University of Essex | Online

Medical Mannequin: Peer Responses

Course: MSc Computer Science

Module: Network and Information Security Management

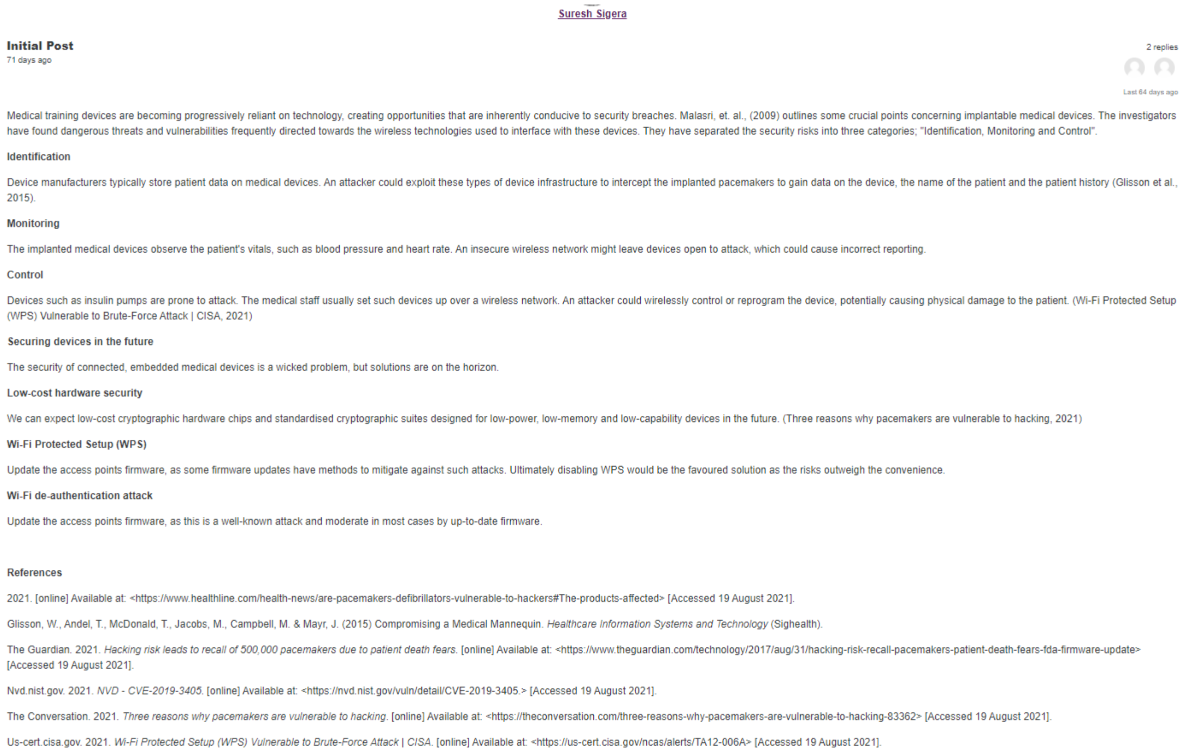
Assignment: ePortfolio

Date: Saturday 30th October 2021

Student ID: 126853

Peer Response 1:

In response to:



Suresh Sigera

Initial Post

71 days ago

2 replies

Last 64 days ago

Medical training devices are becoming progressively reliant on technology, creating opportunities that are inherently conducive to security breaches. Malasri, et. al., (2009) outlines some crucial points concerning implantable medical devices. The investigators have found dangerous threats and vulnerabilities frequently directed towards the wireless technologies used to interface with these devices. They have separated the security risks into three categories; "Identification, Monitoring and Control".

Identification

Device manufacturers typically store patient data on medical devices. An attacker could exploit these types of device infrastructure to intercept the implanted pacemakers to gain data on the device, the name of the patient and the patient history (Glisson et al., 2015).

Monitoring

The implanted medical devices observe the patient's vitals, such as blood pressure and heart rate. An insecure wireless network might leave devices open to attack, which could cause incorrect reporting.

Control

Devices such as insulin pumps are prone to attack. The medical staff usually set such devices up over a wireless network. An attacker could wirelessly control or reprogram the device, potentially causing physical damage to the patient. (Wi-Fi Protected Setup (WPS) Vulnerable to Brute-Force Attack | CISA, 2021)

Securing devices in the future

The security of connected, embedded medical devices is a wicked problem, but solutions are on the horizon.

Low-cost hardware security

We can expect low-cost cryptographic hardware chips and standardised cryptographic suites designed for low-power, low-memory and low-capability devices in the future. (Three reasons why pacemakers are vulnerable to hacking, 2021)

Wi-Fi Protected Setup (WPS)

Update the access points firmware, as some firmware updates have methods to mitigate against such attacks. Ultimately disabling WPS would be the favoured solution as the risks outweigh the convenience.

Wi-Fi de-authentication attack

Update the access points firmware, as this is a well-known attack and moderate in most cases by up-to-date firmware.

References

2021. [online] Available at: <https://www.healthline.com/health-news/are-pacemakers-defibrillators-vulnerable-to-hackers#The-products-affected> [Accessed 19 August 2021].

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. *Healthcare Information Systems and Technology* (Sighealth).

The Guardian. 2021. *Hacking risk leads to recall of 500,000 pacemakers due to patient death fears.* [online] Available at: <https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update> [Accessed 19 August 2021].

Nvd.nist.gov. 2021. *NVD - CVE-2019-3405.* [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2019-3405.> [Accessed 19 August 2021].

The Conversation. 2021. *Three reasons why pacemakers are vulnerable to hacking.* [online] Available at: <https://theconversation.com/three-reasons-why-pacemakers-are-vulnerable-to-hacking-83362> [Accessed 19 August 2021].

Us-cert.cisa.gov. 2021. *Wi-Fi Protected Setup (WPS) Vulnerable to Brute-Force Attack | CISA.* [online] Available at: <https://us-cert.cisa.gov/ncas/alerts/TA12-006A> [Accessed 19 August 2021].

Post:

"The implanted medical devices observe the patient's vitals, such as blood pressure and heart rate. An insecure wireless network might leave devices open to attack, which could cause incorrect reporting."

Hi Suresh,

You raise some excellent points regarding IMD's (Implantable Medical Devices), including Insulin Pumps and Pacemakers, as well as the security surrounding these devices.

Such devices are often programmed/checked with hand-held devices (Communicating via Bluetooth), which are often connected to a wider network using WiFi, leaving them susceptible to attack (Clery, 2015). This, combined with the low frequency of regular firmware updates due to the high risk, leaves the devices open to malicious actions from criminals. For example, the FDA has performed a recall of up to 4,000 devices in the US manufactured by Medtronic, citing security concerns (FDA, 2019).

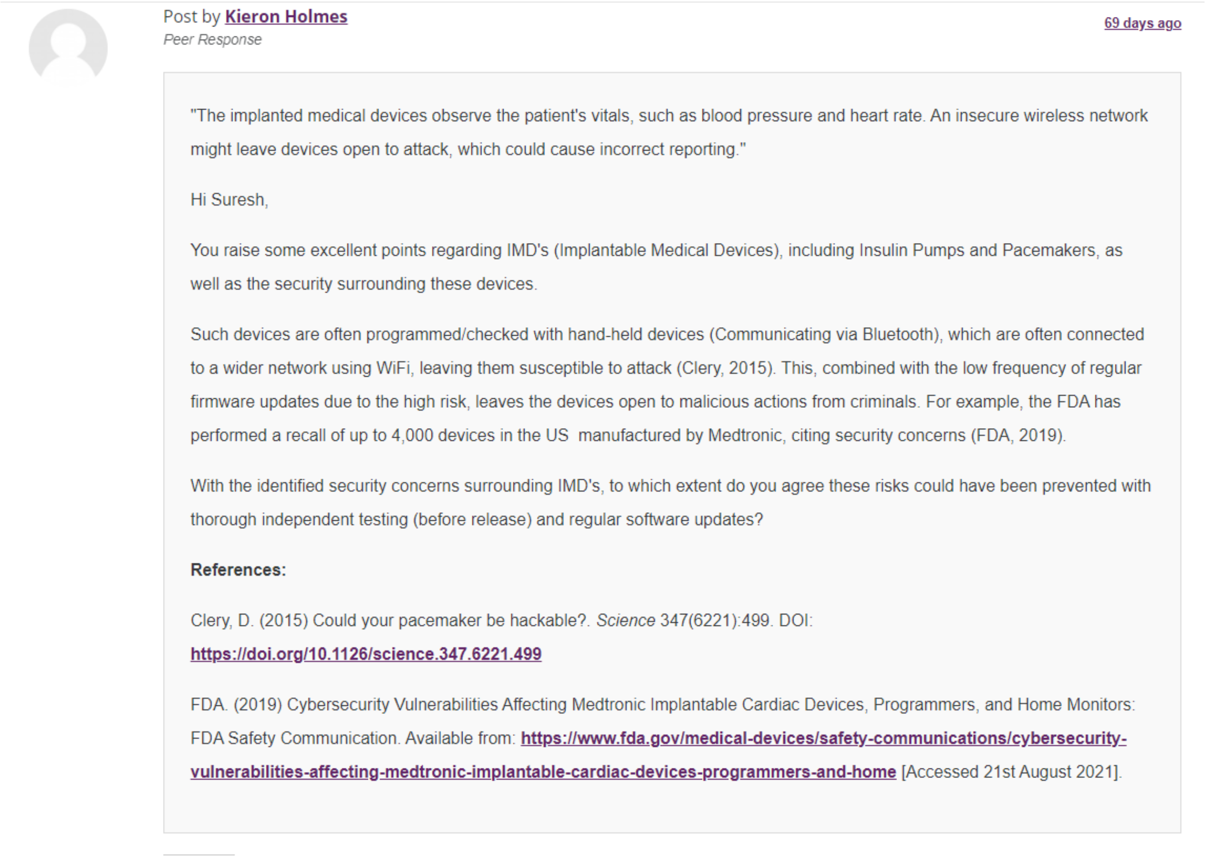
With the identified security concerns surrounding IMD's, to which extent do you agree these risks could have been prevented with thorough independent testing (before release) and regular software updates?

References:

Clery, D. (2015) Could your pacemaker be hackable?. Science 347(6221):499. DOI: https://doi.org/10.1126/science.347.6221.499

FDA. (2019) Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication. Available from: https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home [Accessed 21st August 2021].

Screenshot:



Post by **Kieron Holmes**

Peer Response

69 days ago

"The implanted medical devices observe the patient's vitals, such as blood pressure and heart rate. An insecure wireless network might leave devices open to attack, which could cause incorrect reporting."

Hi Suresh,

You raise some excellent points regarding IMD's (Implantable Medical Devices), including Insulin Pumps and Pacemakers, as well as the security surrounding these devices.

Such devices are often programmed/checked with hand-held devices (Communicating via Bluetooth), which are often connected to a wider network using WiFi, leaving them susceptible to attack (Clery, 2015). This, combined with the low frequency of regular firmware updates due to the high risk, leaves the devices open to malicious actions from criminals. For example, the FDA has performed a recall of up to 4,000 devices in the US manufactured by Medtronic, citing security concerns (FDA, 2019).

With the identified security concerns surrounding IMD's, to which extent do you agree these risks could have been prevented with thorough independent testing (before release) and regular software updates?

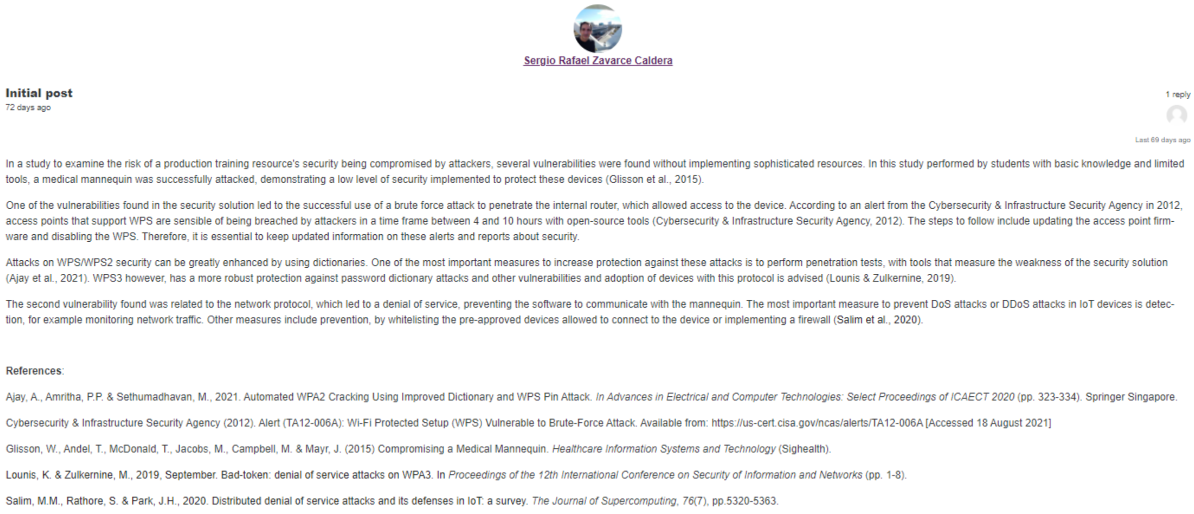
References:

Clery, D. (2015) Could your pacemaker be hackable?. *Science* 347(6221):499. DOI: **https://doi.org/10.1126/science.347.6221.499**

FDA. (2019) Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication. Available from: **https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home** [Accessed 21st August 2021].

Peer Response 2:

In response to:



Sergio Rafael Zavarce Caldera

Initial post

72 days ago

1 reply

Last 69 days ago

In a study to examine the risk of a production training resource's security being compromised by attackers, several vulnerabilities were found without implementing sophisticated resources. In this study performed by students with basic knowledge and limited tools, a medical mannequin was successfully attacked, demonstrating a low level of security implemented to protect these devices (Glisson et al., 2015).

One of the vulnerabilities found in the security solution led to the successful use of a brute force attack to penetrate the internal router, which allowed access to the device. According to an alert from the Cybersecurity & Infrastructure Security Agency in 2012, access points that support WPS are sensible of being breached by attackers in a time frame between 4 and 10 hours with open-source tools (Cybersecurity & Infrastructure Security Agency, 2012). The steps to follow include updating the access point firmware and disabling the WPS. Therefore, it is essential to keep updated information on these alerts and reports about security.

Attacks on WPS/WPS2 security can be greatly enhanced by using dictionaries. One of the most important measures to increase protection against these attacks is to perform penetration tests, with tools that measure the weakness of the security solution (Ajay et al., 2021). WPS3 however, has a more robust protection against password dictionary attacks and other vulnerabilities and adoption of devices with this protocol is advised (Lounis & Zulkernine, 2019).

The second vulnerability found was related to the network protocol, which led to a denial of service, preventing the software to communicate with the mannequin. The most important measure to prevent DoS attacks or DDoS attacks in IoT devices is detection, for example monitoring network traffic. Other measures include prevention, by whitelisting the pre-approved devices allowed to connect to the device or implementing a firewall (Salim et al., 2020).

References:

Ajay, A., Amritha, P.P. & Sethumadhavan, M., 2021. Automated WPA2 Cracking Using Improved Dictionary and WPS Pin Attack. *In Advances in Electrical and Computer Technologies: Select Proceedings of ICAECT 2020* (pp. 323-334). Springer Singapore.

Cybersecurity & Infrastructure Security Agency (2012). Alert (TA12-006A): Wi-Fi Protected Setup (WPS) Vulnerable to Brute-Force Attack. Available from: https://us-cert.cisa.gov/ncas/alerts/TA12-006A [Accessed 18 August 2021]

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. *Healthcare Information Systems and Technology* (Sighealth).

Lounis, K. & Zulkernine, M., 2019, September. Bad-token: denial of service attacks on WPA3. In *Proceedings of the 12th International Conference on Security of Information and Networks* (pp. 1-8).

Salim, M.M., Rathore, S. & Park, J.H., 2020. Distributed denial of service attacks and its defenses in IoT: a survey. *The Journal of Supercomputing*, *76*(7), pp.5320-5363.

Post:

"The most important measure to prevent DoS attacks or DDoS attacks in IoT devices is detection, for example monitoring network traffic."

Hi Sergio,

Great post, which covers a wide variety of preventative measures which can be undertaken to prevent the failures identified within the Medical Mannequin scenario.

Regarding the above point surrounding DoS and DDoS attacks, I agree with your statement that the first step of preventing such attacks is detection. However, it is worth considering that in this case, that the attack performed was not a conventional DoS attack; therefore preventative measures would be slightly different.

Typical DoS attacks intend to make a resource inaccessible to its intended users, often using attack types such as IMCP Flooding, SYN Flooding and Buffer Overflow Attacks (Palo Alto Networks, n.d.). Whereas, the demonstrated form of DoS attack relies on close-proximity spoofing, where "deauthentication" packets are sent to the router, forcing the disconnection of devices (Brandon, 2018).

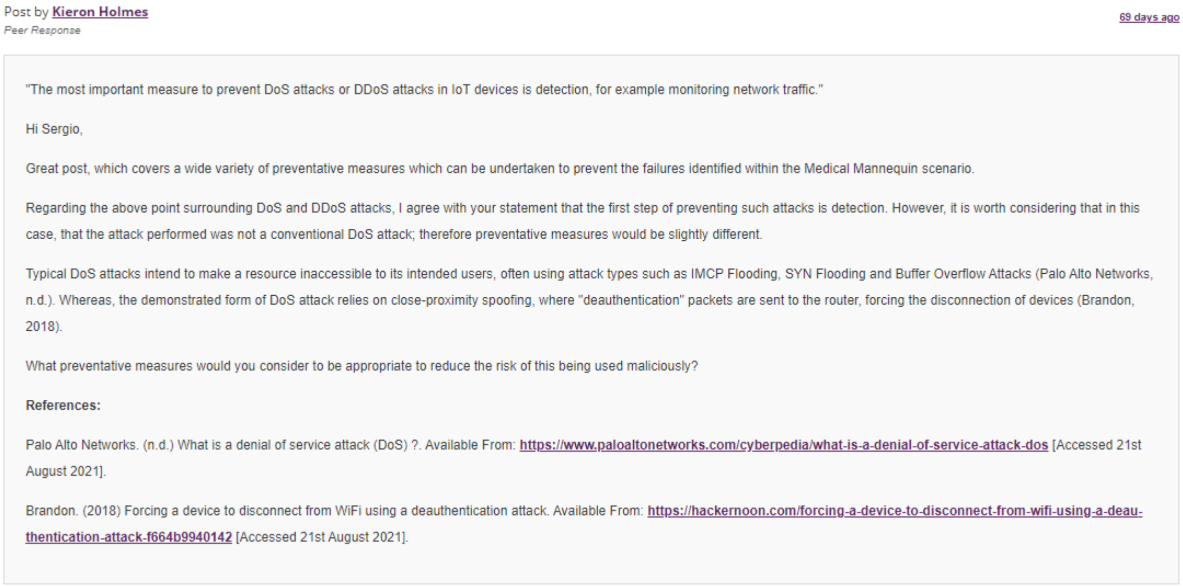
What preventative measures would you consider to be appropriate to reduce the risk of this being used maliciously?

References:

Brandon. (2018) Forcing a device to disconnect from WiFi using a deauthentication attack. Available From: https://hackernoon.com/forcing-a-device-to-disconnect-from-wifi-using-a-deauthentication-attack-f664b9940142 [Accessed 21st August 2021].

Palo Alto Networks. (n.d.) What is a denial of service attack (DoS) ?. Available From: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos [Accessed 21st August 2021].

Screenshot:



Post by **Kieron Holmes**

Peer Response

69 days ago

"The most important measure to prevent DoS attacks or DDoS attacks in IoT devices is detection, for example monitoring network traffic."

Hi Sergio,

Great post, which covers a wide variety of preventative measures which can be undertaken to prevent the failures identified within the Medical Mannequin scenario.

Regarding the above point surrounding DoS and DDoS attacks, I agree with your statement that the first step of preventing such attacks is detection. However, it is worth considering that in this case, that the attack performed was not a conventional DoS attack; therefore preventative measures would be slightly different.

Typical DoS attacks intend to make a resource inaccessible to its intended users, often using attack types such as IMCP Flooding, SYN Flooding and Buffer Overflow Attacks (Palo Alto Networks, n.d.). Whereas, the demonstrated form of DoS attack relies on close-proximity spoofing, where "deauthentication" packets are sent to the router, forcing the disconnection of devices (Brandon, 2018).

What preventative measures would you consider to be appropriate to reduce the risk of this being used maliciously?

References:

Palo Alto Networks. (n.d.) What is a denial of service attack (DoS) ?. Available From: **https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos** [Accessed 21st August 2021].

Brandon. (2018) Forcing a device to disconnect from WiFi using a deauthentication attack. Available From: **https://hackernoon.com/forcing-a-device-to-disconnect-from-wifi-using-a-deauthentication-attack-f664b9940142** [Accessed 21st August 2021].