Unit 1 Collaborative Discussion 1

Summary Post

Considering the vulnerabilities and threats to medical device systems as identified in the paper by Glisson et al. (2021), Denial of Service (DoS) and brute force attacks were highlighted as two main sources of concern. In response to securing these types of devices, Taylor (2021) recommends the use of complex password rules as well and filtering excessive network traffic from a single internet address—a theme which many students agreed with, that is, the role of firewalls, network analysis, and account lockouts after a certain number of failed attempts.

Given that cyberattacks are driven by the valuable nature of data, Anil et al. (2020) consider various types of threats to data security, namely Distributed Denial of Service, phishing, password, dictionary, and brute-force attacks. While there are several systems to help protect against cyber-attacks—Intrusion Detection and Prevention systems, firewalls—the biggest cause of concern is employees within the organisation (Al-Mohannadi et al., 2018). For this reason, cyber-security training is of critical importance within organisations that handle valuable data, as is the use of secure wireless protocols such as WPA3, 2FA authentication, encryption of data and assignment of least privilege to authorised users. Although, as noted by Shan (2021), encryption techniques on small medical devices may be limited due to their lack of processing power, latency, and power consumption.

Microsoft's STRIDE/DREAD model—specifically, STRIDE—is useful to measure the likelihood and impact of exploiting specific vulnerabilities. Zhang et al. (2021) provide a map between Microsoft's STRIDE model and related cyber security features such as authentication and availability. Information system developers can then leverage such mapping to guide the development of resilient systems. The OWASP Foundation also provides several security measures to protect valuable data, for instance, the use of Intrusion Detection (OWASP, 2021). In addition, passwords are a major source of data used for authentication. Smirnov (2021) considers, mitigate typical brute force attacks. It is important that router passwords are sufficiently complex and do not simply use default router passwords.

In summary, information security is a collaboration between data sources and the network environment that hosts the devices. Firewalls, analysis of network traffic and application logs, strong authentication mechanisms (such as CAPTCHAs, 2FA, 802.1x certificates), disabling of default root accounts and request rate-limiting are techniques that, when employed, will greatly increase information system resilience.

References

Al-Mohannadi, H., Awan, I., Al Hamar, J., Al Hamar, Y., Shah, M. & Musa, A. (2018). Understanding awareness of cyber security threat among IT employees. *6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW):* 188-192.

Anil, A., Shukla, V.K. & Mishra, V.P. (2020). Enhancing Data Security Using Digital Watermarking. *International Conference on Intelligent Engineering and Management (ICIEM):*364-369.

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. *Healthcare Information Systems and Technology (Sighealth)*. Available from: **https://arxiv.org/ftp/arxiv/papers/1509/1509.00065.pdf** [Accessed 1 Dec. 2021]

OWASP Foundation Inc. (2021). Intrusion Detection. Available from https://owasp.org/www-community/controls/Intrusion_Detection [Accessed 1 Dec. 2021]

Shan, S. (2021). Collaborative Learning Discussion 1: Initial Post. Available from https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=285306 [Accessed 1 Dec. 2021]

Smirnov, A. (2021). Collaborative Learning Discussion 1: Initial Post. Available from https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=285146 [Accessed 1 Dec. 2021]

Taylor, E. (2021). Collaborative Learning Discussion 1: Initial Post. Available from https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=284761 [Access 1 Dec. 2021]

Zhang, L., Taal, A., Cushing, R., de Laat, C. & Grosso, P. (2021). A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces. *International Journal of Information Security*:1-17.