**Tutor's comment (Dr Nawaz Khan) for Discussion 1 :**

*"Advanced security measures could be proved dangerous in case of emergency."*

Hi Spiros,

This is great work and you demonstrated your good research on the topic. I particularly liked the table where you identified the threats.
You have made a good point in the statement above and I agree. So you are suggesting there should be a balance, does it mean we are compromising the threats?

Regards
Nawaz

**Comment from Anrich Potgieter for Discussion 1 :**

Hi Spiros,

Thank you for your wonderfully formatted post; I thoroughly enjoyed reading your response to the questions, along with how you integrated the CIA triad with the threats matched against the definitions.

I was particularly interested in your reflection regarding the physical limitations of medically implanted devices, which led me to explore these devices' security further.

Frighteningly I discovered that due to the limitations in powering medically implanted devices, encryption is often disabled to save power (Bu, Karpovsky and Kinsy, 2019).

The batteries that power these implants are replaced surgically, which have led to poor decisions regarding the security of the device.

All medical manufacturers should be mandated to follow the IEEE 802.15.6 standards for wireless body area networks in an ideal world. These standards provide stringent guidelines for implementing security on an implanted device that communicates wirelessly with a programming console ('IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks,' 2012).

According to IEEE 802.15.6, a wireless body area network should include MAC level authentication with AES-128 bit encryption; if the power limitations can be navigated, these would provide a much broader attack surface for potential intruders.

I trust that the rapid innovation culture we find ourselves in will fuel a new wave of innovation in this sector that will ultimately protect the lives of those who need these life-saving devices.

**References**

Bu, L., Karpovsky, M. G. and Kinsy, M. A. (2019) 'Bulwark: Securing implantable medical devices communication channels', Computers & Security, 86, pp. 498-511.

'IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks', (2012) IEEE Std 802.15.6-2012, pp. 1-271.

**Comment from Samuel Tselapedi for Discussion 1 :**

The intended goal of security solutions built around implantable (IMD) medical devices is to protect patient's sensitive data and the device's resources (Rathore et al., 2017). The following security properties should be what implantable medical devices should aim to inherently feature:

| Security Feature | Intended Goal | Technology Solution |
|---|---|---|
| Confidentiality. | The information exchanged with the IMD should be concealed from unauthorised access. | Cryptography protects data from unauthorised access and disclosure(O'Reilly Media, 2021). |
| Integrity | To protect the data processed by the IMD and exchanged with the IMD, a more robust authentication mechanism that protects the data from illegal alteration is required | Through the usage of hashing algorithms and message digest, cryptography ensures the integrity and accuracy of information (O'Reilly Media, 2021) |
| Availability | The objective of implanting a medical device in the body is to provide vital functions that the body has lost the ability to perform. Thus, the device must be available for remote access of the patient to the doctor. The doctor should have access to perform required operations when required. | Authentication is a technique used to authenticate a claimed identity.<br><br>Authentication ensures that the data or system is accessible to the authenticate subjects.<br><br>Nonetheless, authentication alone is insufficient to control authenticated subject ability to modify data or system without being authorised to do so. Authorisation as an additional layer of protection determines the subject's privileges on accessing the object (Martin, 2019). |
| Accountability | Nonrepudiation is the assurance that every transaction can be proven to have been performed by a specific subject on a specific object. A party to a contract or communication cannot repudiate the authenticity of their signature on a document or send a message that they originated. | On the internet, a digital signature is a mechanism used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature (TechTarget, 2008). |

**References:**


Martin, J. A. (2019) *What is access control? A key component of data security | CSO Online*. Available at: https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html (Accessed: 26 May 2021).

O'Reilly Media (2021) *The Role of Cryptography in Information Security - CISSP For Dummies, 4th Edition [Book]*. Available at: https://www.oreilly.com/library/view/cissp-for-dummies/9781118417102/a2_13_9781118362396-ch08.html (Accessed: 25 May 2021).

Rathore, H. et al. (2017) 'A review of security challenges, attacks and resolutions for wireless medical devices', *2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC 2017*, (June), pp. 1495–1501. doi: 10.1109/IWCMC.2017.7986505.

TechTarget (2008) *What is nonrepudiation? - Definition from WhatIs.com*. Available at: https://searchsecurity.techtarget.com/definition/nonrepudiation (Accessed: 26 May 2021).