Cyber Security Vulnerabilities in Biomedical Devices: A Hierarchical Layered Framework

Badrouchi, F., Aymond, A., Haerinia, M., Badrouchi, S., Selvaraj, D.F, Tavakolian K.,
Ranganathan, P., Sumathy Eswaran, Shree Ram Abayankar Balaji*
School of Electrical Engineering and Computer Science
University of North Dakota
Grand Forks, ND, USA

Introduction

In fall 2013, a team of elite security researchers known as “white hat hackers” were invited to the Mayo Clinic in Minnesota. They were given forty different medical devices and told to break into them any way they could in an effort to expose vulnerabilities. The team spent one week analyzing the devices and found that every device had backdoor access points making them vulnerable to unauthorized users. The hackers were able to access the devices’ control systems via generic default passwords and unsecured operating systems. After gaining access to the system, the hacker can launch a potentially lethal attacks, such as causing a medication infusion pump to over administer medication without alerting staff [1].

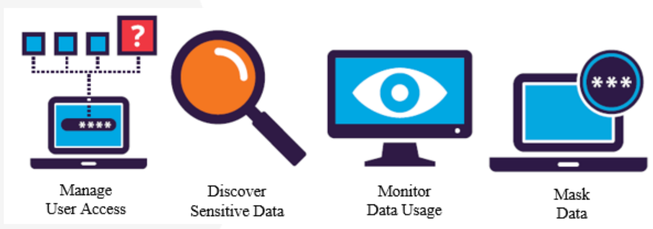

Fig 1. Cyber-Attack detection and prevention tools

Active Medical Devices Cyber-Attacks

Active medical devices rely on alternative source of power and some examples include Magnetic resonance imaging (MRI) scanners, defibrillators, and infusion pumps. These active devices are often connected to a hospital network which allows communication between the diverse devices on the network, including computers, mobile devices, imaging systems, and medication delivery systems. While this network improves the efficiency and continuity of health care, it also creates significant risks due to insufficient monitoring of the network security. Healthcare IT networks are much more vulnerable than other sectors, such as financial services or insurance companies [3].

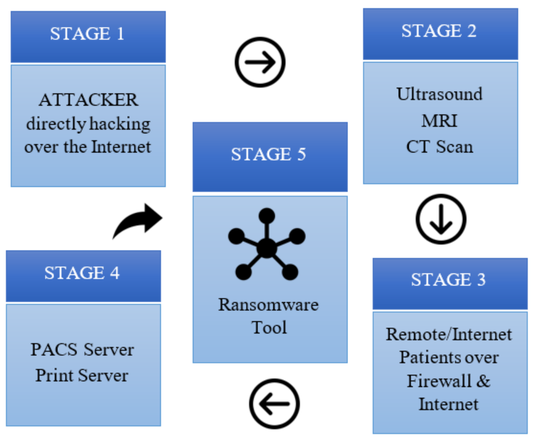

Fig 3. Medical device and hospital network cyber-attack anatomy

Attacker Malicious Activity	Consequences
Override magnetic field strength limit	Possible patient tissue burns. Possibility of damaging the machine
Disable alarms	Unawareness of dangerous conditions by technician
Reboot the machine	Delete configuration settings
Change information of display	Leads to a technician confusion to follow the protocol
Replace patient’s files	Wrongly sent diagnosis to a patient

Table 1 . Potential Cyber Attacks on MRI

Attacker Malicious Activity	Consequences
Alter air purge rate or purge process	Syringe line may contain air during therapy
Disable alarms	Unawareness of dangerous conditions by nurse
Reboot the pump	Delete configuration settings
Change information of display	Leads to a nurse confusion to follow the treatment process
Replace patient’s files	Wrongly delivered medication to a patient
Falsifying information on the dosage delivered	The equipment shows that the patient received the required dose however he did not

Table 2 . Potential Cyber Attacks on infusion pump

Conclusions

A three layered hierarchical framework categorizing the attack vectors of biomedical devices was discussed. Specifically, how the isolation of sensing, communication, and control layer framework in three medical devices as use cases: MRI unit, infusion pump, and implantable medical devices will help in mitigating the cyber-attack vectors was presented. A review of several literatures on possible cyber threats that can occur in biomedical devices was detailed in this chapter. Such a framework will help provide some isolation and lead time to thwart attacks, and enable in implementation of cyber-security policies in the intrusion detection systems or firewall units in health care organizations.

Overview of Existing Technologies

Medical devices have many forms and functions in modern health care. Some medical device such as pacemaker is used by an individual, whereas sphygmomanometer or infusion pump, is used clinically to assess and treat many people daily. Key security-relevant differences for these device usage scenarios are the amount of personal data stored in the device, sensitivity and quantity of data collected, and type or specificity of therapy delivered. Large clinical facilities have a much greater risk of information theft type attack for their electronic medical records and billing info, but may have fewer security concerns at the device level than do personal users. Hospital medical devices are de-identified to be used on many people, which lessens the risk of a personally targeted attack. However; personal devices and hospital devices are both susceptible to denial of service and improper functioning attacks, to be described further later in this chapter. Although the remainder of this chapter will predominately focus on personal medical devices, the security topics discussed are also relevant to devices used in a commercial setting.

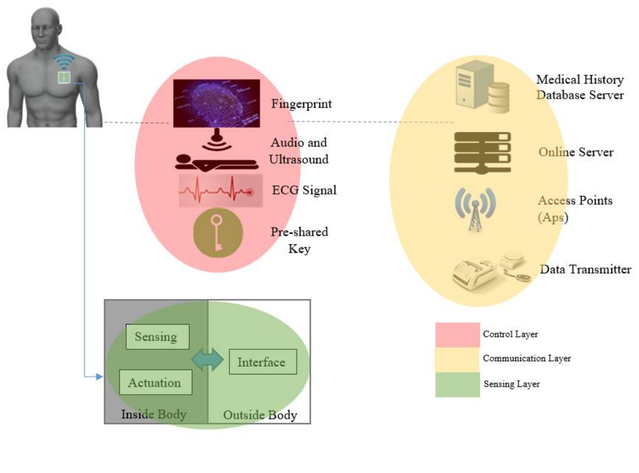

Fig. 2. Control, communication, and sensing layers in IMDs

A Hierarchical Layered Framework for Biomedical Devices

Biomedical devices are extremely diverse in complexity, connectivity, and implementation environment. Devices vary from an extremely large, stationary MRI machine to a small, implantable stimulator. Previously in this chapter, cybersecurity topics for biomedical devices have been discussed in general situations to allow the concepts to be applied to as many distinct devices as possible. Three specific examples of biomedical devices are now explored as case studies to further illustrate the cybersecurity concerns of real applications. Three devices considered further are i) MRI machine, ii) infusion pump, and iii) implanted pacemaker. Each of these devices will be examined using a three-layer architecture consisting of sensing, communication, and control layers.

Case Study

MRI Unit Cyber Attack

MRI units are one of several connected devices that can be attacked by hackers. By gaining access to the MRI unit, hackers can access patient’s files and protected information and even change the test procedure and parameters. The attack starts through the communication layer, which is generally the internet network, then the hacker can go laterally to gain access to the device’s different control layers.

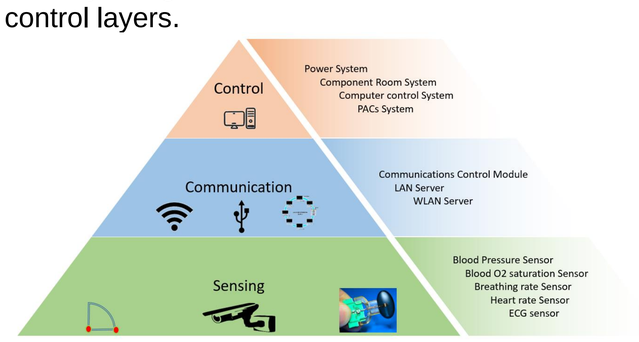

Fig: 4 Three layers in MRI unit.

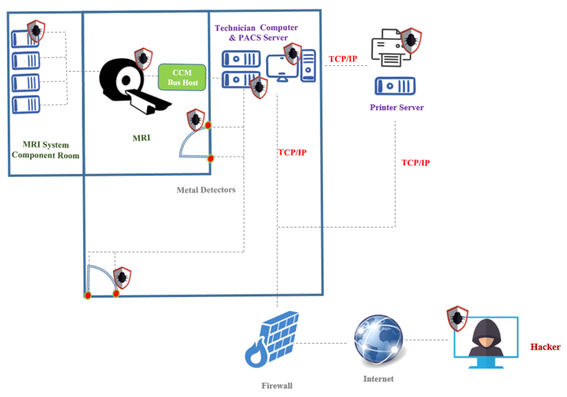

Fig: 5 Network diagram of an MRI unit.

Infusion Pump Cyber Attack

The components of an infusion pump that are relevant to cybersecurity can be classified into three layers: sensing, communication, and control. If an attacker is able to access one of these layers, he may then be able to spread the attack to the other layers.

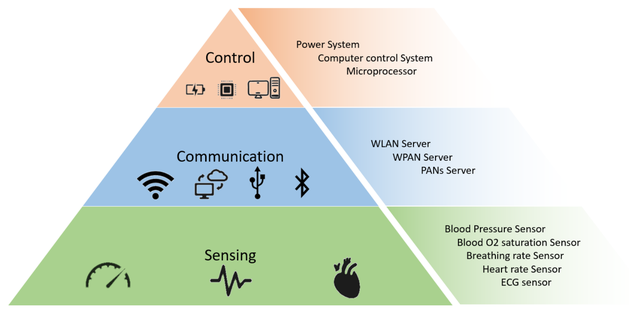

Fig: 6 Three layers in Infusion Pump.

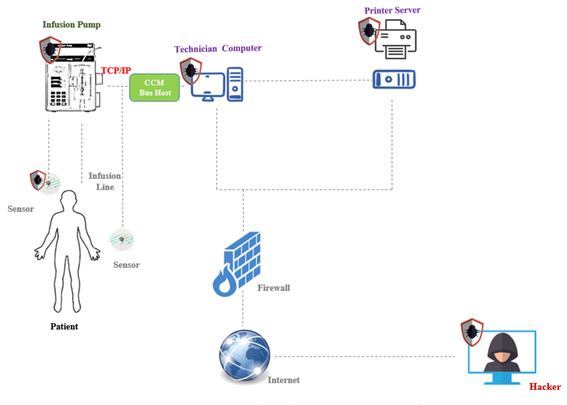

Fig: 7 Network diagram of an Infusion Pump unit.

References

[1] J. Robertson and M. Reel, “It’s Way Too Easy to Hack the Hospital,” 2015. [Online]. Available: https://www.bloomberg.com/features/2015-hospital-hack/. [Accessed: 14-Jul-2019].

[2] A. Schich, “Active medical devices,” 2019. [Online]. Available: https://www.med-cert.com/en_certification/en_medical-device/. [Accessed: 14-Jul-2019].

[3] TrapX Labs, “ANATOMY OF AN ATTACK MEDJACK (Medical Device Hijack),” 2015. [Online]. Available:. https://trapx.com/trapx-labs-report-anatomy-of-attack-medical-device-hijack-medjack/.

[4] FDA, “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,” 2014. [Online]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0. [Accessed: 14-Jul-2019].

Acknowledgements

Badrouchi, F., Aymond, A., Haerinia, M., Badrouchi, S., Selvaraj, D. F., Tavakolian, K., ... & Eswaran, S. (2020). Cybersecurity vulnerabilities in biomedical devices: A hierarchical layered framework. Internet of Things Use Cases for the Healthcare Industry, 157-184.

*Poster Designer(Non - Author)

Contact

Dr. Prakash Ranganathan
Director of Center for Cyber Security Research (C2SR) Associate Professor, IEEE Senior Member of Electrical Engineering College of Engineering & Mines University of North Dakota
prakash.ranganathan@UND.edu | 701.777.4431