The healthcare industry, as with most industries is becoming more digitised in the world we live in today. Digitisation and wireless connectivity of devices provides the opportunity for potential cyber-attacks. The paper written by Glisson et al. (2015), “Compromising a Medical Mannequin” provides insights to threats and vulnerabilities to healthcare systems and medical devices as well as conducting an experiment. The aim and objective of the experiment was to compromise a mannequin system by identifying vulnerable components such as the network security solution and the network protocol (Glisson et al, 2015). These components were breached using brute-force, DOS (Denial of Service) and security control attacks. Other major threats and vulnerabilities discussed include the following:

* Not capturing or logging security-based incidents or failures detected on medical devices (Fu and Blum, 2013)
* Data (device pins) being passed through the network in clear text as indicated in the research performed by Li et al. (2014) on glucose monitors.
* Unencrypted RF-transmissions between devices and programming units for pacemakers allowing hackers to eavesdrop and extract PII (Personally Identifiable Information) as highlighted by Halperin et al. (2008)

Various mitigation techniques for the above-mentioned threats and vulnerabilities exist in the industry today, these include:

* Next Generation Firewalls (NGFW’s) which play a vital role in protecting against sophisticated threats as well as DOS attacks (Soewito & Andhika, 2019). Some NGFW’s have advance features such as an IPS (Intrusion Prevention System) which are able to detect, prevent and log attempts (Check Point, 2021).
* Protection against brute-force attacks include strong password policies, MFA (Multi-Factor Authentication), limitation of failed login attempts, implementation of user lockouts, use of Captcha as well as continuous log monitoring amongst others. (Saito et al, 2016)
* Encryption is also key when data is being transferred across networks, however for medical devices that uses batteries, encryption can reduce battery life (Williams & Woodward, 2015)
* And lastly physical access to medical devices, if the devices are not easily accessible (i.e., locked in a secure place) hackers may be deterred.

In conclusion, cybersecurity threats and vulnerabilities are very similar to other networking systems, the key difference is that in a medical environment the safety of a patient is at risk (Williams & Woodward, 2015). While the above technologies and techniques are effective, they cannot offer complete protection. Cybersecurity awareness training among medical staff also plays a vital role.

List of References

B. Soewito & C. E. Andhika. (2019) ‘Next Generation Firewall for Improving Security in Company and IoT Network’, 2019 International Seminar on Intelligent Technology and Its Applications *2021(1):* 205-209. Available from: https://sci-hub.se/10.1109/ISITIA.2019.8937145 [Accessed 13 November 2021]

Check Point (2021) What is a Next Generation Firewall (NGFW)? <https://www.checkpoint.com/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/> [Accessed 13 November 2021].

Fu, K. & Blum, J. (2013) Controlling for Cybersecurity Risks of Medical Device Software. *Communications of the ACM* 56(10): 35-37.Available from: https://www.researchgate.net/publication/262241251\_Controlling\_for\_Cybersecurity\_Risks\_of\_Medical\_Device\_Software [Accessed 13 November 2021].

Glisson, W., Andel, T., Mcdonald, J., Jacobs, M., Campbell, M. & Mayr, J. (2015). Compromising a Medical Mannequin. Available from: https://www.researchgate.net/publication/281487935\_Compromising\_a\_Medical\_Mannequin [Accessed 12 November 2021].

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., Maisel, W. H. (2008) ‘Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses’, *IEEE Symposium on Security and Privacy*. Oakland, CA, 18-22 May 2008. USA: IEEE. Available from: <https://ieeexplore.ieee.org/abstract/document/4531149> [Accessed 13 November 2021].

Li, C., Zhang, M., Raghunathan, A., & Jha, N. (2014) *Security and Privacy for Implantable Medical Devices.* 1st ed. New York: Springer publishing. Available from: <https://www.springerprofessional.de/en/attacking-and-defending-a-diabetes-therapy-system/1823450> [Accessed 13 November 2021].

Saito, S., Maruhashi, K., Takenaka, M., & Torii, S. (2016). TOPASE: Detection and Prevention of Brute Force Attacks with Disciplined IPs from IDS Logs. *Journal of Information Processing*, 24(2): 217–226. Available from: doi:10.2197/ipsjjip.24.217 [Accessed 14 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 14 November 2021].