**Discussion Forum 1**

Initial Post

Recent advancements in medical technology have resulted in the introduction of devices that can identify, monitor, and control the physiological condition of patients (Glisson et al., 2015). Whilst this provides many opportunities in medicine, it also creates new opportunities for cyber attacks on the industry and provides fresh incentives for adversaries.

There are two major threats covered in this paper. Brute force attacks can be used to compromise the access point credentials which could lead to a compromise of the confidentiality, integrity, and availability of the device. In addition, denial of service attacks can be used to deny access to the access point and therefore prevent genuine user access. From related work in the medical industry, sniffing and tampering with unencrypted connections is also raised as a potential key threat as this can be used to modify device behaviour or extract confidential information, such as medical readings (Halperin et al., 2008).

The successful attacks by a low capability threat actor covered in this paper demonstrate that the iStan device has numerous exploitable vulnerabilities. These include weak authentication which is susceptible to brute force attacks. This device is also vulnerable in that the system has no adequate means of identifying and managing malicious traffic sent to the device. The software dependencies of the device could also open it up to further vulnerabilities.

It is important to mitigate threats holistically through people, process, and technology (Humphreys, 2008). Glisson et al. (2015) suggest that practitioners utilising medical technology should be sufficiently trained in security in order to identify failing or erroneous devices. In addition, procedures should be implemented that ensure they are managed appropriately to prevent any associated harm. The use of two-factor authentication would protect devices from brute force attacks; however due consideration should be given to the implications on performance and usability considering the requirements of the particular medical device (Reese et al., 2019). 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).

References

Glisson, W., Andel, T., Mcdonald, J., Jacobs, M., Campbell, M. & Mayr, J. (2015) ‘Compromising a Medical Mannequin’, 21st Americas Conference on Information Systems. Fajardo, Puerto Rico, 13-15 August.

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.

Halperin, D. et al. (2008) ‘Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses’, 2008 IEEE Symposium on Security and Privacy. Oakland, USA, 18-22 May. IEEE. 129-142.

Humphreys, E. (2008) Information security management standards: Compliance, governance and risk management. *Information Security Technical Report* 13(4): 247-255.

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.

Reese, K. et al. (2019) ‘A Usability Study of Five Two-Factor Authentication Methods’, Fifteenth Symposium on Usable Privacy and Security. California, USA, 12-13 August. USENIX Association.

Peer Response 1 – Charlotte

Further to Charlotte’s point, the medical industry’s historic lack of focus on cyber security does not just aid cyber criminals, it also attracts them (ENISA, 2015). Medical industry systems and devices are often seen as an easier target due to poor defences and the widespread use of legacy systems (Tervoort et al., 2020).

Whilst the WannaCry ransomware attack on the National Health Service (NHS) in 2017 was not aimed at unsupported software, the Microsoft Windows vulnerability was present in unsupported versions of the operating system, including Windows XP, and this was still in use in the NHS for critical medical devices (Smart, 2018). Fortunately, Mircrosoft released a Windows XP patch for this vulnerability in May 2017 despite ceasing support for this software in 2014 (Winder, 2020). Lessons learnt from the Wannacry attack include moving away from legacy Windows operating systems but this is still a work in progress after four years.

Another key recommendation from the NHS review was to improve accountability and leadership around cyber security all the way up to Board level. Active support and engagement with cyber security at a senior level is a key driver in ensuring consistent investment in cyber security as well as the establishment of security culture in a top-down fashion (Abraham et al., 2019).

References

Abraham, C., Chatterjee, D. & Sims, R. (2019) Muddling through cybersecurity: Insights from the U.S. healthcare industry. Business Horizons 62(4): 539-548.

ENISA (2015) Security and Resilience in eHealth. Available from: <https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services> [Accessed 11 May 2021].

Smart, W. (2018) *Lessons learned review of the WannaCry Ransomware Cyber Attack*. Available from: <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf> [Accessed 15 May 2021].

Tervoort, T., De Oliveira, M., Pieters, W., Van Gelder, P., Olabarriaga, S. & Marquering, H. (2020) Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review. *IEEE Access* 8: 84352-84361.

Winder, D. (2020) Are old operating systems putting the NHS at risk in 2020? Available from: <https://www.digitalhealth.net/2020/09/are-old-operating-systems-putting-the-nhs-at-risk-in-2020/> [Accessed 15 May 2021].

Peer Response 2 – Laura

Whilst Laura makes a good point regarding the use of an account lockout mechanism to protect accounts from brute force attacks, due consideration should be given to the impact of this control on availability to genuine users (Mohammed et al., 2017). The implementation of this control should be carefully considered based on the device. In the case of medical devices, there should be mechanisms in place for genuine users to be able to unlock the account quickly and safely (Kirushnaamoni, 2013). Utilising a timed lockout period or requiring administrator support to unlock a device could cause delays in treatment and may not be appropriate during a medical emergency (Khan & Sakamura, 2012).

References

Khan, M. & Sakamura, K. (2012) ‘Context-aware access control for clinical information systems’, *International Conference on Innovations in Information Technology (IIT)*. Abu Dhabi, United Arab Emirates, 18-20 March. IEEE. 123-128.

Kirushnaamoni, R. (2013) ‘Defenses to curb online password guessing attacks’, *International Conference on Information Communication and Embedded Systems (ICICES)*. Chennai, India, 21-22 February. IEEE.

Mohammed, M, Dagadzor, A., Effrim, B. & Appiah, K. (2017) Brute Force Attack Detection and Prevention on a Network using Wireshark Analysis. *International Journal of Engineering Sciences & Research Technology* 6(6): 26-37.

Summary Post

The two key cyber security threats to medical devices discussed in the paper were drawn out in the initial post: brute force attacks and denial of service attacks. Throughout this discussion, there has been support for a holistic approach to protecting devices from these threats through people, process, and technology.

Wilson (2021) reinforces the importance of training through pointing out that the majority of data breaches reported to the ICO have been attributed to human error. Whilst it is important to train medical professionals in how to securely manage these devices, Millward (2021) suggests it is also important to train patients as they are often the main user of the device. Wilson (2021) adds to this through suggesting that processes should be in place to ensure the users can not only identify issues with the device but also are aware of the proper channels for reporting them to avoid any unnecessary delay in resolution.

Whilst Luvaha (2021) makes a valid suggestion that devices should be protected from untrusted networks, it is not always possible to disconnect them entirely in order to prevent the risk. For example, medical staff may need remote access to implanted devices to be able to correct issues whilst avoiding the need for travel or surgery. In these circumstances, the suggestion from Wilson (2021) that technological solutions should be layered to ensure defence in depth may be a more suitable approach to protect devices. This suggestion also helps to reduce the risk of a breach if known weaknesses of technical solutions are exploited, for example in the case of sim swapping attacks on SMS-based two factor authentication (Johansen, 2019).

In conclusion, a holistic approach to securing medical devices should be adopted and standardised in the form of regulation to encourage consistent adherence to best practice across the industry (Martinez, 2018). This approach would not only protect patients but also deter attackers who view the medical industry as an easy target (Tervoort et al., 2020).

References

Johansen, A. (2019) SIM swap fraud explained and how to help protect yourself. Available from: <https://us.norton.com/internetsecurity-mobile-sim-swap-fraud.html> [Accessed 23 May 2021].

Luvaha, D. (2021) Initial Post. Available from: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=255292> [Accessed 23 May 2021].

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.

Millward, D. (2021) Initial Post. Available from: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=255292> [Accessed 23 May 2021].

Tervoort, T., De Oliveira, M., Pieters, W., Van Gelder, P., Olabarriaga, S. & Marquering, H. (2020) Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review. *IEEE Access* 8: 84352-84361.

Wilson, C. (2021) Initial Post. Available from: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=255292> [Accessed 23 May 2021].