Simon Miller

Module 2: Discussion 1

Summary Post and Reflection:

In reflection of the discussion over the last 3 weeks, the medical mannequin case represents a good example of the importance of industry standards first, and second the importance of adhering to them across all levels of an organization's IT and physical infrastructure. This is made clear throughout the paper where a team of university students were able to perform both a denial of service attack on the mannequin as well as crack the device's access point via a brute force attack.

By applying Microsoft's STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) and DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) the overall risk of the student's exploits could be ascertained (Shevchenko, 2018). My group deemed all attacks to represent a medium to high risk; the live CD representing the least risky threat due to the time it took to complete relative to the equivalent virtual machine running Kali Linux (Glisson, et al, 2012).

Ultimately, the relevance of this paper lies less in the attacks themselves, as these exploits are highly unlikely to be successful in most infrastructures today. They do, however, provide an important lesson in the risks and challenges faced by incorporating increasing numbers of medical IoT devices. That a team of technically savvy students with no prior penetration testing experience were able to exploit a medical device is telling of the risks present, especially if carried out by more experienced practitioners. There is no blanket solution to securing the exponential growth of the IoT ecosystem, but steps in standardization and cooperation for broader remote management is being found to be an effective start as it can align policy and avoid outliers “slipping through the cracks” (Sasaki, 2020).

References:

Glisson, W.B., Mcdonald, T., Campbell, M., Andel, T., Jacobs, M. & Mayr, J. (2014) Compromising a Medical Mannequin. (2012), pp.1–11

Sasaki, R. (2020). Risk Assessment Method for Balancing Safety, Security, and Privacy in Medical IoT Systems with Remote Maintenance Function. IEEE 20th International Conference on Software Quality, Reliability and Security Companion. New York City NY United States: IEEE, pp.190–197.

Shevchenko, N. (2018). *Threat Modeling: 12 Available Methods*. [online] SEI Blog. Available at: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/ [Accessed 26 May 2021].