Two security researchers find WPA3 vulnerabilities

13 April 2019, by Nancy Cohen

Credit: CC0 Public Domain

You mean my safety blanket isn't safe? A next-gen standard "was supposed to make password cracking a thing of the past," clucked *Ars Technica*, after learning that vulnerabilities were found in the WPA3 protocol that could allow adversaries to get to Wi-Fi passwords and access the target network.

"Unfortunately," said the two researchers, we found that even with WPA3, an attacker within range of a victim can still recover the password of the network. This allows the adversary to steal sensitive information such as credit cards, password, emails, and so on, when the victim uses no extra layer of protection such as HTTPS."

WPA3 came on the scene in 2018, released by the Wi-Fi Alliance, designed to protect Wi-Fi networks from intruders. What males it leak? *Dark Reading* referred to "flaws in the handshake process" that could bring "low-cost attacks on the passwords used as part of network credentials."

Low-cost attacks? What does that mean? Dan Goodin in *Ars Technica* wrote that the design flaws in WPA3 raised questions about wireless security "particularly among low-cost Internet-of-things devices."

The attack involves a process that allows a legacy WPA2 device to attach to a WPA3-enabled access point; the resulting operation opens up the process "to a brute-force dictionary attack on the passwords used for authentication," said *Dark Reading*.

How big a deal is this, regarding impact? *Dark Reading* quoted Kevin Robinson, vice president of marketing for the Wi-Fi Alliance. Not all WPA3 personal devices were affected, and even the "small number of devices" that were could be patched through software updates.

That login process has the vulnerabilities that could make WPA3 less secure. Specifically, *Dark Reading* reported "side-channel vulnerability issues to the Simultaneous Authentication of Equals (SAE) handshake." The latter was further described as "a key piece of WPA3's improvement over WPA2."

Since the SAE handshake is known as Dragonfly; the researchers call the set of vulnerabilities Dragonblood.

The pair who discovered the flaw were Mathy Vanhoef of New York University Abu Dhabi and Eyal Ronen of Tel Aviv University and KU Leuven.

(In a side-channel information leak attack, explained Catalin Cimpanu, *ZDNet*, "WiFi WPA3-capable networks can trick devices into using weaker algorithms that leak small amounts of information about the network password. With repeated attacks, the full password can eventually be recovered.")

Not that anything about this discovery was shocking to Dan Goodin. "The current WPA2 version (in use since the mid 2000s) has suffered a crippling design flaw that has been known for more than a decade," he wrote.

He said the four-way handshake was a cryptographic process that was used to validate computers, phones, and tablets to an access point and vice versa—and contains a hash of the network password. "Anyone within range of a device connecting to the network can record this handshake. Short passwords or those that aren't random are then trivial to crack in a matter of seconds."

Fortunately, they blogged, we expect that our work and coordination with the Wi-Fi Alliance will allow vendors to mitigate our attacks before WPA3 becomes widespread."

On April 10 the Wi-Fi Alliance released a statement regarding what they described as "a limited number of early implementations of WPA3-Personal, where those devices allow collection of side channel information on a device running an attacker's software, do not properly implement certain cryptographic operations, or use unsuitable cryptographic elements."

They said the small number of device manufacturers affected "have already started deploying patches to resolve the issues. These issues can all be mitigated through software updates without any impact on devices' ability to work well together. There is no evidence that these vulnerabilities have been exploited."

The Wi-Fi Alliance thanked the two researchers, Vanhoef and Ronen, for discovering and "responsibly reporting these issues, allowing industry to proactively prepare updates ahead of widespread industry deployment of WPA3-Personal."

They told Wi-Fi users that they should ensure they have installed the latest recommended updates from device manufacturers.

More information:
papers.mathyvanhoef.com/dragonblood.pdf

APA citation: Two security researchers find WPA3 vulnerabilities (2019, April 13) retrieved 22 April 2019 from https://techxplore.com/news/2019-04-wpa3-vulnerabilities.html