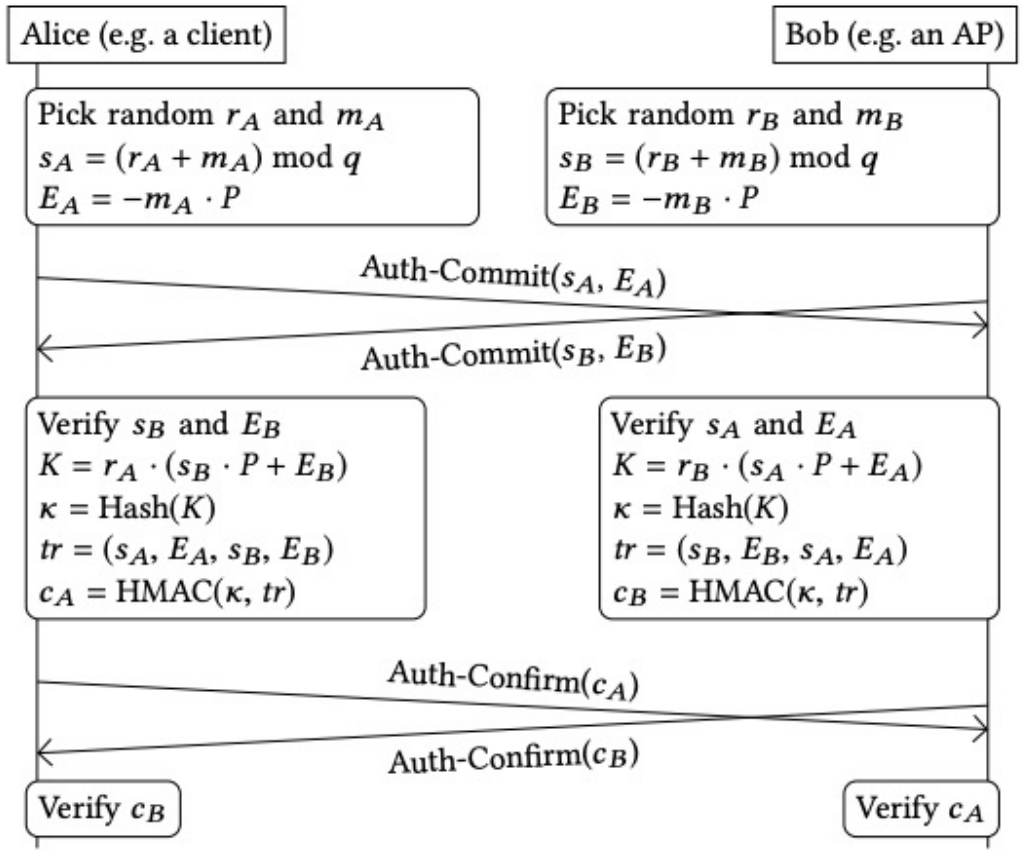

Figure 1: WPA3's SAE handshake. Both stations can simultaneously initiate the handshake, hence the crossed arrows. We assume elliptic curves are used, though similar operations are performed when using multiplicative groups.

WPA3 – Security against a dictionary attack

[Source: Vanhoef, M. and Ronen, E., 2020, May. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 517-533). IEEE.]

P: Password
k: the final / negotiated key

Remember: WPA2 was vulnerable to a dictionary attack by capturing a handshake.
WPA3 offers protection, why?

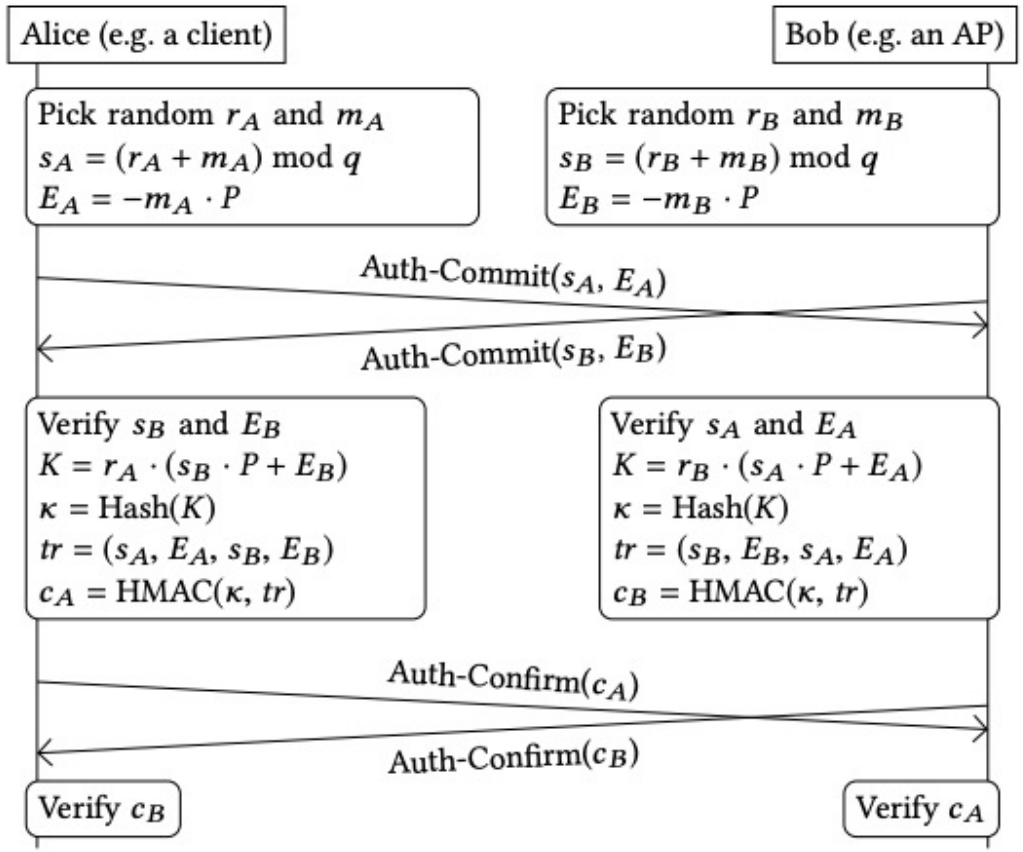

Figure 1: WPA3's SAE handshake. Both stations can simultaneously initiate the handshake, hence the crossed arrows. We assume elliptic curves are used, though similar operations are performed when using multiplicative groups.

Backward compatibility

- Scenario: both WPA2 and WPA3 are supported, and the same password is used
- WPA3 has some detection of downgrade to WPA2 (at changing the AP capabilities in the RSN IE), but this does not help (until detection, a handshake capture already makes the password vulnerable to a dictionary attack in WPA2).

[Source: Vanhoef, M. and Ronen, E., 2020, May. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 517-533). IEEE.]

Other problems

- DoS: spoof commit frames to the AP (the AP will have to do too many verifications)
- Timing attacks, side-channels attacks (mostly caused by how the pre-shared password is encoded into a group element in the Dragonfly handshake)

[Source: Vanhoef, M. and Ronen, E., 2020, May. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 517-533). IEEE.]

Dragonblood (2020)

DRAGONBLOOD

Analysing WPA3's Dragonfly Handshake

By Mathy Vanhoef (NYUAD) and Eyal Ronen (Tel Aviv University & KU Leuven)

INTRO NEW DETAILS PAPER TOOLS Q&A

INTRODUCTION

April 2019 — Modern Wi-Fi networks use WPA2 to protect transmitted data. However, because WPA2 is more than 14 years old, the Wi-Fi Alliance recently announced the new and more secure WPA3 protocol. One of the supposed advantages of WPA3 is that, thanks to its underlying Dragonfly handshake, it's near impossible to crack the password of a network. Unfortunately, we found that **even with WPA3, an attacker within range of a victim can still recover the password**. If the victim uses no extra protection such as HTTPS, this allows an attacker to steal sensitive information such as passwords and emails. We hope our disclosure motivates vendors to mitigate our attacks before WPA3 becomes widespread.

https://wpa3.mathyvanhoef.com/

WiFi Networks

- We have now finished studying WiFi security