Student post: Ying

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.

Thank you, Ying, for the informative discussion. I agree with your points regarding the use of CAPTCHA to mitigate potential DoS attacks. The benefit of CAPTCHA is that it would support the mitigation of malicious users controlling computers to allow automated botnets to perform multiple transactions and attempts at infiltrating the network (Rajaee et al., 2017). CAPTCHA's themselves are fully automated, which is another reason why they can provide a valuable benefit as they require little human maintenance, and the cost is low. This is a valuable benefit when balancing budget costs. However, some limitations can affect the accessibility of users, particularly in the healthcare sector. Not all CAPTCHA's are designed with specific learning or medical needs such as vision impairment or impaired motor skill development. To

support this, some versions have audio options; however, that does require users to hear the letters or numbers clearly where medical environments might be busy and noisy (Kumar & Dhir, 2013). This would also require specific hardware such as speakers on the device to perform this. You could include better solutions with imagery instead of text, but that may increase the implementation costs.

Furthermore, the more significant inconvenience the process becomes for the user, the more frustrated they are likely to become and present a heavy cognition and stressful load (Nakaguro et al., 2013). This can result in the user abandoning their idea of using the device. This can be helpful to mitigate a threat but not for genuine human users. Google introduced reCAPTCHA Enterprise (Google, 2021), succeeding their earlier versions, aiming to provide seamless and fast interaction with advanced security for all users to improve this process.

CAPTCHA offers a useful mitigation tool but would be better if provided with further support strategies such as limiting the number of logins attempts (Mehra et al., 2011). If a failed verification occurred after a set number of times the IP address used could be blocked for a set time interval. This would be simple to integrate, cost-effective for the provider, achieve the same objectives.

Google. (2021). WHAT IS RECAPTCHA? Available: https://www.google.com/recaptcha/about/ [Accessed 2021 21 November].

Kumar, M. & Dhir, R. (2013). Design and Comparison of Advanced Color based Image CAPTCHAs. *International Journal of Computer Applications,* 61, 24-29.

Mehra, M., Agarwal, M., Pawar, R. & Shah, D. (2011). *Mitigating denial of service attack using CAPTCHA mechanism*. *Proceedings of the International Conference & Workshop on Emerging Trends in Technology.* Mumbai, Maharashtra, India: Association for Computing Machinery.

Nakaguro, Y., Dailey, M., Marukatat, S. & Makhanov, S. (2013). Defeating line-noise CAPTCHAs with multiple quadratic snakes. *Computers & Security,* 37, 91–110.

Rajaee, O., Large, G. S. & Bastian, J. D. (2017). In-Depth Study of CAPTCHA. *Pennsylvania State University*.