University of Essex | Online

Medical Mannequin: Summary Post

Course: MSc Computer Science

Module: Network and Information Security Management

Assignment: ePortfolio

Date: Wednesday 22nd September 2021

Student ID: 126853

Post:

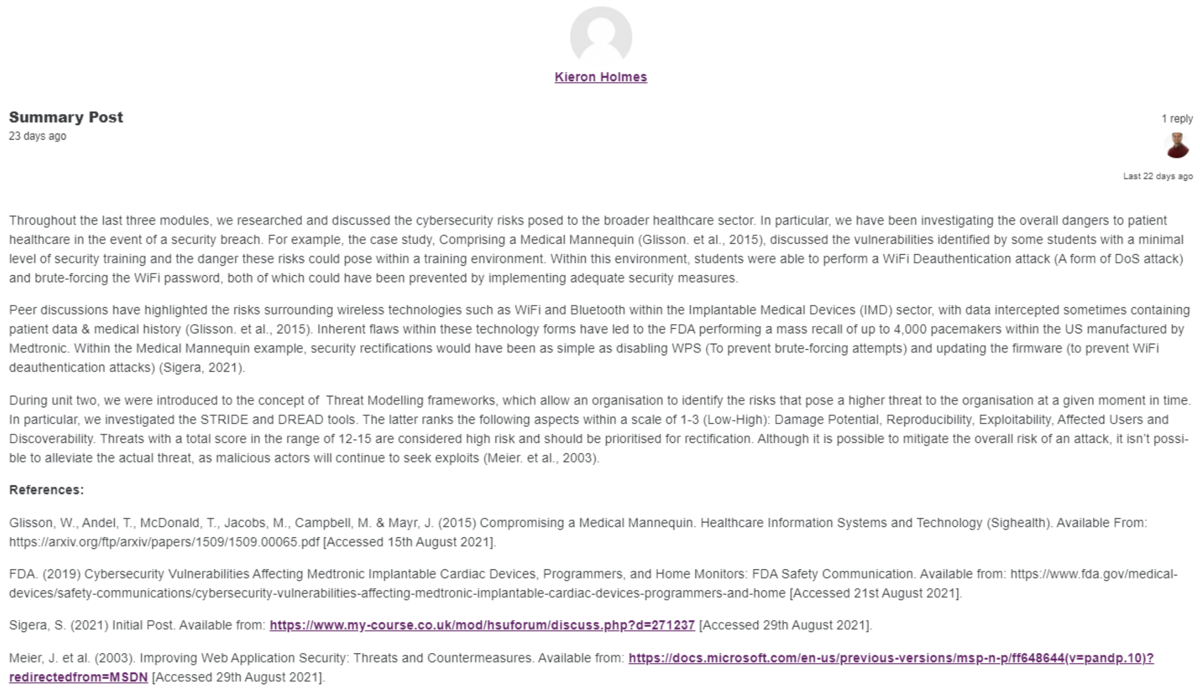
Throughout the last three modules, we researched and discussed the cybersecurity risks posed to the broader healthcare sector. In particular, we have been investigating the overall dangers to patient healthcare in the event of a security breach. For example, the case study, Comprising a Medical Mannequin (Glisson. et al., 2015), discussed the vulnerabilities identified by some students with a minimal level of security training and the danger these risks could pose within a training environment. Within this environment, students were able to perform a WiFi Deauthentication attack (A form of DoS attack) and brute-forcing the WiFi password, both of which could have been prevented by implementing adequate security measures.

Peer discussions have highlighted the risks surrounding wireless technologies such as WiFi and Bluetooth within the Implantable Medical Devices (IMD) sector, with data intercepted sometimes containing patient data & medical history (Glisson. et al., 2015). Inherent flaws within these technology forms have led to the FDA performing a mass recall of up to 4,000 pacemakers within the US manufactured by Medtronic. Within the Medical Mannequin example, security rectifications would have been as simple as disabling WPS (To prevent brute-forcing attempts) and updating the firmware (to prevent WiFi deauthentication attacks) (Sigera, 2021).

During unit two, we were introduced to the concept of Threat Modelling frameworks, which allow an organisation to identify the risks that pose a higher threat to the organisation at a given moment in time. In particular, we investigated the STRIDE and DREAD tools. The latter ranks the following aspects within a scale of 1-3 (Low-

High): Damage Potential, Reproducibility, Exploitability, Affected Users and Discoverability. Threats with a total score in the range of 12-15 are considered high risk and should be prioritised for rectification. Although it is possible to mitigate the overall risk of an attack, it isn’t possible to alleviate the actual threat, as malicious actors will continue to seek exploits (Meier. et al., 2003).

Screenshot:



Kieron Holmes

Summary Post

23 days ago

1 reply

Last 22 days ago

Throughout the last three modules, we researched and discussed the cybersecurity risks posed to the broader healthcare sector. In particular, we have been investigating the overall dangers to patient healthcare in the event of a security breach. For example, the case study, Comprising a Medical Mannequin (Glisson. et al., 2015), discussed the vulnerabilities identified by some students with a minimal level of security training and the danger these risks could pose within a training environment. Within this environment, students were able to perform a WiFi Deauthentication attack (A form of DoS attack) and brute-forcing the WiFi password, both of which could have been prevented by implementing adequate security measures.

Peer discussions have highlighted the risks surrounding wireless technologies such as WiFi and Bluetooth within the Implantable Medical Devices (IMD) sector, with data intercepted sometimes containing patient data & medical history (Glisson. et al., 2015). Inherent flaws within these technology forms have led to the FDA performing a mass recall of up to 4,000 pacemakers within the US manufactured by Medtronic. Within the Medical Mannequin example, security rectifications would have been as simple as disabling WPS (To prevent brute-forcing attempts) and updating the firmware (to prevent WiFi deauthentication attacks) (Sigera, 2021).

During unit two, we were introduced to the concept of Threat Modelling frameworks, which allow an organisation to identify the risks that pose a higher threat to the organisation at a given moment in time. In particular, we investigated the STRIDE and DREAD tools. The latter ranks the following aspects within a scale of 1-3 (Low-High): Damage Potential, Reproducibility, Exploitability, Affected Users and Discoverability. Threats with a total score in the range of 12-15 are considered high risk and should be prioritised for rectification. Although it is possible to mitigate the overall risk of an attack, it isn't possible to alleviate the actual threat, as malicious actors will continue to seek exploits (Meier. et al., 2003).

References:

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. Healthcare Information Systems and Technology (Sighealth). Available From: https://arxiv.org/ftp/arxiv/papers/1509/1509.00065.pdf [Accessed 15th August 2021].

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].

Sigera, S. (2021) Initial Post. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=271237 [Accessed 29th August 2021].

Meier, J. et al. (2003). Improving Web Application Security: Threats and Countermeasures. Available from: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN [Accessed 29th August 2021].

References:

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].

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. Healthcare Information Systems and Technology (Sighealth). Available From: https://arxiv.org/ftp/arxiv/papers/1509/1509.00065.pdf [Accessed 15th August 2021].

Meier, J. et al. (2003). Improving Web Application Security: Threats and Countermeasures. Available from: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN [Accessed 29th August 2021].

Sigera, S. (2021) Initial Post. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=271237 [Accessed 29th August 2021].