Summary Post

It is not uncommon that healthcare industries around the world are adopting technologies through the use of IoMT (Internet of Medical Things) devices to provide better services to patients and medical professionals. The absence of security or poor implementation of security best practices in many of these devices leaves them vulnerable to attacks and access to patient data (Ondiege et al, 2016). This is confirmed by a paper written by Glisson et al. (2015) where a mannequin system was compromised by a group of inexperienced university students.

While the above mentioned attacks are common; effective mitigation techniques do exist. These include clean-desk policies (Biljon, 2021), impersonation attacks (where an attackers pretends to be an employee), updated and hardening of operating systems, effective password policies and the implementation of zero-trust networks (Abdulhak, 2021), views that the writer strongly agrees with. In addition medical devices must adopt robust authentication mechanisms (Madrid, 2021) as well as comply with the Health Insurance Portability and Accountability Act (HIPAA, 1996) which aims to protect medical records and personal information (Sametinger et al, 2015).

Furthermore, Gollakota et al. (2011) suggests an isolated device that acts as a shield to prevent direct access to medical devices, which could possibly prevent DOS attacks (Necat, 2021), a perspective the writer appreciates and agrees with. Similar to networking where CyberArk (CyberArk, 2021) is used to control access to devices; however this technology is based on radio frequencies rather than networking protocols.

In any industry, surveillance, monitoring, alerting and logging is vitally important in the detection and prevention of cyber-attacks. Campbell (2016) mentions that if one cannot see what is happening on systems (real-time monitoring) they cannot effectively manage it. In closing, one should adopt a holistic approach to cybersecurity practices in a healthcare setting involving multidisciplinary groups like system administrators, policymakers, medical professionals and cybersecurity experts (Tully et al, 2020).

List of References

Abdulhak, H. (2021). ’Collaborative Learning Discussion 1’. Peer response submitted to University of Essex Online for [NISM\_PCOM7E November 2021] Initial Post by Zihaad Khan. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=285238 [Accessed 27 November 2021].

Biljon, V, E. (2021). ’Collaborative Learning Discussion 1’. Peer response submitted to University of Essex Online for [NISM\_PCOM7E November 2021] Initial Post by Zihaad Khan. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=285238 [Accessed 27 November 2021].

Campbell, T. (2016) Practical Information Security Management. 1st ed. APRESS.

CyberArk (2021). Privileged Access Manager. Available from: https://www.cyberark.com/products/privileged-access-manager/ [Accessed 27 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 27 November 2021].

Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., & Fu, K. (2011) ‘They Can Hear Your Heartbeats: Non Invasive Security for Implantable Medical Devices’, ACM SIGCOMM 2011 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. Toronto, Canada, 15-19 August. Available from: https://dl.acm.org/doi/pdf/10.1145/2018436.2018438 [Accessed 27 November 2021].

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 27 November 2021].

Madrid, A. (2021). ’Collaborative Learning Discussion 1’. Peer response submitted to University of Essex Online for [NISM\_PCOM7E November 2021] Initial Post by Zihaad Khan. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=285238 [Accessed 27 November 2021].

Necat, B. (2021). ’Collaborative Learning Discussion 1’. Peer response submitted to University of Essex Online for [NISM\_PCOM7E November 2021] Initial Post by Zihaad Khan. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=285238 [Accessed 27 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 27 November 2021].

Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare Challenges in the Era of Cybersecurity. *Health security,* 18(3): 228–231. Available from: https://doi.org/10.1089/hs.2019.0123 [Accessed 27 November 2021].

Feedback from Peers

**Response by Beran**

Hi Zihaad,

You have provided a good selection of mitigations.

Gollakota et al. (2011) recommend a further technical solution in a separate physical device used to prevent any direct access to the medical device thus reducing the risk of certain attacks, including certain denial of service attacks. To further the holistic approach, establishing security regulations for the medical device manufacturing industry would increase understanding of the associated threats and vulnerabilities whilst driving better security practices (Martinez, 2018).

Regards, Beran

References

Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., & Fu, K. (2011) ‘They Can Hear Your Heartbeats: Non Invasive Security for Implantable Medical Devices’, ACM SIGCOMM 2011 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. Toronto, Canada, 15-19 August.

Martinez, J. (2018) ‘Medical Device Security in the IoT Age’, 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). New York, USA, 8-10 November. IEEE.

**Response by Edward**

Hi Zihaad, you have several valid points with regards to security that can be implemented at a healthcare facility.

Healthcare facilities work with patients’ personal information daily and many of these records are stored in files that contains the patient’s history from the day they signed up with there doctor. Securing this information at the facility is vitally important. The data should not be accessible by anyone that does not have the correct clearance. Patient data should be behind locked doors that would require a form of security such as biometrics (Meaghan Kelly, 2018) to access it.

With reconnaissance, attackers look for information. An example would be a clean desk. Medical facilities should look at implementing policies such as “clean-desk” policy if they do not have it in place. This ensures that patient files, prescriptions or any other sensitive information is not left lying around. Information that is lying around, can easily be stolen by someone standing at the front desk (Elliot Bolland, 2021).

Other forms of attack can be in the form of an attacker pretending to be a contractor to come and carry out maintenance. Personally, I have experienced this. The IT manager comes to the desk and says, “Person X is here to do the following job, please let them in”. The front desk person then provided me with a spare access card that had access to many sections of the hospital and this bypasses all security in place as the attacker has unrestricted access and can do anything from plugging in a USB device to capture keystrokes, or when a person leaves their desk, download malware so that later they have a backdoor into the systems.

**Response by Haseeb**

Thank you Zihaad for your valuable post, you mentioned here an important view to threats such as no logging or failure detection and transferring of data in plain text through the network. In addition, locking the devices in a secure place to keep them away from ant unauthorized persons is crucial.

Firch (2021) highlighted keeping operating systems and software up to date as software developers deploy patches to fix bugs or remediate the discovered vulnerabilities to maintain the security of software or system at all, moreover, changing default operating system policies for example default domain password policy such as enforce password history, maximum password age, minimum password length, password complexity requirement, and store password using encryption will improve the security and used as mitigation of threat and vulnerabilities of health devices.

The adoption of zero-trust architecture moves network security toward a model that allows restricted access to the application, network, and environment (Salvi, 2021). Keeping IT infrastructure secure by restricting access to only authorized persons can be the first door of defense against the unwanted intruder.

**Response by Aldo**

Thank you Zihaad for your post explaining and identifying security threats and vulnerabilities that led to compromise the iStan mannequin. Accordingly, to Yaqoob and Atiquzzaman (2019) vulnerabilities and threats in medical devices such as the iStan mannequin are strongly related to communication protocols, design flaws in software and inappropriate security measures added during development.

For example, Man in the Middle (MITM) is an attack that occurs when someone intercepts the communication between a transmitting and a receiving node. The attacker deceives node 1 and node 2 by making them believe that communication is flowing in a secure channel, but attacker can intercept and modify the information flowing through it (Conti et al. 2016). Bluetooth Low Energy (BLE) a protocol alternative to Bluetooth is used by a wide variety of medical devices. It offers low power consumption and short latency periods, ideally for devices where battery life is important and sensed data accuracy is critical. Because of lack of robust authentication mechanisms, devices using BLE are susceptible to MITM attacks (Yaqoob and Atiquzzaman). Classen et al. (2018) demonstrated that measured data, credentials and private information from wearable medical devices using BLE was intercepted by using a customized app and connecting to the devices.

Regulations and mitigation techniques have been enforced in order to prevent personal health information to be leaked. One of those regulation is HIPAA (Health Insurance Portability and Accountability Act) that protects personal health information by requiring suitable privacy-related controls (Annas, 2003). Because of the limited availability of resources in medical devices security mitigation techniques are challenging to incorporate. Some of them proposed are Isolation-Based architecture and Data Flow Integrity mechanisms. The first consists on isolating sensible security parts of the system in an unreachable module and the last on verifying unchanged states of memory using pointers (Yaqoob and Atiquzzaman).