THE PENNSYLVANIA STATE UNIVERSITY

SCHREYER HONORS COLLEGE

COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY

HOW THE USE OF TWO-FACTOR AUTHENTICATION CAN LEAD TO ENHANCED SECURITY IN BLUETOOTH INSULIN PUMPS

EDWARD FITZPATRICK BURKE

SPRING 2023

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Cybersecurity Analytics and Operations

Reviewed and approved* by the following:
David Fusco, Ed.D.
Associate Teaching Professor in Information Sciences and Technology
Thesis Supervisor
Nicklaus A. Giacobe, Ph.D.
Associate Teaching Professor in Information Sciences and Technology
Honors Adviser

* Electronic approvals are on file.

ABSTRACT

Insulin pumps that are operated digitally through the internet are becoming more and more common. These are referred to as the Internet of Things (IoT) insulin pumps. These pumps are able to be digitally operated, allowing for greater ease of use by those who need them. However, because of their digital nature, IoT insulin pumps can be compromised by malicious hackers and leave the users of these pumps in potentially dangerous situations. If hackers gain unauthorized access to an IoT insulin pump, their actions could easily prove fatal for the pump user. Two-Factor Authentication is a security feature that requires users to validate their identity in two different types of manners. Two-Factor Authentication could allow for greater security for IoT Insulin pumps because it would ensure that the people accessing these pumps are legitimately the same people who are utilizing them.

Through conducting a research survey with respondents from both the professional and educational areas of Medical IoT devices, the practicality, usability, and relevance of the use of Two-Factor Authentication in insulin pumps were questioned. The survey inquired about the types of attacks that affect insulin pumps, what data could be stolen, what security implementations were already in place, and what concerns implementing such a method would bring. These responses were analyzed to determine if such a security feature was feasible for such devices. Through this research, it was determined that, despite a number of concerns regarding the feasibility of two-factor authentication, this implementation can be realistic. Overall, two-factor authentication could lead to a safer world for IoT insulin pump users.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to extend my special thanks to Professor David Fusco for serving as my Thesis Supervisor this year. His guidance and support were critical to my completing this thesis and I greatly appreciate his willingness to work with me.

I would also like to thank Professor Nicklaus Giacobe for serving as my Honors Advisor this past year, as well as my Capstone professor. His advice throughout the year greatly improved my understanding of the thesis submission process and allowed me to complete this thesis successfully.

Lastly, I would like to thank my family for their love and support throughout my entire college experience and through my thesis writing process. I could never have done this without them and I will always be grateful for everything they have done for me.

1.

Introduction

Today in the United States, over 350,000 people utilize insulin pumps to help treat their diabetes. These pumps are able to read how much glucose a person requires and inject it automatically into their bloodstream, preventing unnecessary complications with their health problems. Many of these IoT insulin pumps are also able to be controlled over Bluetooth or WiFi.

These Internet of Things (IoT) insulin pumps are able to record trends and patterns in a person's glucose needs. It is also able to record the glucose measurement device on a person's smartphone so that it can determine how much glucose a person needs at any given time. From here, it is able to send alerts to a person's phone regarding the need for an insulin injection. These features help improve the mobility and ease of use of insulin pumps as they help deal with chronic issues such as diabetes. While these features augment the capabilities of the insulin pumps due to their efficiency and accuracy, the added feature of the pump connecting to the phone via wifi or Bluetooth could lead to a potentially dangerous situation, including the pump being compromised by a malicious hacker.

Because of their lack of funding for cyber defense and because of the vulnerable data contained within hospital IT systems, hospitals are a highly targeted entity for cybercriminals. Many hackers attempt to threaten hospitals with malware attacks that would shut down their necessary systems which could lead to life-threatening situations. There was a heavy increase in these types of crimes as a result of the COVID-19 pandemic, starting in March 2020 (Horowitz,

Brian). Another heavy concern regarding this situation was that there was a heavy increase in hospital workers using their own personal devices to utilize IoT devices. This strategy of using bring-from-home devices to access private and sensitive information via IoT devices is a massive security concern. These personal devices can result in data breaches if they are not secure devices. (Basch, Corey) It can also make them more vulnerable to malware attacks such as Distributed Denial of Service (DDOS) attacks, phishing, and network breaches. Furthermore, these attacks are potentially life-threatening for insulin pump users. If a hacker decides to either withhold the insulin supply or inject it all at once, they could easily end the life of a pump user. This could be the result of a hacker's malicious intent, to fulfill a desire to kill their user, or to utilize this leverage for personal gains, such as blackmailing the pump user into paying them money, so that they will not kill the user.

The concept of a hacker taking control of an IoT pump is no longer theoretical. Such a stunt was perfumed at the notable cyber convention, Black Hat Technical Security Conference. This is an annual conference that features experienced hackers, who draw experience from ventures both legal and illegal (Ngak, Chanda). At the 2011 Black Hat Conference, Jerome Radcliffe, who is diabetic himself, held a presentation regarding how vulnerable people with his condition are to malicious hackers. Radcliffe, who is also a senior threat intelligence analyst for a notable computer security organization, discussed the two forms of a device he carries at all times: an insulin pump and a continuous glucose monitor. Radcliffe was able to reprogram the pump's remote to respond to the remote of a stranger. He was also able to use a commonly obtained USB to not only eavesdrop on the pump but to also tell the pump what to do. For this to occur, the attacker would theoretically need to be relatively close to the pump (about a couple

hundred feet). After further experimenting, Radcliffe was also able to take control of his glucose monitor, affecting the amount of insulin that the pump would calculate for injection. Such a miscalculation could easily prove fatal for a pump user. Radcliffe also did require the use of the pump's six-digit verification code. However, he also claimed that this could be obtained through brute force or social engineering tactics (Klonoff, David).

A potential solution to prevent these pumps from being infected by hackers is the implementation of two-factor authentication. This is a system where any person seeking to gain access to this pump and its controls has to have two forms to authenticate that they are the person who truly has access to the pump (password, phone call, biometric). This ensures that only individuals with access to the pump are able to control it. It also ensures that malicious hackers will not be able to easily take control of the pump through the use of a malware attack. This will ensure the greater safety of medical IoT pump users, so they do not find themselves at the mercy of a malicious hacker.

Purpose of the Research

As has been mentioned, over a third of a million people in the United States of America alone require some form of an insulin pump for medical reasons. These people need these insulin pumps to work both efficiently and accurately or they risk severe sickness or death as a result of insulin withdrawal or insulin overdose. This means that anyone using an IoT insulin pump requires both the pump itself and the network communication of the pump to their personal device to rely heavily on this system working properly. As a result of this, this vulnerable

community faces the threat of malicious hackers taking advantage of their conditions, either for monetary gain, or another sinister reason.

In general, healthcare entities (machines, hospitals, medical facilities) are the most common targets for cybercrime. This is mostly because these entities are vulnerable as a result of not having suitable funding to defend against cyber-attacks (more commonly, funding for medical entities is diverted elsewhere). In addition to this, hospitals have vulnerable patient information, which, if compromised, could be easily fatal for patients. They also utilize old and outdated equipment (which is often more easily hackable), and have a broad attack surface (Robinson, Phillip). Because of this, combined with the vulnerable nature of IoT insulin pumps, protecting them from malicious attacks and being able to thwart malware before it begins threatening the functionality of the pump is crucial in their safeguarding. With this understanding, this research and types of research like it are necessary to further the understanding of the protection of IoT medical devices. Because of the fairly new nature of these devices, there is little research or testing on pumps such as these, making security a difficult concept to test for them. Because of this, performing research of this nature is crucial to the greater development and understanding of the protection of Medical IoT devices.

Research Methodology

Given the type of data that the researcher was searching for to complete this thesis, it was decided that it would be best to collect data in the form of a survey. This would allow the researcher to collect data from a wide range of experienced persons in the field of medical Internet of Things devices (college professors, PHDs, and workers in both the private and public sectors). It would also be a way to avoid the time constraints of some of the other methods of

gaining data, as conducting interviews would be time-consuming and would require scheduling with multiple people. In addition to this, the survey respondents would be able to fill out the survey at their own convenience. For these reasons, the researcher decided that collecting research through a survey would be most efficient for the purposes of this research.

When the survey had been completed, it contained ten questions, both of an open nature and of a multiple-choice nature. These questions were wide regarding common attacks and malfunctions with insulin pumps. It also included the risk and security that comes with insulin pumps as well as the effect that COVID-19 Pandemic had on the MIoT world. The survey also included an open-ended question at the end of the survey asking the respondents if they had any knowledge of relevant research within the field of IoT insulin pumps. Below are the questions asked as part of the survey.

1. What type of attack have you seen to be most common when it comes to Mobile Internet of Things (MIoT) Devices? (MIM, DDOS, Logic Bomb, etc.)
2. What data could be obtained about a patient from a compromised pump?
3. What dangers would losing access to an insulin pump hold?
4. How could the implementation of security features possibly lead to complications in the pump's operations?
5. Has the COVID-19 Pandemic affected the MIoT World in terms of an increase of cyber-attacks?
6. What are your concerns about implementing two-way authentication for the enhancement of the security of these pumps?
7. What part of the pump has the highest potential to be compromised?

8. What security implementations are in place for standard MIoT Devices?

9. Could the benefits of the implementation of two-factor authentication outweigh any potential usage complications that come with the added security measures?

10. Is there any research currently in the works to prevent the use of malware against these devices?

11. If there is any other information that you would like to share regarding, Medical IoT devices, please share it here.

After initial preparations were completed for the survey, the researcher spent about a month collecting data by sending the survey to professors within the Penn State Community (both at University Park and a few of the nineteen Commonwealth Campuses of Penn State). The researcher also attempted to find survey respondents within the professional workforce, people who have experience with these devices through work experience. Many of these people were found on the popular professional social networking website, LinkedIn. After about a month of collecting data, the survey compiled seven quality responses, both from professors and people from LinkedIn. This allowed the researcher to obtain enough adequate data to being the coding process for this thesis.

After the researcher had gathered sufficient data to be able to effectively write the thesis, the researcher went about coding the responses that had been received on the survey. For this process, the researcher identified certain trends and consistencies that were present in the survey. Because of this, the researcher was able to draw meaningful conclusions from these trends. In addition to this, the researcher also worked to identify certain aspects between different questions. These included trends, consistencies, contradictions, and unexpected answers. These

findings are relevant to important aspects of the thesis, especially regarding the necessity, practicality, and reliability of the potential of two-factor authentication implementation in IoT insulin pumps. Furthermore, these trends will also allow the researcher to delineate a more complete understanding of the security and usability of medical IoT devices.

2.

The COVID-19 Pandemic's Affect on Healthcare Cybersecurity

When the COVID-19 Pandemic occurred in March 2020, the entire world was affected. This was especially true for the medical industry. Hospitals and medical centers experienced overflowing and understaffing, ventilators ran low, and certain medicines and medical supplies were hard to come by. Healthcare entities were one of the most heavily affected entities as a result of the COVID-19 Pandemic. This is even true from an information security standpoint when it comes to defending against cyber-attacks. Because of the vulnerability of hospitals and healthcare entities at the time, cybercriminals took full advantage of the situation. There was a 123% increase in ransomware attacks in the year 2020, affecting 18 million more patients, which is a 470% increase (Horowitz, Brian). These hackers stole 2.1 million dollars as a result of these ransomware attacks.

Hackers were able to take advantage of healthcare facilities directly as a result of the factors caused by the pandemic. According to Bill Conner, the CEO of the network security hardware vendor, SonicWall: "The pandemic—along with remote work, a charged political climate, record prices of cryptocurrency, and threat actors weaponizing cloud storage and tools—drove the effectiveness and volume of cyberattacks to new highs" (Horowitz, Brian). Because of the increase of virtual, online work, as well as the heavy increase of use in healthcare resources, healthcare-based entities made easy targets for ransomware schemes. In addition to this, internet-connecting hospital equipment is especially vulnerable to cyber-attacks because they tend to be outdated. In the span of the pandemic, much of this equipment was also vulnerable as a result of

it being overburdened throughout the pandemic, as a result of the increase of patients within hospitals.

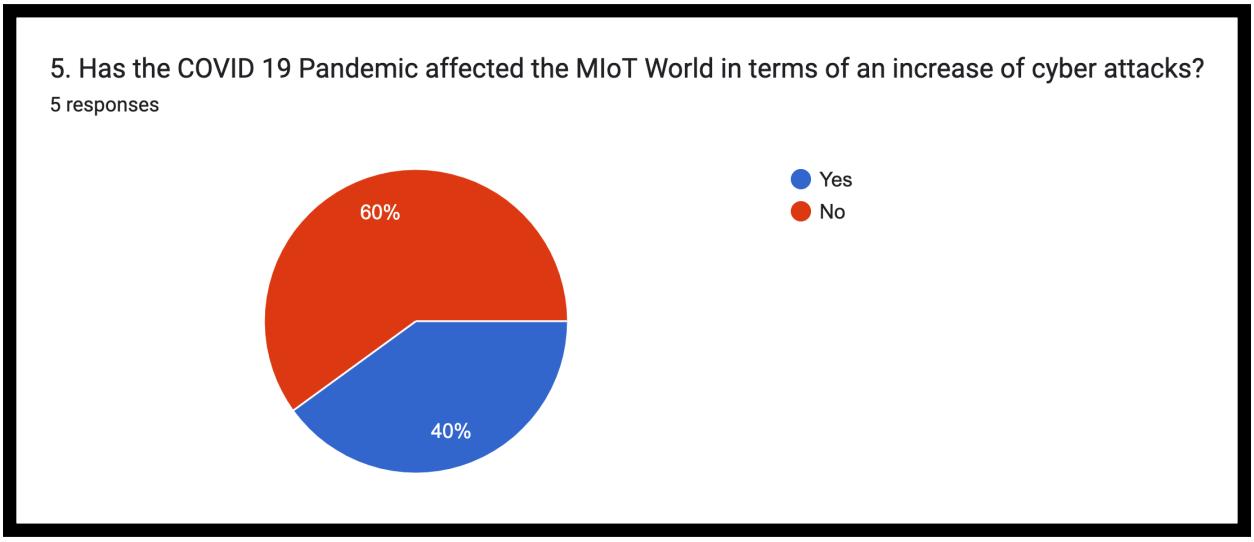
In 2020, the Department of Health and Services did report an uptick in cybersecurity breaches from medical entities, many of which occurred as a result of a hacker taking advantage of an IoT medical device. According to the Department of Health and Services, there was a 50% increase in cybersecurity breaches between the months of February and May in the year 2020 (Healthcare Finance). Natali Tshuva, CEO and founder of Sternum, a company that manufactures built-in security solutions for IoT devices cite medical devices as a popular gateway for cyber criminals to gain unauthorized access to a hospital's security network. This can lead to hackers gaining access to hospital databases, medical machines, and other electronic tools that are necessary for the efficient operation of a hospital. In addition to this, temporary COVID-19 treatment centers were also a common target for cyber hackers, as they often lacked the capability to force or prevent any attacks in a manner even more unprepared than hospitals at the time.

Because of the vulnerable nature of healthcare entities at the time of the COVID-19 Pandemic, as well as the uptick in malicious cyber-attacks on healthcare entities, there has been even more of a focus on targeting healthcare entities from cybercriminals. Many hospitals will often pay cyber criminals to release themselves from whatever damage or constraint has been placed on their systems. While this practice is necessary to save lives at points, it often enables hackers, which results in them continuing to perform this malicious practice, as it proves profitable for them in the past. According to Tsguya: "Hackers know that the healthcare industry is a mess right now in terms of cybersecurity and this gives them even more motivation to create

more and more attacks,". This shows that hackers have even more of a motive and means to hack medical entities. In addition to this, it is important to note how important a role defense plays in preventing cyber-attacks. Oftentimes, if a system has been hacked, it is too late to administer any defense at this point. Because of this, stopping a cyber-attack before it happens is the best way to mitigate the effects of cyber-attacks so that their malicious intents will be thwarted and they are unable to cause harm.

While medical entities were greatly affected as a result of the COVID-19 Pandemic, it remains unclear how greatly or not greatly the pandemic affected insulin pumps and other medical devices. According to survey question 5 (Has the COVID-19 Pandemic affected the MIoT World in terms of an increase of cyber-attacks?) (in which there were 5 responses), two of the respondents claimed that the MIoT World was greatly affected by the pandemic. The other three respondents claimed that MIoTs was not greatly affected by the COVID-19 Pandemic.

Figure 1. Survey Response 5



As shown in Figure 1, the survey question provided rather inconclusive results as to whether or not the pandemic did greatly affect the MIoT World directly. However, it is clear that the pandemic did greatly affect the healthcare world as a whole. This is clear given the effect it has had on hospitals, shortages of medical supplies and equipment, and the negative effect it has had on supply chains. Given this, the MIoT World has been affected indirectly by the pandemic because of the effects on medical entities. Hospitals were overworked and understaffed during the pandemic. As a result, much of the work was outsourced to medical devices and at-home medical methods. This led to.a very large increase in medical device usage. Because of this, attacks on medical devices and medical entities as a whole grow more and more common. The increase in devices makes for a bigger target for malicious hackers, leading to those using MIoTs being even more vulnerable as a result of the increase in emphasis on their devices.

Despite the pandemic being in its waning days, the cybercrime world as a whole still seems to grow. It is predicted that global cybercrime will have an overall worth of about $10.5 trillion by the year 2025 (Dickerson, Shawn). This would make cybercrime a bigger industry than the international drug trade, making it the biggest illicit money-making industry in the world. With this massive jump in value to the cybercrime industry, it is inevitable that healthcare entities will be some of the most targeted entities by cybercrime if steps are not taken to prevent malicious hackers.

As a result of all of this, having a defense against malware and cyber-attacks for medical devices, particularly insulin pumps remains of the utmost importance. The addition of a two-factor authentication protocol in IoT insulin pumps could prove to be critical in defending insulin users against cyber-attacks. This could lead to the prevention of any damage that is done by

malicious hackers and could lead to insulin pump users to have a safer method for administering insulin.

3.

Literature Review

The implementation of two-factor authentication can potentially allow for greater security amongst MIoT devices. This is a topic explored in the scholarly paper, “Two Factor Authentication Protocol for IoT based Healthcare Monitoring System.” This article was written by Abhay Kumar Agragari, Shirshu Varma, and S. Venkatesan. This article overviews the use of an authentication protocol using certificate less cryptography to resolve security issues (Kumar Agrahari, Abhay, Varma, Shirshu, and Venkatesan, S.). According to a formal security analysis, the protocol proves to be effective against attacks. In addition to this, it also proves to be cost-efficient with even greater functionality.

This paper begins with an introduction that details the role of IoT sensors becoming more prevalent in everyday life (medicine, in homes, on the electrical grid). It also explains the extensive body metrics that they are able to test, as well as their uses and effectiveness amongst older populations. This information is collected in a Wireless Body Area Network (WBAN) and is transmitted to a regulator, potentially a Personal Digital Assistant (PDA). Because this is all completed across a public network and contains sensitive health information, it is vital that the network have capable and efficient security, as well as trustworthiness. Furthermore, only authorized individuals must have access to the information that is transmitted through these networks.

The system described in the paper includes four separate entities: the server, the user, the Trusted Authority (TA), and the PDA. The process begins when the user sends the initial

verification request to the TA. The TA then creates a start key for the user to authenticate themselves. A request is also sent to the TA, which is referred to as the registration phase. After this, the login phase can begin, in which the authenticity of the user is verified by the server. After this, the PDA, and server are able to mutually authenticate one another. This ensures that every entity within this interaction is authentic.

The paper then goes into their description of the proposed scheme for the implementation of their certificate-less cryptography scheme. This scheme allows for mutual authentication as well as the key establishment. There are four phases within this scheme: “setup phase”, “registration phase”, “login phase”, and “authentication and key establishment phase”. In the setup phase, the TA creates both public and private keys, in addition to forming the system parameter. In the registration phase, the server, the PDA and the user all register themselves securely. This is done through the use of unique IDs and randomly generated numbers assigned to each entity. Next is the Login Phase, in which the user utilizes their smart card to authenticate themselves. Lastly is the Authentication and Key Establishment Phase. Here is when the server and PSA are able to mutually authenticate one another. They are also able to generate a session key for use in future communication.

The paper then discusses the security benefits that come from utilizing such a method. Here issues, including but not limited to Mutual Authentication, User Anonymity, Resistance to man-in-the-middle attacks, and user privilege, among many other things are discussed in this section. The authors also address the security from a BAN (Burrows-Abadi-Needham) Logic standpoint. This is a way to mathematically analyze the effectiveness of network transfer protocols (Burrows, Michael, Abad, Martin, and Needham, Roger). They did this by analyzing

the three basic aspects of BAN logic (Principals, Keys, and statements) and confirming the basic postulates of BAN. The paper then analyzed this protocol using the Real or Random (ROR) model, as well as the Automated Verification Security Protocol and Analysis tool (AVISPA), which utilizes fake attacks and scenarios to see how effective the network authentication system is.

The paper concludes with a brief overview of why the protection of private data as it is transmitted is necessary to healthcare. It then gives a brief overview of the proposed scheme as well as the security analysis tools that it was tested against. Lastly, it discusses the shortcomings and concerns of the proposed model if it were to be implemented. Lastly, the authors discussed the next step for them would be to test their model within a real environment, to see what results were produced.

This paper does an effective job of explaining their new protocol for secure authentication in a public network. The authors are able to describe their proposed scheme as well as test it against several well-known security analysis protocols. This shows that this method of implementing two-factor authentication is not only possible within medical devices, but it also has the potential to be both secure and cost-effective. These are both necessary aspects of promoting two-factor authentication within insulin pumps. While security is a massive concern when it comes to implementing security within insulin pumps, so too is the idea of practicality. While this scheme still remains somewhat theoretical, it shows that the idea of an effective two-factor authentication method for medical devices is viable. Because of this, this scheme or something similar to it could be the first step in ensuring that IoT insulin pumps are

better protected against various types of cybercrime, be they ransomware, man-in-the-middle attacks, or distributed denial of service.

4.

What are the Threats that Come with Using IoT Insulin Pumps

There are many potential dangers that come into play when dealing with the security of Medical IoT pumps. As with any device, there is always a chance of failure, malfunction, or misuse. However, the risk associated with these things increases greatly when one factors in the danger of cyber-attacks. Many of these attacks are highly sophisticated and can result in great harm to insulin pump users if certain vulnerabilities are exploited. This can include the dangers to the users' health, a leak of personal and private medical information, damage to the expensive insulin pump, and, in extreme cases, death for the user, if the insulin is either withheld or an attacker decides to remotely inject a heavy dose of insulin at once.

One common theme that was heavily acknowledged in the survey results was the threat of Distributed Denial of Services (DDOS) attacks. These attacks seek to overflow a device by having a large number of machines attempt to connect to it. DDOS attacks targeting medical devices have been increasing in popularity as the number of MIoT devices has been booming (McKeon, Jill). This is mostly because they lack adequate security to defend against them and, therefore, pose an easy target to cybercriminals looking to disrupt the operations of medical devices. Concerns regarding DDOS attacks was mentioned in three out of seven responses within the survey. This situation could potentially lead to the pump being unable to operate properly and could lead to a user not being able to get their insulin when they need it resulting in them getting very sick or dying.

Another primary concern when it comes to dealing with the security of insulin pumps would be the possibility of as a Man-In-The-Middle attack (MITM). This is a type of attack

where the hacker is able to install malware that allows them to intercept data and information as it transmits from a user. Potentially, a hacker could install a MITM, which would result in them being able to steal valuable personally identifiable medical information about certain users. Because there are often data sensors that collect data in IoT medical devices, this data is then collected and transmitted to the local processing unit (LPU). This is the point at which data is most vulnerable to MIoT attacks (Salem, Osmen et al). If this data is stolen, it can be dangerous for users, especially if the hackers decide to sell it or use it to blackmail the user. This is a common practice called ransomware, in which hackers will threaten to harm a user by compromising their system unless they do as the hacker says. This usually involves some form of monetary payment, in which the user is forced to pay or lose access to their system, which, in the case of medical devices, could easily result in severe sickness or death.

Another aspect of IoT insulin pumps that could potentially be a threat to users is the concept of the loss or theft of their personal data that transmits through the pump. This data is included but is not limited to usage of the pump, address, location, what level of insulin a user might need, and information on individual sensors on the pump. These are all concerns that were brought up by the respondents in the survey, as they referenced personally identifiable information and pump data (sensor usage, insulin levels, etc.) within their concerns about important data that could be stolen from IoT pumps. This personal information could potentially harm users in many ways, as it could be sold, taken advantage of, or used to harm the user even further. One major concern amongst respondents was what would happen if a hacker was able to modify the body metrics that are included when it comes to determining how much insulin a user needs (glucose levels, insulin levels, when the pump is used, etc). If a hacker could modify or

alter the data so that the pump would administer the improper amount of insulin, which could result in death to the user in extreme circumstances.

Because of these scenarios, it is important to ensure that IoT insulin pumps are protected from unauthorized users not only to prevent them from having complete control of the pumps but also to prevent them from mining private and valuable data. Either of these scenarios could prove to be very dangerous for the pump user, resulting in either death or illness.

5.

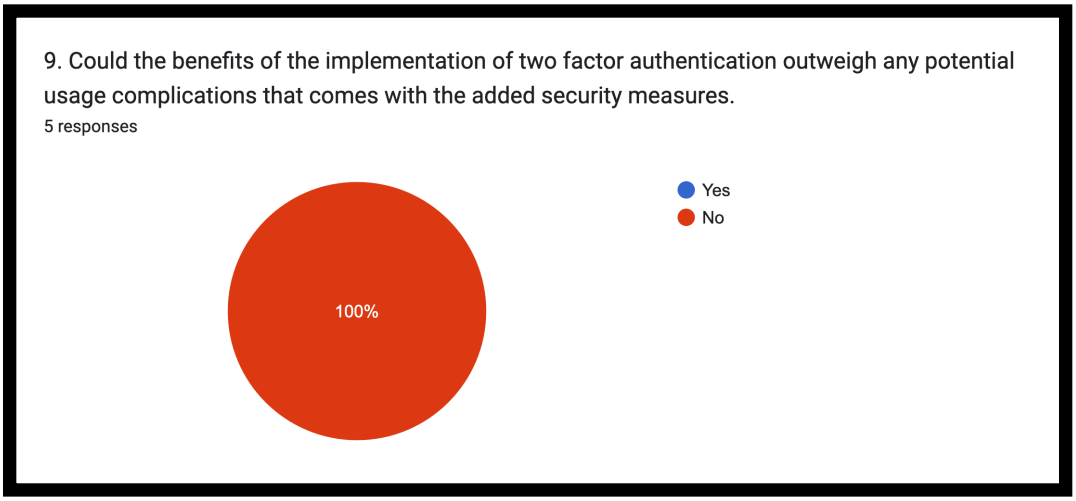
The Use of Two-Factor Authentication within IoT Pumps

Many of the aforementioned attacks can occur as the result of a user exploiting unauthorized access to an IoT insulin pump. Because of this, ensuring that unauthorized hackers are unable to gain access to the IoT device is vital to ensuring that hackers are unable to manipulate their way into having access to the pump. For this reason, utilizing two-factor authentication could be a step toward making it harder for hackers to gain access. This would require any users attempting to gain access to the pump to provide two levels of authentication. Because of this, malicious hackers would have a harder time gaining unauthorized access to pumps that they were trying to hack.

For a user to fully operate the pump, they would need to have two separate ways of authenticating themselves. One common method would to use a password that is known only by the user. This password would come have a minimum letter limit and would also need to require the use of special characters, to make the password harder for malicious hackers to brute force. Other methods of authentication could include having a call sent to the user's cellular phone for them to answer, holding a device in which there is a verification code that changes every 30 minutes, or having the user present a unique body metric. This would result in the user being able to doubly authenticate oneself with methods that would be difficult for unauthorized entities to spoof or fake.

According to the survey, many believe that the benefits of utilizing two-factor authentication would not outweigh the cost and potential complications that come along with utilizing it.

Figure 2. Survey Response 9



As seen in Figure 2, all five respondents voted that the benefits would not outweigh the costs when talking about implementing two-factor authentication. While this was not the expected answer, it does beg the question, "What dangers are made present by implementing two-factor authentication to insulin pumps?" While the use of two-factor authentication could result in a lesser chance of the pumps being compromised by unauthorized users, it also gives the potential to make the pumps overly complicated to operate.

Despite the survey results, there are potential two-factor authentication schemes that could possibly prove to be effective two-factor authentication methods. One such method was the method proposed by Abhay Kumar Agragari, Shirshu Varma, and S. Venkatesan. While this method has not yet been tested against a real-world environment, it has been tested against several security authentication methods (BAN, ROR, AVISPA). The scheme has tested well

against these methods and it has proven to hold enormous potential in the overall security of the insulin pump. In addition to this, it also has proven to be cost effective, meaning it has the potential to be commercially available to the public. As a result of these findings, it remains possible that such a feature becoming widespread in insulin pumps is plausible.

6.

Potential Dangers of Implementing Two-Factor Authentication to IoT Devices

While there are benefits to implementing two-factor authentication in IoT insulin pumps, there are also many dangers. Implementing this type of authentication system could lead to complications that would result in a danger greater than the benefits could outweigh. Such dangers could include potential damage to the pump or insulin as a result of overheating, or users getting locked out of the pump. There is also concern regarding the time required to authenticate leading to complications, and the possibility of the user losing their phone or device that allows them to authenticate.

One such danger that would come from implementing two-factor authentication within insulin pumps would be the level of complication that it brings to the overall operation of the pump. This was a common theme within the responses to the survey. In general, adding such a security method would add another task to complete before allowing for the pump's operation. This could possibly result in the usability of the pump being delayed operations as a result of the increased login time. This increased login time could potentially lead to complications when it comes to administering insulin and could result in sickness if the insulin is delayed for too long as a result of the authentication. In addition to this, there is also the factor of the computation power of the authentication, which can also add complication to the pump's operation if it does not perform correctly. According to one of the respondents, a typical insulin pump user will interact with their pump about 20 times a day. Because of this, it is important that the pumps be relatively easy to use.

Another potential danger that comes with the implementation of two-factor authentication is the chance of the users not being able to authenticate themselves because of complications with a form of authentication. Essentially, if a factor gets lost, then the user would be locked out of their own device (Korzsun, Jennifer). Examples of this scenario would be if a user's phone was lost, broken, had no battery, or was in any way unable to access the information that would allow a user to authenticate oneself. Another scenario would be if there were complications with a user's passcode device. Any of these scenarios, among others, could result in the user being unintentionally locked out of their own insulin pump and potentially unable to administer insulin to themselves. This is a situation that can occur in many scenarios that involve two-factor authentication.

Another situation that could occur as a result of the implementation of two-factor authentication would be the potential draining of battery life more quickly. Because adding authentication is a process that runs consistently along with the operation of the pump, it is possible that this operation could result in the pump using the battery at too fast a rate. Such was the case with Microsoft Authenticator, in which this two-factor authentication method resulted using up battery too quickly (Nopanen, Vesa). This could potentially result in a battery depleting too quickly, which would result in the user being unable to inject insulin if the user does not have a backup battery.

Another concern with the concept of implementing two-factor authentication would be the potential of a pump overheating. Because there is the added function of two-factor authentication, there is a chance that the function causes the pump to heat up in a way that it would not normally heat otherwise. This could result in the pump not operating properly, or the

supply of insulin contained within the pump being damaged as a result of the overheating. This would ruin the insulin and result in it not properly controlling the level of blood sugar within the person (Long, Larissa).

Despite the benefits that come from the implementation of two-factor authentication, there are also a fair amount of potential dangers that come from them as well. These are including but are not limited to complications of pump functionality, overheating of the pump and insulin, inadvertent lockout, and draining battery life. Considering these dangers, to properly implement two-factor authentication within insulin pumps, it would be important to take any necessary steps to mitigate these potential risks.

7.

Conclusion

Healthcare entities are the most vulnerable and targeted entities by cybercriminals. This is mainly due to inadequate protective measures, the importance of medical information, and the urgency required of medical systems, among other things. As a result of the COVID-19 Pandemic, there has been an even greater amount of attacks targeting healthcare entities. Internet of Things Insulin Pumps are no exception to this increase in attacks, as they are vulnerable to Man-in-the-Middle attacks, Distributed Denial of Services, and ransomware. As a result of being vulnerable to malicious hackers, it is of the utmost importance to emphasize protection for these medical devices.

Two-factor authentication could potentially result in more enhanced security for insulin pumps. In this process, a person will have to authenticate themselves in two separate ways to ensure that they are authorized to utilize the pump. This will, ideally, prevent any unauthorized intruders from taking advantage of the pump and causing harm or even death to the user. Overall, this would result in a safer authorization protocol for insulin pump users, which would ensure the safer usability of the pump.

While there are many positives to implementing two-factor authentication to insulin pumps, there are also many potential negative aspects that could result from this implementation. There are included but not limited to overheating, complications of pump usage, accidental lockout, and increased login time. These dangers could result in the user not being able to be

administered insulin in a timely manner and, therefore, every effort should be made to mitigate them.

While there are some potential downsides to utilizing two-factor authentication within IoT insulin pumps, this implementation has the potential to prevent malicious hackers from implementing malware that will either damage or prevent the operations of the pump. This system could result in a safer world for medical IoT users, particularly in the realm of IoT insulin pumps.

BIBLIOGRAPHY

Basch, Corey. April 23, 2021. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. National Library Medicine. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8059789/

Burrows, Michael, Abad, Martin, and Needham, Roger. (May 1989). A Logic Authentication. *ACM Transactions on Computer Systems.* http://www.cs.cmu.edu/~dga/15-712/F07/papers/Burrows90.pdf

Horowitz, Brian. (March 26, 2021). 2020 offered a 'perfect storm' for cybercriminals with ransomware attacks costing the industry $21B. *Fierce Healthcare.* https://www.fiercehealthcare.com/tech/ransomware-attacks-cost-healthcare-industry-21b-2020-here-s-how-many-attacks-hit-providers

Long, Larissa. (December 15, 2022). How Insulin Works in The Body. *Endocrine Web*. https://www.endocrineweb.com/conditions/type-1-diabetes/what-insulin/how-does-insulin-work.

McKeon, Kill. (November 4, 2021). The Threat of Distributed Denial-Of-Service Attacks in Healthcare. TechTarget: Health Security. https://healthitsecurity.com/features/the-threat-of-distributed-denial-of-service-attacks-in-healthcare

Morgan, Steve. (November 13, 2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine.* https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Klonoff, David. (April 16, 2015). Cybersecurity for Connected Diabetes Devices. *Journal of Diabetes Science and Technology: Sage Publications.* https://journals.sagepub.com/doi/full/10.1177/1932296815583334

Korzsun, Jennifer. (October 25, 2017). 3 Disadvantages to Two-Factor Authentication (2fa). *Electronic Products.* https://www.electronicproducts.com/3-disadvantages-of-two-factor-authentication/

Kumar Agrahari, Abhay, Varma, Shirshu, and Venkatesan, S. (April 18, 2022). Two factor authentication protocol for IoT based healthcare monitoring system. *National Library of Medicine.* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9013638/

Ngak, Chanda. (April 29, 2011). Black Hat Hacker Can Remotely Attack Insulin Pumps and Kill People. *CBS News.* https://www.cbsnews.com/news/black-hat-hacker-can-remotely-attack-insulin-pumps-and-kill-people/

Nopanen, Vesa. (September 9, 2019). Solved: Microsoft Authenticator draining battery on Android phone. *My Metaverse Day*. https://mymetaverseday.com/2019/09/24/solved-microsoft-authenticator-draining-battery-on-android-phone/

Robinson, Phillip. (January 10, 2022). 7 Reasons Why Healthcare Is A Prime Target for Cyber Criminals. *Lepide.* https://www.lepide.com/blog/7-reasons-why-healthcare-is-a-prime-target-for-cyber-criminals/

Salem, Osmen et al. (March 3, 2022). Man-in-the-Middle Attack Mitigation in Internet of Medical Things. Institute of Electronic and Electrical Engineers. https://rboutaba.cs.uwaterloo.ca/Papers/Journals/2021/SalemTII21.pdf

(June 4, 2020). Number of cybersecurity attacks increases during COVID-19 crisis. *Healthcare Finance.* https://www.healthcarefinancenews.com/news/number-cybersecurity-attacks-increase-during-covid-19-crisis

ACADEMIC VITA

Edward Burke

EDUCATION

The Pennsylvania State University, University Park

Schreyer Honors College — June 2020 - Present

BS in Cybersecurity Analytics and Operations — Expected May 2023

Dean's List — August 2019 - Present

EXPERIENCE

Cyber Intern, Deloitte Government and Public Services, Arlington, VA — June 2022 - July 2022

- Completed an 8-week long internship program in which I assisted in data center migration.
- Researched IoT devices for the Border, Trade, and Immigration Account.

Research Member, Penn State University Summer REU, State College PA — May 2021- July 2021

- Completed a ten-week long research project regarding the identification of unsafe Rust code.
- Had weekly meetings with my mentor and fellow cohort members to discuss various cybersecurity topics.

Learning Assistant, Pennsylvania State University, University Park. — August 2020 - May 2023

- Assists in teaching beginner Java to underclassmen.
- Grades student assignments such as quizzes and problem sets.

Delivery Driver, DoorDash, Wayne PA — June 2020 - Present

- Completes food deliveries to customers.
- Communicates with customers regarding potential issues.

SKILLS

Languages: Java, Python, Rust, HTML, JavaScript

Applications: NetBeans, PyCharm, SQL

LEADERSHIP AND INTERESTS

THON Captain — September 2021 - March 2023

- Student volunteer for Dance Marathon Benefitting research for Childhood Cancer, serving on both the Communications and Dancer Relations Committees. In my second year, I led a committee of 28 individuals on the Dancer Relations Committee. I also served as a liaison for over 25 fundraisers in the 2022 year, as well as a liaison for all EMS services for the event in the 2023 year.

Lion Ambassador — January 2021 - Present

- Leads tours for prospective students and participates in various projects around campus.