Unit 2 Reflection

Learning

This unit considered a hacking scenario of a medical mannequin (Glisson et al., 2015) to demonstrate how easily medical devices can be compromised using available tools. This scenario introduced Denial of Service (DoS) and brute force attacks that hackers may leverage. DoS attacks attempt to overwhelm systems that aim to disrupt the system. In contrast, brute force attacks are employed against password policies in a system. I consider DoS a cybersecurity threat and brute force attacks to target system vulnerability. Humayun et al. (2020) list additional vulnerabilities as credential reuse, cross-size scripting (XSS), malware, phishing, man-in-the-middle attacks, and SQL injection. Their systemic mapping study considers DoS, malware and "other" as the top three vulnerabilities, with DoS occupying 37% of vulnerabilities. This was a good validation of the medical mannequin scenario since we touched on how devastating DoS can be on medical devices; therefore, the CIA triad (introduced in Unit 1) are core design goals of medical devices, though I think Confidentiality may not be relevant if no patient data processing takes place on the device.

In the module Secure Software Development, I focused on the importance of using secure programming techniques applicable in medical devices. Sametinger et al. (2015) note that "loss, theft, or exposure of personally identifiable information is one major problem … which accounts for one-fifth of all these reported issues". They also mention that more than 90% of device recalls are due to software related issues.

Exploits

DoS vulnerability can be exploited by using a ping of death technique which sends Internet Control Message Packet (ICMP) network packets larger typically supported, for instance, ICMP packets that are over 100KB in size, which may cause the machine to freeze, crash or reboot. Some tools that can be leveraged for DoS include Low Orbit Ion Cannon (https://sourceforge.net/projects/loic/) or OWASP Switchblade (https://owasp.org/projects/). Brute force attacks exploit weak password policies and are often leveraged in penetration testing. Tools in the category include Brutex (https://github.com/1N3/BruteX), AirCrack-ng (https://www.aircrack-ng.org/) used to assess Wi-Fi network security or John the Ripper (https://www.openwall.com/john/), Rainbow Crack (http://project-rainbowcrack.com/) that uses pre-computed rainbow tables.

Collaborative Discussion

Continuing the discussion, I found a fellow student's rather informative post. They mention that due to limited power requirements and computation power, medical devices may be susceptible to using poor encryption (Swanlow, 2021). I thought this was quite insightful because it highlighted the limited processing capabilities that may lead to vulnerabilities.

Teamwork

We continued to collaborate as a team using the Discord platform and often got to know a little more about each other, such as a language nuance which is enlightening. Following the previous module in which the team leveraged Google Calendar, the team chose to leverage similar eventing notifications in Discord. Discord is a unique platform to leverage for team discussions; however, I would recommend alternate team-friendly platforms such as Slack or Teams.

Eportfolio

Based on feedback from the previous module, I decided to take a slightly different approach to the content layout for this module. The last module's feedback mentioned the focus on unit content. So, I decided to make unit content more upfront and centre via a single scrolling area. This change involves JavaScript and styling changes and took me to investigate scrolling observers and CSS backgrounds. I thoroughly enjoy the JavaScript language based on the *prototype* model and am constantly awed by the power of CSS.

References

Glisson, W.B., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015). Compromising a medical mannequin. arXiv:1509.00065.

Humayun, M., Niazi, M., Jhanjhi, N.Z., Alshayeb, M. & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45(4):3171-3189.

Chapple, M., Stewart, J.M. & Gibson, D. (2018). CISSP Certified Information Systems Security Professional Official Study Guide. John Wiley & Sons.

Sametinger, J., Rozenblit, J., Lysecky, R. & Ott, P. (2015). Security challenges for medical devices. *Communications of the ACM,* 58(4):74-82.

Swanlow, S. (2021). Collaborative Learning Discussion: Initial Post. Available from https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=285306 [Accessed 03 Jan. 2021]