Peer Response

Edward, this post about mitigating brute force and denial of service (DoS) attacks is instructive. Especially highlighted the type of Wi-Fi protocol that could improve on the security.

Wi-Fi Protected Access III (WPA3) become mandatory for all new Wi-Fi certifications since July 1, 2020 (CETECOM, 2020). WPA3 offers greater protection against offline brute-force attacks by replacing the WPA2 Pre-Shared Key (PSK) authentication with Simultaneous Authentication of Equals (SAE) (Wi-Fi Alliance, N.D.). Nevertheless, if the WPA2 password combination is complex enough, it could still resist offline brute-force attacks in a reasonable of time. On the other hand, the Key Reinstallation Attacks (KRACK) were serious weaknesses in WPA2 (Mathy, 2017) that discovered a similar vulnerability under WPA3. Due to the KRACK targeting the device instead of the router, plus the supposed advantages of dragonfly handshake in WPA3 found vulnerabilities under certain conditions. KRACK can recover the password within range of a victim who does not use extra protection such as HTTPS, these vulnerabilities present as Dragonblood attacks (Mathy & Eyal, 2019). Fortunately, the Wi-Fi Alliance has published software patches for that which supported the pre-existing WPA3 devices and remained the standard being issued.

The WPA3 certification program, according to Mathy, was focused on making WPA3 easier to adopt for vendors, and it missed an opportunity to truly improve Wi-Fi security (Mathy, 2018). In conclusion, the WPA3 protocol does not significantly show improvement on WPA2, while still stronger than the WPA and WPS applied in Gilson et al., 2015's article "Compromising a Medical Mannequin" (Gilson et al., 2015).

References:

CETECOM (July 4, 2020) Wi-Fi CERTIFIED WPA3™ will become mandatory on July 1, 2020. *Knowledge Center*. Available from: https://www.cetecom.com/en/news/wi-fi-certified-wpa3-will-become-mandatory-july-1-2020/ [Accessed 22 November 2021].

Wi-Fi Alliance (N.D.) Security. *Discover Wi-Fi*. Available from: https://www.wi-fi.org/discover-wi-fi/security [Accessed 22 November 2021].

Mathy, V. (2017) Breaking WPA2 by forcing nonce reuse. *Key Reinstallation Attacks*. Available from: https://www.krackattacks.com/ [Accessed 22 November 2021].

Mathy, V. & Eyal, R. (April 2019) Analysing WPA3's Dragonfly Handshake. *DRAGONBLOOD*. Available from: https://wpa3.mathyvanhoef.com/ [Accessed 22 November 2021].

Mathy, V. (June 27, 2018) WPA3: A Missed Opportunity. Available from: https://www.mathyvanhoef.com/2018/06/wpa3-missed-opportunity.html [Accessed 22 November 2021].

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. *Healthcare Information Systems and Technology (Sighealth).* Available: https://www.researchgate.net/publication/281487935\_Compromising\_a\_Medical\_Mannequin [Accessed 13 November 2021].

Edward van Biljon

<https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=284755>