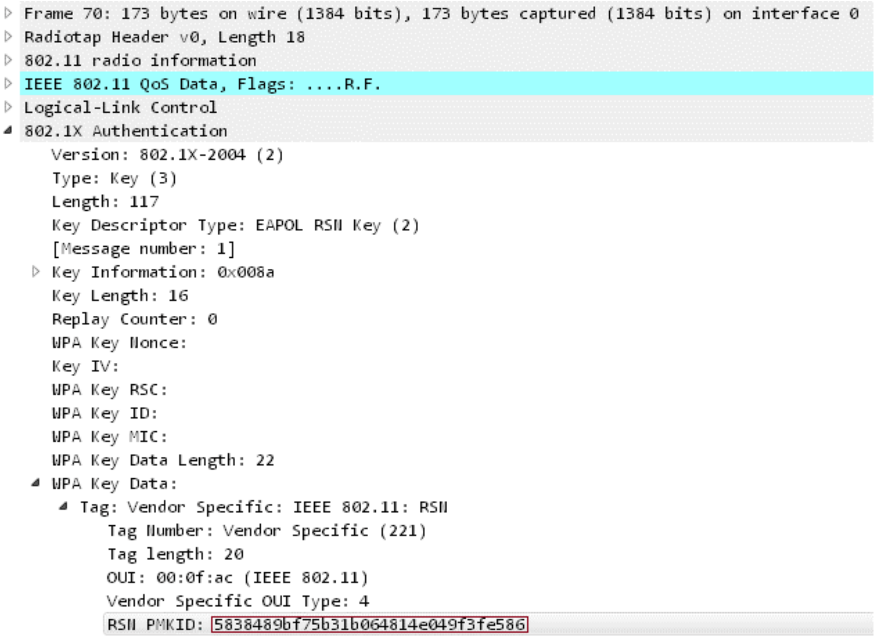
SwiftSafe Follow

SwiftSafe is a Cyber Security Company established by a group of highly motivated technologists and offers Security Consulting, Auditing and Testing Services.

Aug 18 · 3 min read

Hacking WiFi Password in a few steps using a new attack on WPA/WPA2



```
▷ Frame 70: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface 0
▷ Radiotap Header v0, Length 18
▷ 802.11 radio information
▷ IEEE 802.11 QoS Data, Flags: ....R.F.
▷ Logical-Link Control
◢ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  ▷ Key Information: 0x008a
    Key Length: 16
    Replay Counter: 0
    WPA Key Nonce:
    Key IV:
    WPA Key RSC:
    WPA Key ID:
    WPA Key MIC:
    WPA Key Data Length: 22
  ◢ WPA Key Data:
    ◢ Tag: Vendor Specific: IEEE 802.11: RSN
        Tag Number: Vendor Specific (221)
        Tag length: 20
        OUI: 00:0f:ac (IEEE 802.11)
        Vendor Specific OUI Type: 4
        RSN PMKID: 5838489bf75b31b064814e049f3fe586
```

A security researcher has devised a new WiFi hacking technique that could be exploited to easily crack WiFi passwords of most modern routers.

The security researcher Jens 'Atom' Steube, lead developer of the popular password-cracking tool Hashcat, has devised a new WiFi hacking technique that could be exploited to easily crack WiFi passwords of most modern routers.

The new WiFi hacking technique allows to crack WPA/WPA2 wireless network protocols with Pairwise Master Key Identifier (PMKID)-based roaming features enabled.

The expert was analyzing the recently launched WPA3 security standard when accidentally the new technique.

"This attack was discovered accidentally while looking for new ways to attack the new WPA3 security standard. WPA3 will be much harder to attack because of its modern key establishment protocol called "Simultaneous Authentication of Equals" (SAE)." Steube wrote in a post.

"The main difference from existing attacks is that in this attack, capture of a full EAPOL 4-way handshake is not required. The new attack is performed on the RSN IE (Robust Security Network Information Element) of a single EAPOL frame."

Older attack techniques required capturing a full 4-way handshake of Extensible Authentication Protocol over LAN (EAPOL), that is a network port authentication protocol. The new attack technique, differently from the previous ones, targets the Robust Secure Network Information Element (RSN IE).

The RSN protocol was designed for establishing secure communications over an 802.11 wireless network and it is part of the 802.11i (WPA) standard. Every time it attempts to establish a secure communication channel, the RSN broadcasts an RSN IE message within the network.

The Robust Security Network protocol has the PMKID (Pairwise Master Key Identifier), that is the key needed to establish a connection between a client and an access point.

An attacker can obtain the WPA PSK (Pre-Shared Key) password from the PMKID.

The WPA PSK is used in the "Personal" version of WPA and is designed for home and small office networks.

"Since the PMK is the same as in a regular EAPOL 4-way handshake this is an ideal attacking vector," Steube added.

"We receive all the data we need in the first EAPOL frame from the AP."

Below the description of the technique step by step:

Step 1—*An attacker can use a tool like hcxdumptool (v4.2.0 or higher) to request the PMKID from the targeted access point and dump the received frame to a file.*

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

***Step 2* —Run hcxpcaptool tool to convert the captured data from pcapng format to a hash format accepted by hashcat**

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

__Step 3—__Use Hashcat (v4.2.0 or higher) password cracking tool to obtain the WPA PSK (Pre-Shared Key) password that is the password of the target wireless network.

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

The time to crack the password depends on its complexity.

“At this time, we do not know for which vendors or for how many routers this technique will work, but we think it will work against all 802.11i/p/q/r networks with roaming functions enabled (most modern routers).” Steube concluded.

“The main advantages of this attack are as follow:

· 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 eventual invalid passwords sent by the regular user

· 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”

If you are searching for a good step by step explanation, give a look at the blog post published by the penetration tester Adam Toscher.

The new attack technique does not work against the recently introduced WPA3 security protocol.

The WPA3 protocol is "much harder to attack because of its modern key establishment protocol called "Simultaneous Authentication of Equals" (SAE)."