Compromising a Medical Mannequin case study discussion summary

Given that cyber threats rise exponentially and due to the inherently sensitive nature of the medical field, it becomes apparent that devices like pacemakers, insulin pump systems, cochlear devices, and many more are also vulnerable to cyber-attacks.

This case study has been a great example of cybersecurity risks in the medical industry and became a stimulus for further research leading me to conclude that the medical sector has overlooked the cybersecurity part despite the stringent safety and approval protocols applying on these devices.

Key points :

- Implant devices' size and capacity set some unavoidable limitations regarding the resources and the security technics that can be implemented. Therefore, cryptography and authentication parts should be considered diversely and more efficiently.
- A wired connection for the setup or for changing parameters is not an option in most cases. That is the most critical vulnerability, which was also presented in the case study.
- The most challenging part is the equilibrium between security and accessibility. It is vital to get the best from both worlds to ensure that the health personnel will have the necessary access in the shortest period in case of emergency.
- Some innovative and promising research paradigms could constitute a solid framework for medical devices' security.
- The intrinsic bureaucracy character of the Health Industry is also an obstacle that has to be taken into consideration while at the same time new cyber threats emerge constantly.

Final Thought: The Medical Industry seems that will suffer more from the cyber-crime perpetrators in the coming years. Medical IoT and implant devices will be hackers playground, and the impact on human lives could be disastrous. This fact changes completely the priorities and the risks we have already faced. It is the human being under attack, and therefore the threat is upgraded to a whole different level.

Steve Morgan (2019), in his article "Patient Insecurity: Explosion Of The Internet Of Medical Things", cites some very stressful data, pointing out the magnitude of the problem in a very comprehensive way.

Reference:

Morgan, S., (2019) *Patient Insecurity: Explosion Of The Internet Of Medical Things*. Available from: https://cybersecurityventures.com/patient-insecurity-explosion-of-the-internet-of-medical-things/ [Accessed 23 June 2021].

(Original Post)

The “Compromising a Medical Mannequin” case study points out some security concerns regarding the critical Medical sector and the increasing emergency for measures against the constant increase of cybercrime events. Given the fact that medical devices nowadays incorporate and rely on technology, it becomes apparent that they are also prone to cybersecurity threats. This case study shows how some common security vulnerabilities could also have an impact on this critical sector.

The threats identified in this case study are affecting all CIA attributes (Confidentiality, Integrity, Availability). Specifically, due to the inherent need for wireless communication that implantable devices embody, common security issues related to wireless technology are also present. Therefore, the wireless connection poses the most significant vulnerability.

In this specific case study, some widespread wireless vulnerabilities were exploited:

1)The Wifi Protected Setup (WPS) vulnerability

2) Wifi de-authentication vulnerability

HPING3 and Reaver tools were utilised to perform the attack, but similar results could also be achieved using alternatives like aircrack-ng and wifite. (OffSec Services Limited, 2017)

Regarding the threats identified in this case study, the following table is matching the CIA properties with potential threats:

CIA property	Normal Use	Possible Threat (Abuse case)
Confidentiality	Patient’s Data and vitals’ information are accessible while using the appropriate software and the dedicated device for receiving data (receiver)	A malicious user could eavesdrop on the implant’s transmission and extract sensitive information about the patient’s health status and personal data either by using an identical receiver or not.
Integrity	An authorised handler can make the appropriate changes when the patient’s data deviate from the expected values.	Due to the limited amount of security that these devices incorporate are prone to tampering(Zheng et al., 2017). Therefore, there is a high possibility of intentional value change, causing even death to the targeted individual.
Availability	The devices are manufactured with unique elements that are corrosion-resistant, and they are designed to operate flawlessly for a specific time (Altawy et al. 2016)	In the same fashion, the malicious user can use known wireless vulnerabilities to send a significant number of requests, disrupting the connection and stop the service.

Even though this case study did not mention remote access to the device via the internet, in case that this service takes place, further analysis is needed, and common web application vulnerabilities have to be assessed in addition.

Before suggesting measures to mitigate the vulnerabilities mentioned above, we have to consider some limitations regarding the Health Industry and the implanting devices nature:

a) Advanced security measures could be proved dangerous in case of emergency.

For example, if a patient has a very secure pacemaker device with robust cryptography or a unique programmer to communicate; How secure would the device be proved if this patient was away from his doctor and immediate access to the device were needed?

b) Implant devices have some limitations regarding volume, weight and life expectancy. Hence, we have to admit that the resources (i.e., CPU, battery) cannot carry out advanced and demanding tasks similar to a personal computer.

c) Compatibility is also a big challenge, especially when different manufacturers are involved. To make things worse, even if the manufacturer were the same, backwards compatibility would be a challenging issue.

d) Bureaucracy in Health Industry is also a factor that has to be taken into account. Changes and innovations in this field demand several years of testing and compliance before they become approved. (Altawy et al. 2016)

Measures and Mitigations:

1) WPS or any similar technology that facilitates easy access to the device should be disabled. If this service deemed necessary for any reason, a longer and more complex password should be used instead of a single pin.

2) Hei & Du (2011) have proposed a two-level access control, utilising biometrics (i.e., iris. height, fingerprint) that seems to mitigate the devices computational limitations (partial biometric data) whereas, the security level increases significantly. The proposed model suggests that the patient's biometrics have to be inserted into the device before the implantation. In this way, biometrics become the credentials that give access to the device even if the individual is unconscious. The first level gives lightweight access in emergencies, whereas the second one is the most effective and requires an iris scan to proceed.

This model or something similar could be a good step in the right direction by minimizing the proximity needed for access, also combining biometrics to enhance security.

3) Add a shutdown command after the session expires (Marin et al., 2016). Although this measure's effectiveness is limited, it could add some value to the security process by putting the implant device to sleep mode and, therefore, not easily reachable from a potential attacker.

4) Frequent personnel security training. Medical staff should become familiar with cybersecurity issues by raising awareness and enhancing the security mindset.

References:

Altawy, R. & Youssef, A.M. (2016) Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. *IEEE Access*, 4, pp.959–979. Available from: https://doi.org/10.1109/ACCESS.2016.2521727.

Glisson, W.B., Mcdonald, T., Campbell, M., Andel, T., Jacobs, M. & Mayr, J. (2014) Compromising a Medical Mannequin. (2012), pp.1–11.

Hei, X.& Du, X.(2011) Biometric-based two-level secure access control for Implantable Medical Devices during emergencies. *Proceedings - IEEE INFOCOM*, pp.346–350. Available from: https://doi.org/10.1109/INFCOM.2011.5935179.

Marin, E., Singelée, D., Garcia, F.D., Chothia, T., Willems, R. & Preneel, B. (2016) On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them. *ACM International Conference Proceeding Series*. 5-9-December, pp.226–236. Available from: https://doi.org/10.1145/2991079.2991094.

OffSec Services Limited (N.D.) Kali Linux Tools Listing | Penetration Testing Tools. *Tools.Kali.org*. Available from: https://tools.kali.org/ [Accessed 10 May 2021].

Zheng, G., Zhang, G., Yang, W., Valli, C., Shankaran, R. & Orgun, M.A. (2017) From WannaCry to WannaDie: Security trade-offs and design for implantable medical devices. *2017 17th International Symposium on Communications and Information Technologies, ISCIT 2017*, pp.1–5. Available from: https://doi.org/10.1109/ISCIT.2017.8261228.