Hi Haseeb

Thank you for your post. You have provided some great mitigation techniques.

In addition, if we take a closer look at the Muse software and the way it communicates with the iStan device, this is done over http which is insecure. This is where encryption in transit comes in by making use of HTTPS. HTTPS is simply HTTP with encryption. HTTPS uses TLS (Transport Layer Security) to encrypt HTTP requests and responses (Digicert, 2021). Vendors manufacturing medical devices that support web-based connectivity needs to ensure that encrypted protocols are supported. Furthermore, if TLS is used, the latest version of TLS should be implemented to avoid POODLE and BEAST attacks (Sheffer, 2015).

Another aspect to consider is physical brute-force where malicious users are granted physical access to medical devices that are not securely stored and/or locked. If attackers gain access to these devices, they can extract the physical disk and obtain patient information (Wang et al., 2020). If locking the device is not possible one should consider storage encryption or encryption at rest, in this way if the attacker gains access to the physical disk, it will be very difficult to decrypt and extract sensitive patient information (Wang et al., 2020).

List of References

Digicert (2021) What is SSL, TLS & HTTPS? https://www.digicert.com/what-is-ssl-tls-and-https [Accessed 20 November 2021]

Wang, Z., Ma, P., Zou, X., Zhang, J., & Yang, T. (2020) ‘*Security of Medical Cyber-physical Systems: An Empirical Study on Imaging Devices’, IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops.* Canada, 6-9 July 2020. USA: IEEE. Available from: https://ieeexplore.ieee.org/document/9162769 [Accessed 20 November 2021]

Y. Sheffer, R. Holz & P. Saint-Andre. (2015) Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS). *Internet Engineering Task Force (IETF*). Available from: https://tools.ietf.org/html/rfc7457 [Accessed 20 November 2021]

Hi Kingsley

A good read, thank you for sharing.

In addition, to adequately protect medical devices in a healthcare network, the surrounding I.T network infrastructure needs to be protected as well. These include wireless access points, network routers and switches as well as computers that has access to patient information. Very often these computers are left with legacy and unpatched operating systems, outdated anti-virus software and are easily accessible with the use of weak passwords (Williams & Woodward, 2015). Furthermore, I.T network devices are often connected to the same VLAN as medical devices since this network architecture is less complicated to implement. This brings about additional threats as well; if a single device in the network is hacked, others can be easily accessible and hacked as well. Network segmentation is highly important in network design and is one mitigation technique that limits and minimizes the attack surface (Williams & Woodward, 2015).

Computers and/or laptops that are used in a medical environment should have the latest anti-virus installed, operating systems should be patched up to date and local hard disk drives should be encrypted. Furthermore, USB ports should be disabled to prevent downloading of any sensitive information.

In relation to the above-mentioned points, according to Sametinger et al. (2015) I.T infrastructure used to connect medical devices must comply with the Health Insurance Portability and Accountability Act (HIPAA) which aims to protect medical records and personal information (HIPPA, 1996).

List of References

HIPPA (1996) *Health Insurance Portability and Accountability Act of 1996*. Available from: https://www.healthit.gov/sites/default/files/rules-regulation/health-insurance-portability.pdf [Accessed 20 November 2021]

Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security challenges for medical devices*. Communications of the ACM, 58(4): 74–82.* Available from: https://dl.acm.org/doi/fullHtml/10.1145/2667218 [Accessed 20 November 2021]

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical devices. *Health Informatics Journal, 25(2):* 305–316. Available from: https://journals.sagepub.com/doi/pdf/10.1177/1460458217706184 [Accessed 20 November 2021]