SECURITY WARNING: New Method Simplifies Cracking WPA/WPA2 Passwords on 802.11 Networks

By **Lawrence Abrams**

0

A new technique has been discovered to easily retrieve the Pairwise Master Key Identifier (PMKID) from a router using WPA/WPA2 security, which can then be used to crack the wireless password of the router. While previous WPA/WPA2 cracking methods required an attacker to wait for a user to login to a wireless network and capture a full authentication handshake, this new method only requires a single frame which the attacker can request from the AP because it is a regular part of the protocol.

This new method was discovered by Jens "atom" Steube, the developer of the popular Hashcat password cracking tool, when looking for new ways to crack the WPA3 wireless security protocol. According to Steube, this method will work against almost all routers utilizing 802.11i/p/q/r networks with roaming enabled.

This method works by extracting the RSN IE (Robust Security Network Information Element) from a single EAPOL frame. The RSN IE is a optional field that contains the Pairwise Master Key Identifier (PMKID) generated by a router when a user tries to authenticate.

The PMK is part of the normal 4-way handshake that is used to confirm that both the router and client know the Pre-Shared Key (PSK), or wireless password, of the network. It is generated using the following formula on both the AP and the connecting client:

"The PMKID is computed by using HMAC-SHA1 where the key is the 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." stated Steube's post on this new method.

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

You can see the PMKID inserted into a management frame below.

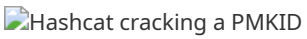
RSN IE field with PMKID

Previous WPA/WPA2 crackers required an attacker to patiently wait while listening in on a wireless network until a user successfully logged in. They could then capture the four-way handshake in order to crack the key.

"With any previous attacks on WPA an attacker has to be in a physical position that allows them to record the authentication frames from both the access point and the client (the

user)," Steube told BleepingComputer. "The attacker also has to wait for a user to login to the network and have a tool running in that exact moment to dump the handshake to disk."

Now an attacker simply has to attempt to authenticate to the wireless network in order to retrieve a single frame in order to get access to the PMKID, which can then be cracked to retrieve the Pre-Shared Key (PSK) of the wireless network.



Hashcat cracking a PMKID

It should be noted that this method does not make it easier to crack the password for a wireless network. It instead makes the process of acquiring a hash that can can be attacked to get the wireless password much easier.

How long to crack a WPA/WPA2 wireless password?

While Steube's new method makes it much easier to access a hash that contains the pre-shared key that hash still needs to be cracked. This process can still take a long time depending on the complexity of the password.

Unfortunately, many users do not know how to change their wireless password and simply use the PSK generated by their router.

"In fact, many users don't have the technical knowledge to change the PSK on their routers," Steube told BleepingComputer. "They continue to use the manufacturer generated PSK and this makes attacking WPA feasible on a large group of WPA users."

As certain manufacturers create a PSK from a pattern that can easily be determined, it can be fed into a program like Hashcat to make it easier to crack the wireless password.

"Cracking PSKs is made easier by some manufacturers creating PSKs that follow an obvious pattern that can be mapped directly to the make of the routers. In addition, the AP mac address and the pattern of the ESSID allows an attacker to know the AP manufacturer without having physical access to it," Steube continued to tell us via email. "Attackers have collected the pattern used by the manufacturers and have created generators for each of them, which can then be fed into hashcat. Some manufacturers use pattern that are too large to search but others do not. The faster your hardware is, the faster you can search through such a keyspace. A typical manufacturers PSK of length 10 takes 8 days to crack (on a 4 GPU box)."

Protecting your router's password from being cracked

In order to properly protect your wireless network it is important to create your own key rather then using the one generated by the router. Furthermore this key should long and complex by consisting of numbers, lower case letters, upper case letters, and symbols (&%$!).

"There's actually a lot of scientific research on this topic. There's many different ways to create good passwords and to make them memorable," Steube told BleepingComputer when we asked for recommendations on strong wireless passwords. "Personally I use a password manager and let it generate true random passwords of length 20 - 30."

Updated 8/6/18 12:00 EST with corrections from Steube. Thanks Jens!