Collaborative Discussion 1

Initial Post

Glisson et al conducted a proof-of-concept study to evaluate the potential security flaws exhibited in a medical simulation training model. The students partaking in the study managed to penetrate the security in place in 7 hours using a live cd brute force attack, and under 3 hours using a virtual machine brute force attack. Their denial-of-service attack was also successful.

The participants were able to gain access to the BIOS boot menu and force the pc to boot from the CD-ROM, thus bypassing the systems privileges. A simple method to mitigate against this attack would be to disable boot from cd and USB and enabling a BIOS password. This would prevent booting from a cd or USB and bypassing the OS (Haken, 2015).

The DDOS attack is best managed by constant logging and monitoring. The IT professional should always be on alert and detection measures active to mitigate the effects of this attack (Chakkaravarthy *et al.*, 2018). Research by Salim et al identified many convergent methods of detecting and preventing DDOS attacks, some of which include : firmware updates, firewalls, password education and others (Salim, Rathore and Park, 2020).

Of interest, is a study conducted on with regards to ventilation machines. As the covid pandemic has forced mass production of these machines, stringent security protocols were not always adhered to. As such, the study showed a flaw resulting in the attacker being able to simulate false respiratory vitals of patients connected to the ventilation machine. This machine is supposed to provide supplemental ventilation to patients when certain vital conditions are met, such as low blood Oxygen or decreased respiration. When the attacker falsified the vital signs, the ventilator did not provide the required ventilation, which could cause the death of patients. This is a catastrophic design flaw, which should be fixed with utmost urgency (Burke and Saxena, 2021).

Burke, G. and Saxena, N. (2021) ‘Cyber Risks Prediction and Analysis in Medical Emergency Equipment for Situational Awareness’.

Chakkaravarthy, S. S. *et al.* (2018) ‘Futuristic cyber-attacks’, *International Journal of Knowledge-Based and Intelligent Engineering Systems*, 22(3), pp. 195–204. doi: 10.3233/KES-180384.

Haken, I. (2015) ‘Bypassing Local Windows Authentication to Defeat Full Disk Encryption’,

Salim, M. M., Rathore, S. and Park, J. H. (2020) ‘Distributed denial of service attacks and its defenses in IoT: a survey’, *Journal of Supercomputing*. Springer US, 76(7), pp. 5320–5363. doi: 10.1007/s11227-019-02945-z.

Peer Response to David Bouret

Hi David, I agree with you regarding your suggestions relating to security around medical devices, however, I disagree that we should be minimizing the use of connected devices. I think we are at a point in time whereby connected devices are essential to innovation and treatment in the medical field.

Implantable medical devices have increased by 300-500% in 2018 alone (Yaqoob, Abbas and Atiquzzaman, 2019). The usability of these devices, have proven to be critical in illness management, such as:

- Automatic Insulin administration in diabetics
- Implantable pacemakers or defibrillators

These devices, when connected, allow medical professionals to monitor and administer treatment for their patients in real time, as opposed to only when the patient presents for follow up treatment. In addition, it allows for management modification as an when needed. It also provides invaluable data on the management of patients, and more insight into the illness processes which improves patient care for many other patients in the long term(Joung, 2013).

A significant issue is that most medical device companies rely on proprietary technology as opposed to open source systems, and as such security progress is hampered (Ransford *et al.*, 2014).

As such, I believe that instead of limiting device connectivity, we should be focusing on methods to improve security features so that these devices are immune from attack, or at the very least, mitigate against potential threats. This would only be possible by continuous monitoring and improvements in design and security advancements.

Joung, Y. H. (2013) 'Development of implantable medical devices: From an engineering perspective', *International Neurourology Journal*, 17(3), pp. 98–106. doi: 10.5213/inj.2013.17.3.98.

Ransford, B. *et al.* (2014) 'Design challenges for secure implantable medical devices', *Security and Privacy for Implantable Medical Devices*. IEEE, 9781461416746, pp. 157–173. doi: 10.1007/978-1-4614-1674-6_7.

Yaqoob, T., Abbas, H. and Atiquzzaman, M. (2019) 'Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review', *IEEE Communications Surveys Tutorials*, 21(4), pp. 3723–3768. doi: 10.1109/COMST.2019.2914094.

Peer Response to Suresh Sigera

Hi Suresh, you have raised a very important point pertaining to attackers gaining access to patients built in devices, such as insulin pumps.

In my research, I have found that the attacker may gain access to the dosage system and administer an incorrect dose of insulin for the patient. This may lead to hyperglycemia if more than the required dose is given, or hypoglycemia if less than the required dose is given. This may lead to a loss of consciousness, coma, or even death. I have also found that implantable defibrillators, which are used to administer a minute electrical shock to normalize a patient's cardiac rhythms, may be attacked, and forced to either withhold a shock in an emergency, or administer a shock when none is required, leading to cardiac damage or even death.

Most of the current research suggests regular audits, bug reporting and regular updates to prevent such an attack. Interestingly, a researcher suggested multifactor authentication, in the form of the patient's biometric data to prevent unauthorized access to the device (Pycroft and Aziz, 2018).

Due to the relative ease with which attackers may intercept wireless communications, a communications cloaker or IMD shield has been proposed. This is a device that the patient wears on their wrist, which acts as a gateway to the IMD. If authentication is perceived to be a threat, no access is granted. If the patient has an emergency, and the attending physician, who is not an authorized user requires immediate access to the patients IMD, the IMD shield may simply be taken of, and communication may be established bypassing authentication procedures. While this proposal relies on the patients constant wearing of the IMD shield, it provides consistent protection against wireless intrusions (Zheng *et al.*, 2017).

Pycroft, L. and Aziz, T. Z. (2018) 'Security of implantable medical devices with wireless connections: The dangers of cyber-attacks', *Expert Review of Medical Devices*. Taylor & Francis, 15(6), pp. 403–406. doi: 10.1080/17434440.2018.1483235.

Zheng, G. *et al.* (2017) 'Ideas and Challenges for Securing Wireless Implantable Medical Devices: A Review', *IEEE Sensors Journal*. IEEE, 17(3), pp. 562–576. doi: 10.1109/JSEN.2016.2633973.

Summary Post

Over the course of the discussion, my colleagues have made valid points relating to network security. We all agree that security of network devices should be of utmost importance.

Medical devices and equipment are particularly susceptible due to the fact that lives are at risk. Hospitals and clinics are far more likely to pay a ransom when people may die without the requisite clinical care (Williams and Woodward, 2015).

My colleague Suresh pointed out an alarming risk to implantable medical devices. Malfunctioning of these devices directly put the patient at risk.

In the COVID 19 era, where isolation and distance between people is key, more equipment is networked. As such, an estimated 6-fold increase in cyber-attacks were reported as a result of the covid pandemic (Burke and Saxena, 2021). Unsuitable security, largely due to fast and mass production of these devices, may lead vulnerable patients and hospitals without adequate protection from malicious actors (Burke and Saxena, 2021). Despite the required speedy production required, security must not be sacrificed. Pranggono and Arabo, 2021, detailed many instances where hospitals, healthcare workers or those seeking healthcare were targeted during the coronavirus pandemic (Pranggono and Arabo, 2021).

Vulnerability and risk assessments need to be regularly conducted, and updates continuously rolled out. Software developers should continue to incorporate security into their software development life cycle.

I feel that this is an ethical issue, whereby if security cannot be guaranteed, or at least a “best effort” made, the equipment should not be distributed.

Burke, G. and Saxena, N. (2021) ‘Cyber Risks Prediction and Analysis in Medical Emergency Equipment for Situational Awareness’.

Pranggono, B. and Arabo, A. (2021) ‘ COVID -19 pandemic cybersecurity issues ’, *Internet Technology Letters*, 4(2), pp. 4–9. doi: 10.1002/itl2.247.

Williams, P. A. H. and Woodward, A. J. (2015) ‘Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem’, *Medical Devices: Evidence and Research*, 8, pp. 305–316. doi: 10.2147/MDER.S50048.