Initial Post

The number of medical devices connected to networks is increasing at an exponential rate. These devices have the inherent security risk of exposing both data and device control. Compared to the first quarter of 2020 and 2021 in healthcare organisations, targeted attacks increased by 76 per cent, while IoT attacks increased by 57 per cent according to the survey by Obrela’s Q3 Digital Universe Study. (George, 2021).

With reference to this article “Compromising a Medical Mannequin” (Gilson et al., 2015) discussed the two common major cyber threats, brute force attack and denial of service attack (DoS). The brute force attack uses the trial-and-error approach to guess login information or hash keys, with dictionary and rainbow tables that contain pre-computed data to improve efficiency. DoS attack is a malicious attempt to make an online service unavailable by overloading it. By using the attack tool, BackTrack 5, Gilson’s team was able to crack the WiFi Personal Identification Number (PIN) within a few hours with a brute force attack. Moreover, with the same tool, they performed a DoS attack on the software by blacklisting the found MAC address.

In most cases, strong passwords, limited login attempts, or two-factor authentication could mitigate brute force attacks. In the case of this article research, the choice of WiFi security protocols is indispensable. Both WiFi security protocols WPA and WPS found vulnerabilities, Key Reinstallation Attack (ENISA, 2017) and VU#723755 (CISA, 2013), which should replace by WPA3 (Rob, 2018). On the other hand, the DoS attack could mitigate with CAPTCHAs and adding deny list to block the location or source. With the widespread of Content Distribution Network (CDN) and Web Application Firewall (WAF), abnormal traffic or common attack patterns or behaviour could be monitored and blocked.

References:

George, P. (April 21, 2021) Obrela’s Digital Universe Study: Europe sees 67% increase in brand attacks. *Digital Universe Study.* Available:

https://www.obrela.com/digital-universe-study-q1-2020-vs-q1-2021/ [Accessed 13 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].

ENISA (October 19, 2017) An overview of the Wi-Fi WPA2 vulnerability. *Cyber security info notes*. Available: https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability [Accessed 13 November 2021].

CISA (January 23, 2013) Wi-Fi Protected Setup (WPS) Vulnerable to Brute-Force Attack. *Alert (TA12-006A).* Available: https://us-cert.cisa.gov/ncas/alerts/TA12-006A [Accessed 13 November 2021].

Rob, T. (January 9, 2018) WPA3 protocol will make public Wi-Fi hotspots a lot more secure. *TECHSPOT*. Available: https://www.techspot.com/news/72656-wpa3-protocol-make-public-wi-fi-hotspots-lot.html [Accessed 13 November 2021].