Cybersecurity for Connected Diabetes Devices

Review Essay, Assignment 2

Pawan Kumar

CWID-10474820

Department of Computer Science, Stevens Institute of Technology

CS 573-A, Fundamentals of Cybersecurity

Dr. Edward Amoroso

May 2nd, 2022

Today, about 422 million people have diabetes worldwide, so the demand for diabetes devices like blood sugar monitors, and automatic insulin pumps is also increasing. These diabetes devices are increasingly connected wirelessly to each other, and to data-displaying reader devices. Threats to the accurate flow of information and commands may compromise the functionality of these devices and put their users at risk of health complications. To preserve the confidentiality, integrity, and availability of data and commands, connected diabetic devices must have strong cybersecurity. In this essay, we discuss what cybersecurity means for medical devices and especially what it means to diabetic devices, and also why sound cybersecurity is needed for diabetes devices. We will also see what are cyber-threats to connected diabetes devices and response to those cyber threats.

For medical devices cybersecurity means the protection of data and command information that are transmitted wirelessly between connected medical devices. These devices include blood glucose monitors, continuous glucose monitors (CGMs), insulin pumps, other wearable sensors, cloud computer systems, and readers, such as desktop computers, laptops, pads, smartphones, and watches. Diabetic medical devices contain a stream of patient personal information and can allow remote commands for data delivery, treatment instructions, and insulin administration. This personal information, as well as the software that provides the ability to transmit and receive remote commands, are all assets. Any threat to these assets will degrade their function and cause the user of diabetes devices a health risk. The threat can come in any form of unauthorized disclosure, modification, or loss of function. The goal of cybersecurity for connected diabetes devices is to secure these devices against unauthorized disclosure, alteration, and loss of functionality. Avoiding such disclosure preserves confidentiality, avoiding modification preserves the integrity, and avoiding loss of function preserves availability.

Jay Radcliffe, a security researcher analyst hacked an insulin pump 150 feet away to either disable the device or cause delivery of an overdose of insulin. He demonstrated this at a security conference in Las Vegas. For his demonstration, he required special hardware and a program he wrote to communicate with the device. He also required knowledge of the pump's six-digit identification (ID) number but he also said that this identification number can be obtained through social engineering or through software designed for brute-force guessing. The next example, the author has presented, will show how diabetes devices can be hacked even without knowing the identification number of the device. A research architect, Barnaby Jack wirelessly hacked into an insulin pump at a security conference in February 2012 in San Francisco without first knowing the device's ID number, which was placed in a see-through mannequin, from 300 feet away. He developed a scanner with a high-gain antenna to boost its range and then scanned the company-designated frequency for a pump, retrieved the target pump's ID and gained control. The author has remarkably presented these real examples to show how concerning these cyber threats are for connected diabetes devices.

Now, responding to these cyber threats to connected diabetes devices FDA and DHA are working together to prevent medical systems and implanted devices from being hacked. On June 13, 2013, the FDA issued a statement on the topic: "We recommend that manufacturers review their cyber-security practices and policies to assure that appropriate safeguards are in place to prevent unauthorized access or modification to their devices". On October 2, 2014, the FDA released important cybersecurity guidance titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices". This guidance clearly described guiding principles for sound cybersecurity practices and how to work with FDA to get products cleared when they contain cybersecurity features. A challenge for diabetes device developers is that although data must be protected, in many cases data are now intended to be made available to not only patients, but also relatives, health care providers, and hospitals. Patients

with diabetes have a special need for impeccable data fidelity when they access their current glucose levels, glucose trend data, predictive data, insulin dosing records, hypoglycemia alerts, blood pressure records, calorie information exercise records, and various reminders and timely notifications. Everything about the importance of robust cybersecurity that is true for medical devices, in general, is particularly true for diabetes devices. To address the aspect of the security of insulin pump systems, in 2011 Kohno, Paul, and the author reviewed the security of these devices. Kohno, Paul, and the author recommended five features that would lead to robust cybersecurity for these devices. These include (1) constant availability of access to systems; (2) confidentiality of information; (3) integrity without alteration of data; (4) authentication for privileged access; and (5) authorization of identity before execution of commands. In my opinion, these features presented by the author will definitely help in making these diabetes devices robust.

As a diabetic myself I can relate to these points mentioned by the author and I know how important are the readings of blood glucose monitor for a diabetic person. For people like me, who are diabetic, we take our insulin according to the readings of a blood glucose monitor and I totally agree with the author that if someone hacks into the glucose monitor and changed the readings then we will take insulin/medicine according to those false readings which may put our health at risk. Patients with diabetes have an extremely high need for secure information flow to display glucose information and deliver insulin dosing commands when sensor and actuator information is transmitted wirelessly through connected medical devices. Therefore, sound cybersecurity is needed for connected diabetes devices to maintain confidentiality, integrity, and availability of the data and commands. The author has mentioned in the paper and I agree that the best way to assure cybersecurity of diabetes devices is to both: (1) mandate a level of performance at the front end such that failure to attain this performance would lead to adverse regulatory or economic consequences; and (2) test the product in a post-market

surveillance program at the back end to ensure that the device is continuing to maintain its initial level of performance. A cybersecurity standard designed specifically for connected diabetes devices will improve the safety of these products and increase confidence of users that the products will be secure.

References

Cybersecurity for Connected Diabetes Devices by David C. Klonoff, MD, FACP,

FRCP (Edin), Fellow AIMBE

Google link of the paper: -

https://journals.sagepub.com/doi/10.1177/1932296815583334#:~:text=The%20purpose%20of%20cybersecurity%20for,loss%20of%20function%20preserves%20availability.