CERT-EU Security Advisory 2018-019

New attack on WPA/WPA2 using PMKID

Aug 07, 2018 — v1.0

History:

- *07/08/2018 — v1.0: Initial publication*

Summary

On August 4th the researcher Jens Steube published on his website a new method to get a hash which involves the Pre-Share Key (PSK) for a wifi access point [1]. A successfull exploitation of the technique allows an attacker to retrieve the PSK.

Technical details

The PSK could be recovered from this hash by brute force cracking. Although this technique has no advantage for the PSK cracking process - which depends essentially on the password length and complexity - it allows to have a hash, which can be attacked, much faster than other techniques, speeding up the overall process.

Other methods requires that the attacker sniff the network in order to record an authentication handshake. On the other hand, the new method just requires a single frame from the authentication handshake that can be generated as part of an authentication tried started by the attacker. From this authentication frame - which is a regular part of the protocol - the attacker can retrieve the PMKID, which is an optional hash value potentially present in all the wifi networks which support roaming between the access points (AP). The issue is, that it is well-known the way this hash is computed by using HMAC-SHA1, where the key is the Pairwise Master Key (PMK) and the data part is the concatenation of a fixed string label “PMK Name”, the access point’s MAC address and the station’s MAC address.

```
PMKID = HMAC-SHA1-128(PMK, "PMK Name" | MAC_AP | MAC_STA)
```

Besides just note, that in a pre-shared-key network, the PMK is actually the PSK. However,when wifi networks use the authentication protocol 802.1X - which means the use of an authentication server - instead of Pre-Shared keys, the PMK is a shared secret key between the AP and the client derived from the authentication process [2].

According the original post [1] these are the advantages of this new method in comparison with the former relying the full handshake recording:

- No more regular users required - because the attacker directly communicates with the AP (aka “client-less” attack)

- No more waiting for a complete 4-way handshake between the regular user and the AP
- No more eventual retransmissions of EAPOL frames (which can lead to uncrackable results)
- No more lost EAPOL frames when the regular user or the AP is too far away from the attacker
- No more fixing of nonce and replaycounter values required (resulting in slightly higher speeds)
- No more special output format (pcap, hccapx, etc.) - final data will appear as regular hex encoded string

Products Affected

As far as this attack harness an standard part of the protocol, it seems it should work in all wifi routers using the protocols 802.11i/p/q/r with roaming enabled. Of course, networks using authentication servers in the context of the 802.1X protocol are not affected. Finally, WPA3 is not affected.

Recommendations

As far as this new method provides a hash that has to be cracked by brute force, strengthen the password by generating long enough random passwords including special characters is a good security measure (twenty characters can be more than enough).

Workarounds

Turning off the roaming option can be helpful, but that should be tested in each specific implementation since optional fields of the protocol are involved. On the other hand, just strengthen the password can be an easier solution.

References

[1] https://hashcat.net/forum/thread-7717.html

[2] https://en.wikipedia.org/wiki/IEEE_802.11i-2004#The_four-way_handshake

[3] https://www.bleepingcomputer.com/news/security/new-method-simplifies-cracking-wpa-wpa2-passwords-on-80211-networks/