Securing home Wi-Fi with WPA3 personal

Raoul Dijksman and Erik Lamers

Securing home Wi-Fi with WPA3 personal

Making Wi-Fi great again

With security this time, right?

Why is WPA3 needed?

WPA2 has been broken for many years. There are plenty of easy to use tools and techniques out there to crack and manipulate WPA2.

Think about:

- Aircrack-ng
- KRACK
- RSN-PMKID attack
- And more…

What does WPA3 bring?

WPA3 tries to fix most of the attacks previously mentioned. It does this by improving the way that the PMK is generated for the EAPOL 4 way handshake.

WPA3 personal add the Simultaneous Authentication of Equals before the 4 way handshake. This key exchange ensures a temporary PMK is generated for each authentication.

WPA3 mandates the use of 802.11w Protected Management Frames.

Simultaneous Authentication of Equals (SAE)

- Based on the Dragonfly handshake and (re)defined in 802.11-2016
- Encapsulated in the 802.11 authentication packets
- Two stages; Commit and Confirm
- Both parties can initiate the handshake
- Successful completion results in the generation of a PMK for that authentication

WPA3 modes of operation

WPA3 Personal

- WPA3 only
  - WPA3-SAE authentication
- WPA3 transition mode (WPA3-TM)
  - WPA3-SAE / WPA2-PSK authentication

WPA3 Enterprise

- Out of scope

Why do we need WPA3 transition mode?

- Current devices will stick around
- Many devices won't receive updates
- For example IoT devices
- WPA2 adoption took almost a decade to reach 70% adoption [1]
- "With regards to security: nothing good ever comes out of transition modes (ever)." [2]

Related work

- Christopher Kohlios and Thaier Hayajneh (2018), first security review of WPA3
- Mathy Vanhoef and Eyal Ronen (2019), Dragonblood. Found the first vulnerabilities in WPA3
- Wi-Fi Alliance - WPA3 Security Considerations (2019)

How can WPA3 personal transition mode be secured in such a way that downgrade attacks are not feasible?

Research Questions

How can WPA3 personal transition mode be secured in such a way that downgrade attacks are not feasible?

- What are the requirements for WPA3?
- How can WPA3 personal transition mode be manipulated in downgrading stations to WPA2?
- What techniques can be utilised to prevent these downgrade attacks?

Methods

Four experiments

Access Points

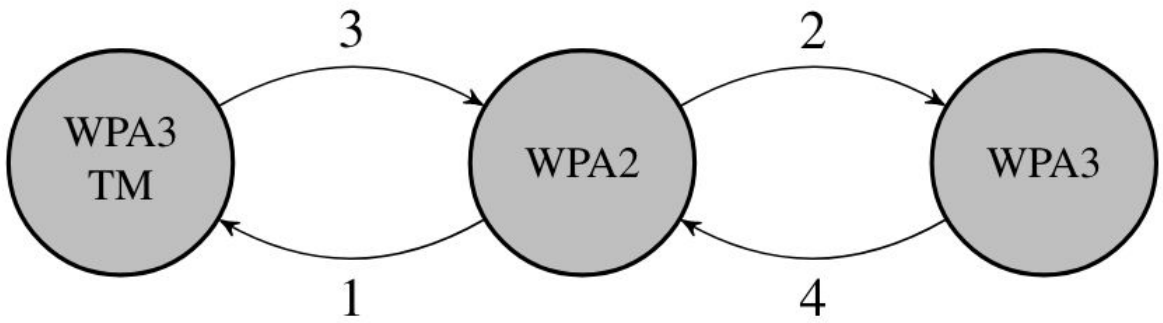
- AP vendor A
- AP vendor B

Stations

- Android on Samsung Galaxy S10
- iOS on Apple iPhone X
- MacOS on Apple Macbook
- Windows 10
- NetworkManager on Fedora 32

Station auto-connect - Methods

- Setup an AP to a specific Authentication Key Management (AKM)
- Connect station, without prior knowledge, to AP
- Alter AKM on AP
- Auto-connect behaviour from station is observed
- Repeated for every station and alternating the AKM



Station auto-connect - Results

Device	WPA2 -> WPA3-TM	WPA2 -> WPA3	WPA3-TM -> WPA2	WPA3 -> WPA2
Android 10 (S10)	Yes	No	Partial	No
iOS	Yes	No	Yes	No
macOS	Yes	No	Yes	No
Windows 10	WPA2	No	No	No
NetworkManager	WPA2	No	No	No

Station BSS selection - Methods

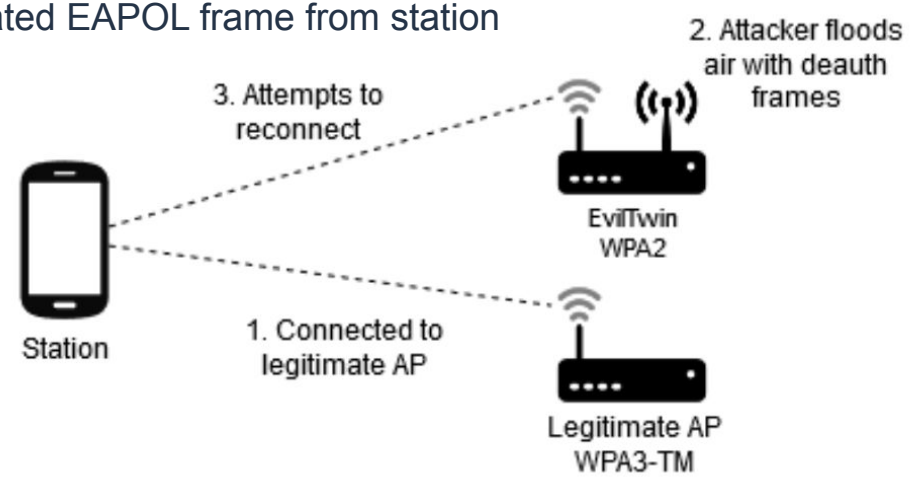
- Setup AP with two BSSIDs with identical SSID
- First BSSID is setup for WPA2
- Second BSSID is setup for WPA3
- Command station to connect to the SSID
- Observe the selected BSSID
- Repeat for every station

Station BSS selection - Results

Device	BSSID Selected
Android 10 (S10)	Displayed two selections
iOS	Random
macOS	WPA3
Windows 10	WPA3
NetworkManager	Random

Downgrade attack - Methods

- Setup legitimate AP
- Connect station to legitimate AP
- Start EvilTwin with WPA2
- EvilTwin floods air with deauth frames
- Monitor EvilTwin for first authenticated EAPOL frame from station



Downgrade attack - Results

Device	WPA2 deauth	WPA3-TM -> WPA2	WPA3 -> WPA2
Android 10 (S10)	Yes	Partial	No
iOS	Yes	Yes	No
macOS	Yes	Partial	No
Windows 10	Yes	No	No
NetworkManager	Yes	No	No

AP DoS - Methods

Flood the AP with forged SAE handshakes to create a Denial of Service for connected stations

- SAE handshakes a computationally expensive
- Both parties can initiate the handshake, each SAE commit message is evaluated by the AP
- DoS should be prevented by the SAE anti clogging mechanism

We used the Dragondrain tool to create up to 200 forged SAE handshakes per second

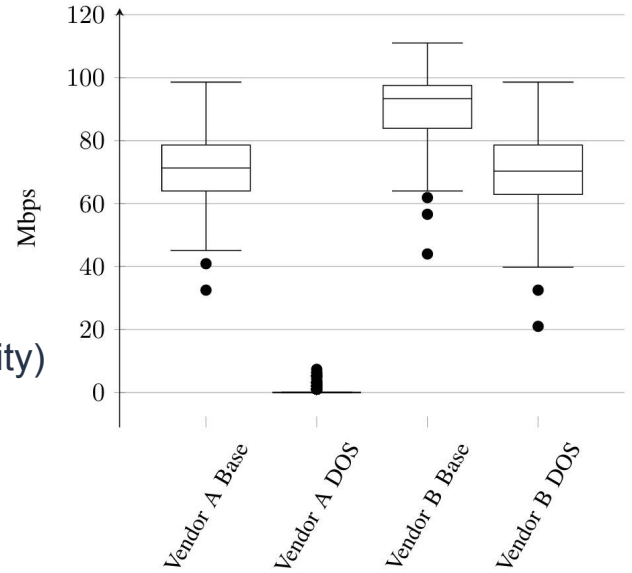
AP DoS - Results

AP vendor A

- Primary functions affected (connectivity)
- Session drops
- Single station downlink throughput close to zero

AP vendor B

- No loss of primary functions (authentication, connectivity)
- Single station downlink throughput decrease of 35%



Producing mutual trust

Current

- Station to AP authentication

Desired

- Mutual authentication

Solution

- SAE Public Key
- Verified SSIDs

SAE Public Key

- Brand new addition to the WPA3 specification (not approved yet)
- Adds a static public and private key pair to the ESS
- Wi-Fi password is a base32 hash of the ESS public key
  - Acts as a fingerprint
  - Trust bootstrap
- AP sends a SAE-PK element to the station in the SAE confirm message, this frame includes
  - ESS public key
  - Signature
- Station can verify the public using the fingerprint encoded in the Wi-Fi password
- Station can verify the signature using the public key

Transition Disable indicator

- Another addition in the WPA3 specification draft
- Enables a AP to signal to a station which AKMs to use and which to disable
- Only allows the use of WPA3 and up
    - Automatically disable of WEP and TKIP
- Standardizes the way stations remember which AKM to use for known networks
- Should be used in combination with SAE-PK to prevent TOFU

Wi-Fi URI

- Standardizes the way Wi-Fi authentication information can be encoded into a URI
- Can be used to represent Wi-Fi network information into a QR code
- Allows for the full SAE-PK public key to be encoded
- Allows the Transition Disable indicator to be encoded

Verified SSIDs

- Current SSID scheme can be chosen at will and are not unique
- FQDNs SSIDs can make SSIDs unique enough for identification
- In combination with CA signed certificates
    - AP includes a trusted certificate, which corresponds to the FQDN SSID, to each authentication
    - Proving to that station that the AP belongs to that domain

Discussion

- Secure implementations versus user-friendliness
  - Removing freedom to choose password in SAE-PK
  - Removing freedom to choose SSID in Verified SSIDs
  - Splitting Wi-Fi network into a WPA2 and WPA3 on single LAN
    - Unclear to user
    - Network still susceptible to WPA2 attacks
  - Splitting Wi-Fi network into a WPA2 and WPA3 on seperate LANs
    - Unclear to user
    - Connection problems

Conclusion

- Stations should not fallback to WPA2 if a SSID is WPA3 capable
- Stations should display the WPA version of a given SSID
- Stations should upgrade to SAE on known networks
- Mutual authentication important stepping stone for Wi-Fi


THANK
YOU

Key takeaways

- WPA3 has significant improvements over WPA2
- WPA3-TM vulnerable to downgrades if stations fallback to WPA2
- Stations should use WPA3 when possible and disable WPA2 for an SSID
- Personal Wi-Fi requires mutual authentication

References

[1] - WiGLE.net, Wi-Fi stats

[2] - Stephen Orr, Advancements in Wireless Security. At Cisco Live 2020