Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System

Chunxiao Li
Department of EE
Princeton University
chunxiao@princeton.edu

Anand Raghunathan
School of ECE
Purdue University
raghunathan@purdue.edu

Niraj K. Jha
Department of EE
Princeton University
jha@princeton.edu

***Abstract*—Wearable and implantable medical devices are being increasingly deployed to improve diagnosis, monitoring, and therapy for a range of medical conditions. Unlike other classes of electronics and computing systems, security attacks on these devices have extreme consequences and must, therefore, be analyzed and prevented with utmost effort. Yet, very little work exists on this important topic and the security vulnerabilities of such systems are not well understood.**

We demonstrate security attacks that we have implemented in the laboratory on a popular glucose monitoring and insulin delivery system available on the market, and also propose defenses against such attacks. Continuous glucose monitoring and insulin delivery systems are becoming increasingly popular among patients with diabetes. These systems utilize wireless communication links, which are frequently utilized as a portal to launch security attacks. Our study shows that both passive attacks (eavesdropping of the wireless communication) and active attacks (impersonation and control of the medical devices to alter the intended therapy) can be successfully launched using public-domain information and widely available off-the-shelf hardware. The proposed attacks can compromise both the privacy and safety of patients. We propose two possible defenses against such attacks. One is based on rolling-code cryptographic protocols, and the other is based on body-coupled communication. Our security analysis shows that the proposed defenses have the potential to mitigate the security risks associated with personal healthcare systems.

I. Introduction

Personal healthcare systems based on implantable and wearable medical devices are expected to transform healthcare by enabling diagnostics, monitoring, and therapy anytime, anywhere and on a continuous and personalized basis. A common trend in these systems is towards greater "intelligence," fueled by the use of increasingly powerful embedded processors, wireless communications, and connectivity to back-end computing infrastructure. Complexity, programmability, and network connectivity have colluded to make information security a significant challenge in general-purpose computing systems; therefore, it is reasonable to expect that these trends foretell of security attacks on personal healthcare systems as well. However, in the context of such systems, the consequences of security attacks can be extreme, often allowing attackers to cause the appliances to operate in a life-threatening manner.

In this work, we demonstrate successful security attacks on a commercially deployed glucose monitoring and insulin delivery system and propose defenses against the proposed attacks. Glucose monitoring and insulin delivery systems are used for the treatment and management of diabetes. In the US, the Centers for Disease Prevention and Control estimate that 25.8 million people (8.3% of the population) [1] live with diabetes. Most diabetics use glucose meters and a rapidly growing number of them are using insulin pumps for therapy. There were around 245,000 insulin pump users in 2005, and the market for insulin pumps is expected to grow at a compound rate of 9% from 2009 to 2016 [2], [3].

Continuous glucose monitoring and insulin delivery systems commonly employ wireless communication among components of the system, such as the glucose monitor, insulin pump, and remote control, connecting them to form a real-time monitoring and response loop. Unfortunately, the wireless channel also serves as a portal to launch security attacks. For example, what if incorrect blood glucose results are sent to the insulin pump wirelessly by malicious attackers? And what if the attackers can control the insulin pump remotely and stop the required insulin injection, or inject insulin at a much higher dose than necessary?

The above scenarios are not as far-fetched as they may appear. We have analyzed a popular glucose monitoring and insulin delivery system that is currently available on the market. With only the user's manual and some publicly available information, such as the specifications of the radio chip used by the insulin pump, we were able to eavesdrop on the wireless communications using off-the-shelf hardware and a publicly available software radio platform. Since cryptography is not employed, we were able to eavesdrop on the data in a cleartext form. After reverse-engineering the communication protocol and packet format, we were able to fully discover the device PIN of the remote control and glucose meter, and regenerate a legitimate data packet, which is accepted by the insulin pump, containing misleading information, *e.g.*, an incorrect reading of the glucose level, control command for stopping/resuming of insulin injection, and control command for immediately injecting a dose of insulin into the human body. Studies [4] have shown that blood glucose results from miscoded meters may result in significant insulin dose errors. Misconfigured insulin therapy may cause hyperglycemia (high

Acknowledgment: This work was supported by NSF under Grant No. CNS-0720110 and CNS-0914787.

978-1-61284-697-2/11/$26.00 ©2011 IEEE

blood glucose) or hypoglycemia (low blood glucose) and endanger the patient's life. However, we are not aware of any efforts to analyze these insulin therapy systems under malicious security attacks.

We suggest two possible defenses against the proposed security attacks, which are also applicable to many other personal healthcare systems. One solution is to employ cryptography in the communication protocol. However, cryptographic algorithms and protocols used in general-purpose computing platforms are too heavyweight (in terms of processing capability, memory, and power requirements) for many medical devices. Inspired by cryptographic techniques used in remote-entry systems for automobiles and buildings, we propose the use of rolling code based encryption and apply it to the insulin delivery system. We also explore a more novel defense based on the concept of body-coupled communication (BCC), which significantly raises the difficulty for the attacker to eavesdrop on the communication channels among the components of a personal healthcare system. We experimentally demonstrate the efficacy of BCC compared to a conventional wireless channel.

The rest of the paper is organized as follows. Section II presents background material on glucose monitoring and insulin delivery system, and previous research on medical device security. Section III describes passive and active attacks against the insulin delivery system. Section IV describes the potential attack scenarios based on the identified security breaches. Section V proposes two types of defenses and Section VI concludes the paper.

II. Background and related work

In this section, we present some background material on insulin therapy and related research on personal healthcare system security.

A. Glucose monitoring and insulin delivery system

A glucose monitoring and insulin delivery system may consist of several components:

- A blood glucose monitor samples blood glucose levels on a continuous basis, typically every few minutes. The monitor includes a disposable glucose sensor placed under the skin to measure the glucose level, and a transmitter attached to the sensor to transmit data to a computer or insulin pump.
- The insulin pump is a medical device that is used for autonomous administration of insulin through subcutaneous infusion. The pump delivers insulin in two doses: bolus and basal. A bolus dose is pumped quickly to account for the food eaten or to correct a high blood glucose level. A basal dose is slowly and continuously injected at an adjustable rate between meals and at night. Its injection time, rate, and dose can also be programmed based on the patient's needs. There are four different programming and communication interfaces implemented on current insulin pumps: (1) buttons on the pump itself, (2) wireless connection to a remote control, (3) wireless connection to a computer, used to upload data and/or manage the programming, and (4) wireless connection to a blood glucose monitor.
- The remote control is a device that controls and programs the insulin pump. A full-featured remote control can do all the programming required by the insulin pump, whereas a simple remote control may only allow the user to deliver a discrete bolus dose or stop/resume insulin delivery.
- Computers log data from the continuous blood glucose monitor, blood glucose meter, and insulin pump, organize and visualize the data, and report them to the patient and doctor for improved therapy management.

Diabetics are increasingly migrating from the traditional glucose meter and manual insulin injection systems to continuous glucose monitoring and automatic insulin delivery systems, since they offer greater convenience and better control over blood glucose levels. In a recent study, patients who wore insulin pumps for continuous insulin injection reported a better quality of life than when using other devices [5]. In such systems, as shown in Fig. 1(a), there exist several wireless links to automate the process: the link from the meter/monitor to the pump to transmit glucose levels, and the link from the remote control or computer to the pump to transmit control commands. These wireless links are security-critical to the whole insulin delivery system — they impact confidentiality, integrity, and availability. However, as shown in this paper, the wireless links in currently available glucose monitoring and insulin delivery systems may be insecure. We specifically show how to successfully intercept and attack the wireless links using off-the-shelf hardware and software, and how these attacks may then be used to undermine the correct operation of the insulin delivery system and endanger the patient's life.

B. Related work

While we believe our work to be the first demonstration of a malicious attack on a real glucose monitoring and insulin delivery system, previous research has investigated accidental failures in medical devices, such as radiation treatments [6] and insulin dose errors from miscoded glucose meters [4].

In the more general research area of medical sensor network security, researchers have discussed security threats and solutions for pervasive healthcare [7], requirements and design spaces of mobile medical care [8], interoperability and security in wireless body area network infrastructures [9], and a deployment model of wireless sensor networks for pervasive healthcare [10]. A survey article [11] reviews the security and privacy issues for implantable medical devices. Another body of research focuses on the implementation of secure medical sensor networks. Secure key exchange protocols and schemes for verifying the authenticity of patient data are discussed in [12]. A lightweight security system allowing for distributed key management for medical sensor networks is introduced in [13].

The closest study to our research [14] demonstrated attacks on pacemakers and implantable cardiac defibrillators, and

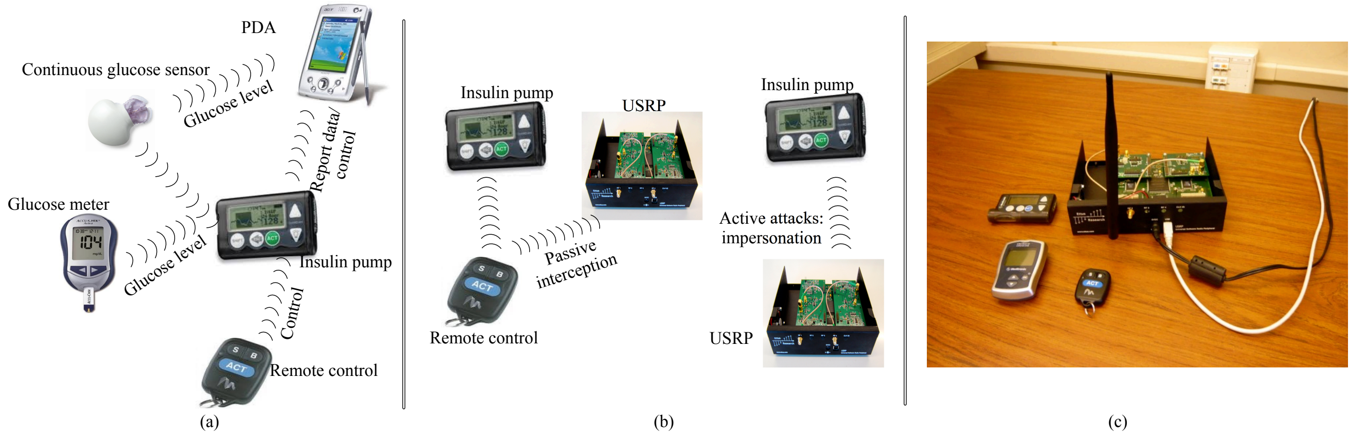

Fig. 1. (a) Insulin delivery system, (b) security attacks, and (c) experimental setup used in the attacks

proposed zero-power defenses. This work was the first to practically demonstrate a security attack on a medical appliance. Although similar in overall objectives, our work differs significantly in our attack methodology and proposed defenses. As the authors stated in [14], they did not perform packet analysis or reassembly, "only simple waveform manipulation and repetition." We, however, fully reverse-engineered the radio protocol of the insulin delivery system so that adversaries can reassemble the packets and emulate the full functions of a remote control: wake up the insulin pump, stop/resume the insulin injection, or immediately inject a bolus dose of insulin into the human body. The defenses that we propose are also different from those presented in [14].

Proximity-based access control has been proposed as a technique for implantable medical devices to verify the distance of the communicating peer before initiating wireless communication, thereby limiting attackers to a certain physical range [15]. Our proposal for using BCC is different in that we replace the traditional wireless channel, and not add an additional channel.

In the area of BCC, initial research tried to model the body-coupled channel [16], [17]. Another work was based on an experimental study and discussed the characterization of the human body as a signal transmission medium [18], [19], [20]. A third group of studies dealt with the design and implementation of the transceiver for BCC [21], [22], [23].

III. Passive and Active Attacks on Wireless Links of an Insulin Delivery System

We next discuss successful passive and active attacks on a commercially available insulin delivery system. Our experimental setup included a glucose meter, an insulin pump, a remote control, and a Universal Software Radio Peripheral (USRP) [24]. We choose not to fully disclose the model information (brand, type and model no.) here.

USRP is an off-the-shelf software radio board that costs about $700. With free software (GNU radio [25]) and appropriate daughter boards, the USRP can intercept radio communications within a frequency band, and generate wireless signals with different configurations of data, frequency, modulation, and power.

As shown in Fig. 1(b), we focused on the wireless link from the remote control to the insulin pump and intercepted the communication. We then fully reverse-engineered the communication protocol and were able to successfully launch active attacks that remotely control the insulin pump. We show the experimental setup in Fig. 1(c).

A. Frequency

The operating frequency of the wireless link needs to be determined first. The frequency of any wireless device is publicly available online and easily obtained through its FCC ID. In our example system, the communication between the remote control and insulin pump uses 915 MHz. A 915 MHz daughter board and antenna are attached to the USRP board to receive and generate the signal in the 915 MHz frequency band.

B. Modulation type

We intercepted the wireless signal around 915 MHz and down-converted it to near the baseband, as shown in Fig. 2. After analysis, we found that on-off keying was used in the communication. This modulation scheme uses the presence of a carrier wave to indicate a binary 1 and its absence to indicate a binary 0.

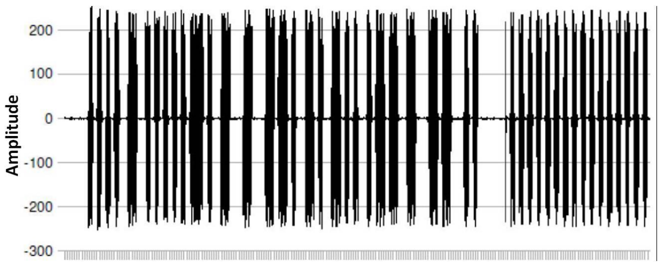

Fig. 2. Signal intercepted by USRP

C. Packet format

For both the glucose meter and remote control, in order to make the insulin pump receive the data or control command, a code of six hexadecimal digits needs to be entered manually by the users into the insulin pump. The digits are printed on the back of a glucose meter or remote control as a "PIN." We

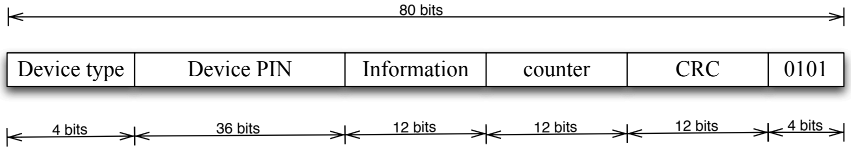

Fig. 3. Format of the communication packet in the insulin delivery system

ascertained that not entering the PIN or entering the wrong PIN causes a failed communication. However, as explained below, the PIN is transmitted in plaintext and can be captured by simply eavesdropping on the communication between the devices.

We intercepted the data packets from the remote control (generated by different buttons) to the glucose meter. After the synchronizing sequence of "0"s and "1"s, there are 80 information bits. We deciphered these bits after a thorough analysis: (1) the first 4 bits represent the device type because they are different when different types of devices are used (glucose meters or remote controls); (2) the next 36 bits constitute the device PIN because they are different for each device, and (3) the last 40 bits can be split into four parts: the first 12 bits are payload bits indicating which button was pressed or what glucose level reading was transmitted; the next 12 bits are counters and repeat after 256 counts; the next 12 bits seem "random," but actually perform a cyclic redundancy check (CRC); the last four bits are always "0101."

After more testing and analysis, we were finally able to parse the communication packet, in the format shown in Fig. 3.

D. Counter and CRC

After identifying the 12-bit counter, we found that the pattern that it repeats after 256 counts indicates that a sequence of six bits represents a hexadecimal digit – an increasing count of two hexadecimal digits repeats after 256 counts. We then constructed a correspondence table between the bits in the communication packet and the corresponding hexadecimal digits. We found that the device PIN is actually sent in a clear-text without any encryption – every PIN digit is represented by six bits based on the same correspondence table and the total of 36 PIN bits represent six hexadecimal digits printed on the back of the medical device. For security reasons, we choose not to disclose the mappings between the information bits and the hexadecimal digit.

The 12 bits next to the counter are for the CRC. The sender (remote control in this case) calculates a short, fixed-length binary sequence (12 bits in this case) for each block of data and sends them together as a packet. When a packet is received, the device repeats the calculation using the same CRC algorithm. If the calculated CRC does not match the one received, the data may contain a transmission error and the packet is dropped. There are several parameters involved in the CRC calculation: CRC order, CRC polynomial, initial value, final XOR value, whether to reverse data bytes, and whether to reverse the CRC result before the final XOR. After many trials, we were able to find the CRC parameters used in the insulin delivery system. Note that these parameters are needed if we want to generate a legitimate packet with our own information bits that is acceptable to the insulin pump, because packets without the correct CRC will be dropped. In Table I, we show the parameters of the CRC for both the remote control and glucose meter (they use similar CRC parameters). For security reasons, some of the parameters are replaced with "*x*".

TABLE I
CRC PARAMETERS FOR THE REMOTE CONTROL AND GLUCOSE METER

Parameters	remote control	glucose meter
CRC order	8	8
CRC polynomial	*x*	*x*
Initial value	0	0
Final XOR value	*x*	*x*
Reverse data bytes	N	N
Reverse CRC result	N	N

E. Replay

The system employs a simple security mechanism to defend against replay attacks: a packet is not accepted if its counter has exactly the same value as the last packet. However, we found that as long as the counter has a different value from the last one, the packet is accepted. Therefore, we were able to intercept two packets and transit them in an alternating fashion. Replaying can be used for simple attacks, such as reporting an outdated glucose level to the insulin pump.

F. Generation of arbitrary data packets

Having determined the format of the packet and the parameters of the CRC, it is now possible to regenerate a legitimate packet that will be accepted by the insulin pump. We performed tests on the real system by entering a new random device PIN into the pump and generating a new control packet using this PIN. We were able to fully control the insulin pump using the USRP as a remote control.

IV. ATTACK SCENARIOS BASED ON SECURITY BREACHES OF THE INSULIN DELIVERY SYSTEM

Next, we analyze the possible practical attacks that can be launched by exploiting the security breaches on the wireless links. Attacks are categorized into two groups, as discussed in the next two subsections.

A. Attacks without the knowledge of the device PIN

If the attacker does not know the device PIN of the remote control or glucose monitor, some of the possible attacks are:

- **Privacy attacks.** Eavesdropping on any wireless link in the insulin delivery system would expose: (1) the existence of the therapy and the glucose level, and thus the medical condition of the patient, (2) the device type, and (3) the device PIN, which will give the attacker an open door to launch all the attacks discussed in the next group.

- **Integrity attacks.** Even without the knowledge of the device PIN, using the alternating transmission of two consecutive packets, the attacker can still control the insulin pump, or report an incorrect (past) glucose reading to the insulin pump. More details are given below.
- **Availability attacks.** Attackers can simply jam the communication channel between the medical devices, causing incorrect operation. However, these attacks can be easily detected by the patient: either the remote control does not work or the data transmission fails.

B. Attacks with the knowledge of the device PIN

If the attacker knows the device PIN of the remote control (glucose meter) of the insulin pump, either by reading the printed device PIN from the medical device or using the eavesdropping attacks discussed above, some other attacks that can be launched are as follows: (1) one can stop insulin injection into the human body, which will cause a high glucose level, (2) one can resume insulin injection into the human body if it is currently stopped, and (3) one can inject a bolus dose into the human body, which may lead to hypoglycemia and endanger the patient's life.

We have not verified that the format of the communication protocol between the continuous glucose monitor and the insulin pump is the same as that between the remote control and pump discussed before. However, we believe that one can easily attack this wireless link using the same methodology. If the attacker knows the device PIN of the continuous glucose monitor, he can report a false reading to the pump and mislead the patient into injecting more or less insulin than needed. This attack is less feasible if a traditional glucose meter with a display is used because the user can always verify whether the two readings are the same. However, since the continuous glucose monitor is attached to the human skin and no display is available, this attack can be more easily launched.

Note that besides intercepting the communication on the wireless link first, the attackers have other means for obtaining the device PIN, such as peeking at the printed PIN, or through insider information from the device manufacturing or supply chain.

C. Attack experiments using USRP

First, we have experimentally determined that the remote control can program the insulin pump at a distance of up to 4.5 meters, when there are no obstacles in between.

Second, we have set up the passive attack scenario: while the remote control is communicating with the insulin pump, we eavesdrop on the signal and measure the signal strength (amplitude in Fig. 2.) using the USRP eavesdropping device at different distances from the remote control. We have concluded that within 7-8 meters, the signal strength is well above the noise level and it is easy to eavesdrop on the signals and extract the device type, device PIN, and the control command sent to the insulin pump. Note that since the maximum attacking distance depends on the antenna and the sensitivity of the receiver, a better antenna and receiver chip may expand this distance further.

Third, we have set up the active attack scenario: we use the USRP to control the insulin pump from a distance to see how far away the active attacks can still succeed. We use the device PIN extracted from the last step to regenerate some unauthenticated control commands. We have verified that using the maximum allowed power level of the USRP daughter board, which is 200 mW (23 dB), the insulin pump will accept the control and stop/resume insulin injection at a distance even farther than 20 meters. We believe that, with a better antenna and larger output power, much larger active attack distance can be achieved.

In conclusion, using an off-the-shelf device, such as the USRP, passive and active attacks on the insulin delivery system are possible. For example, in a hospital, an attacker can eavesdrop and extract the device PIN of the remote control from outside a patient's room at a distance of 7-8 meters, and secretly control insulin injection even from 20 meters away.

V. Possible defenses against the attacks

In this section, we discuss two possible defenses against the attacks discussed earlier. One simple and obvious solution is to use cryptography. A very similar scenario to the insulin delivery system is automobile keyless entry. Both have the following characteristics: one-way communication, very low data rate, and high security requirements. We refer to the current security protocols in automobile keyless entry and propose their application to the insulin delivery system.

Another more general solution is to use BCC in the system to avoid attacks from the lowermost physical layer. We introduce the principles of BCC and, for the first time, show experimental results related to the security of BCC and its implications on body-area medical device networks.

A. Traditional cryptographic approach

Instead of sending a fixed device PIN every time, rolling codes are widely used in automobile keyless entry systems [26]. Based on this technique, we propose a rolling code encoder embedded in the remote control, and a rolling code decoder in the insulin pump, as shown in Fig. 4.

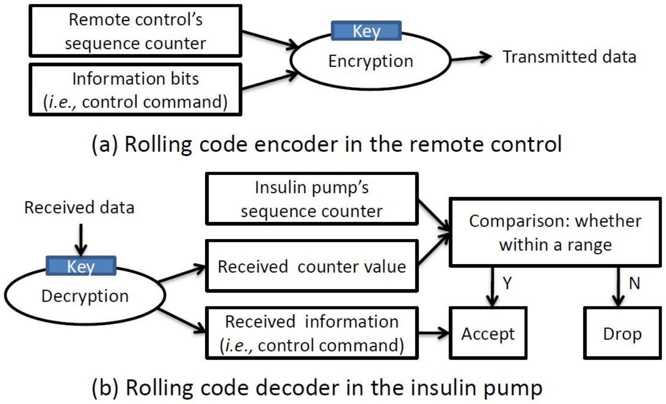
Remote control's sequence counter
Information bits (i.e., control command)
Key
Encryption
Transmitted data
(a) Rolling code encoder in the remote control
Received data
Key
Decryption
Insulin pump's sequence counter
Received counter value
Received information (i.e., control command)
Comparison: whether within a range
Y
N
Accept
Drop
(b) Rolling code decoder in the insulin pump

Fig. 4. Proposed rolling code en/decoder in the insulin delivery system

The remote control and insulin pump share an encryption key. The key in the remote control is used to encrypt a number in the sequence counter. The number is increased by 1 for every communication packet. In the insulin pump, the encrypted data are decrypted using the shared key, and the decrypted sequence number is compared to the receiver's counter. If the difference is within a certain range (the remote control may have had several failed communications before), the insulin pump believes that the received control code is valid, synchronizes the sequence counter, and performs the task.

With the rolling code technique, it becomes impossible for the attackers to simply extract the device PIN, or to launch replay attacks, because the transmitted data are encrypted and the rolling code changes every time. The security of the rolling code system depends on the encryption/decryption algorithm and the encryption keys. Previous research [27] has shown successful attacks on one popular encryption block cypher – KeeLoq, used in rolling code systems.

B. Body-coupled communication

Another promising technology that can be used is BCC. We first introduce the BCC technology and then show some BCC-based experimental results to show how the insulin delivery system can be protected.

1) Introduction to BCC: BCC [19] is a technology that uses the human body as the transmission medium to enable wireless communication, in contrast to the conventional over-the-air communication. One claimed advantage of BCC [19] is that the communication range is limited to the close proximity of the human body, which prevents interference between BCC-based body area networks. Another key advantage is that BCC may consume less power because the data are only sent around the body rather than through free space [28].

In the insulin delivery system, all devices are attached to the body: the continuous glucose meter and the insulin pump need to be directly attached for monitoring and injection; the remote control buttons also need to be pressed, thus are connected to the skin while communicating. If BCC is limited to the close proximity of the human body, not only would the attacks described in this paper be useless, some other attacks can also be eliminated, such as the unauthorized or accidental use of the remote control, as long as the attacker is not within very close proximity of the patient or touching the patient's skin.

Previous work has provided various measurements [19] for BCC, such as propagation loss as a function of frequency, transceiver position, and electrode size. In this paper, we focus more on the security of BCC and design experiments to show how BCC can defend against passive and active attacks described earlier.

2) Experiments: The equipment used in the experiments includes a function generator, a middle-wave/short-wave active loop antenna, electrodes, and USRP.

The first group of experiments is set up to discover which frequency band for BCC causes the least propagation loss. We use the USRP as a receiver and the function generator as a transmitter that transmits a mono-frequency signal. Both are directly connected to the human body via electrodes. The USRP performs a fast Fourier transform on the received signal and the spur-free dynamic range (SFDR) is measured. SFDR is the strength ratio of the fundamental signal to the strongest spurious signal in the output, and is a measure of the signal strength relative to the noise level. We decided to use the frequency of 5 MHz, which has a maximum SFDR of 84 dB (with a function generator output peak-to-peak amplitude of 200 mV), as the BCC transmission frequency in the following experiments.

The second group of experiments is set up to show how BCC can defend against passive eavesdropping attacks. We use the function generator to generate a 5 MHz signal, attached to the human body. The USRP mimics the eavesdropping attacker and picks up the signal from some distance. To receive better signals, we used an active-loop antenna in the corresponding frequency band. The results are shown in Fig. 5. The original insulin delivery system is also experimentally evaluated for comparison. We adjusted the output power of the function generator to enable a fair comparison between BCC and the original air channel: the SFDR of the BCC is the same as that of the remote control signal at a distance of 0.5 meters (a typical distance during the normal usage of an insulin delivery system).

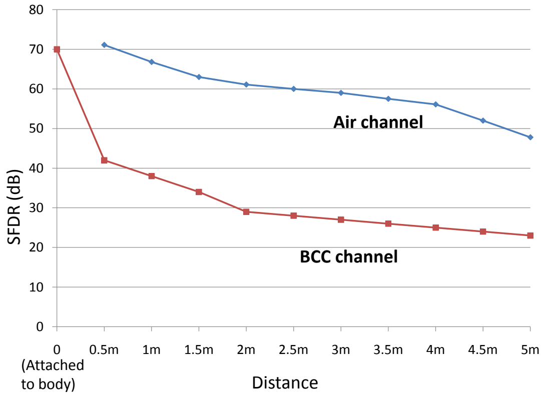

Fig. 5. SFDR as a function of distance using air and BCC channels in the case of passive attacks

The third group of experiments is set up to show how the BCC can defend against active attacks. We use the function generator equipped with an antenna to broadcast the signal, and then use the USRP, which is attached to the human body via electrodes, to pick up the signal. The function generator mimics the active attacker trying to control the medical device and the device attached to the body receives the signals. The results are shown in Fig. 6. The original insulin delivery system is also evaluated for comparison.

From the experiments, we can conclude that BCC does help mitigate passive and active attacks: for passive eavesdropping attacks, at the same distance, the SFDR of the signal is around 30 dB less than in the case of conventional communication, thus, making the signal more difficult to eavesdrop on; for

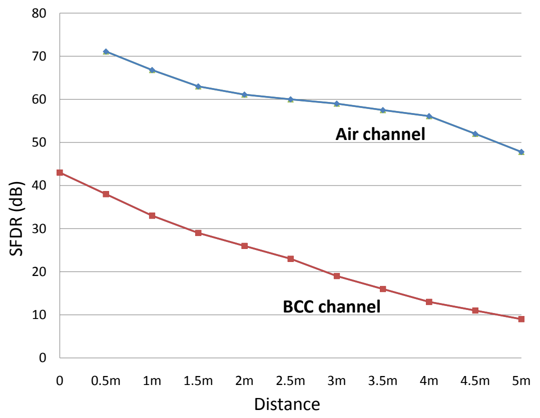

Fig. 6. SFDR as a function of distance using air and BCC channels in the case of active attacks

active attacks, the strength of the received signal from the human body is also much less (30-40 dB) than in the case of conventional communication, thus, making it more difficult to control the insulin pump from some distance away.

However, note that the SFDR of the received signal also depends on the antenna and the output power of the transmitter. Therefore, even though the above experiments show that BCC can help mitigate the security problem, experiments need to be performed for each device in the different attack scenarios in order to confirm the security enhancement.

VI. Conclusion

In this paper, we discussed security and privacy issues related to a current continuous glucose monitoring and insulin delivery system. We showed that through reverse engineering of the radio protocols, both passive and active attacks can be launched on the system using off-the-shelf hardware and software. We then analyzed the various attack scenarios and proposed two types of defenses against them. We believe that the proposed attack methodology and defenses may be applicable to several wearable and implantable medical systems. Medical appliance security is a critical challenge that demands the immediate attention of the research community.

References

[1] "2007 national diabetes fact sheet." [Online]. Available: http://www.cdc.gov/diabetes/pubs/pdf/ndfs_2011.pdf

[2] "US healthcare equipment and supplies – diabetes." [Online]. Available: http://www.research.hsbc.com

[3] "Insulin pumps - global pipeline analysis, opportunity assessment and market forecasts to 2016, GlobalData." [Online]. Available: http://www.globaldata.com

[4] C. Raine, L. Schrock, S. Edelman, S. Mudaliar, W. Zhong, L. Proud, and J. Parkes, "Significant insulin dose errors may occur if blood glucose results are obtained from miscoded meters," *J. Diabetes Science and Technology*, vol. 1(2), pp. 205–210, Mar. 2007.

[5] "Experiences with insulin pump in 52 patients." [Online]. Available: professional.diabetes.org/Abstracts_Display.aspx?TYP=1&CID=70361

[6] N. Leveson and C. Turner, "An investigation of the Therac-25 accidents," *Computer*, vol. 26, pp. 18–41, July 1993.

[7] K. Venkatasubramanian and S. Gupta, "Security solutions for pervasive healthcare," in *Security in Distributed, Grid, Mobile, and Pervasive Computing*. Boca Raton, FL: Auerbach Publications, 2007, ch. 15, pp. 349–366.

[8] P. Kulkarni and Y. Öztürk, "Requirements and design spaces of mobile medical care," *SIGMOBILE Mobile Computing Communications Review*, vol. 11, pp. 12–30, July 2007.

[9] S. Warren, J. Lebak, J. Yao, J. Creekmore, A. Milenkovic, and E. Jovanov, "Interoperability and security in wireless body area network infrastructures," in *Proc. IEEE Int. Conf. Engineering in Medicine and Biology Society*, Jan. 2006, pp. 3837–3840.

[10] O. Garcia-Morchon, T. Falck, T. Heer, and K. Wehrle, "Security for pervasive medical sensor networks," in *Proc. Int. Conf. Mobile and Ubiquitous Systems*, July 2009, pp. 1–10.

[11] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Computing*, vol. 7, pp. 30–39, Jan. 2008.

[12] K. Malasri and L. Wang, "Design and implementation of a secure wireless mote-based medical sensor network," in *Proc. Int. Conf. Ubiquitous Computing*, Sept. 2008, pp. 172–181.

[13] O. Morchon and H. Baldus, "Efficient distributed security for wireless medical sensor networks," in *Proc. Int. Conf. Intelligent Sensors, Sensor Networks and Information Processing*, Dec. 2008, pp. 249–254.

[14] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Security and Privacy*, May 2008, pp. 129–142.

[15] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. ACM Conf. Computer and Communications Security*, 2009, pp. 410–419.

[16] Y. Gao, S. Pun, M. Du, P. Mak, and M. Vai, "Simple electrical model and initial experiments for intra-body communications," in *Proc. IEEE Int. Conf. Engineering in Medicine and Biology Society*, Sept. 2009, pp. 697–700.

[17] S. Pun, Y. Gao, P. Mak, M. Du, and M. Vai, "Simple electrical model and initial experiments for intra-body communications," in *Proc. IEEE Int. Conf. Engineering in Medicine and Biology Society*, Sept. 2009, pp. 693–696.

[18] N. Cho, J. Yoo, S.-J. Song, J. Lee, S. Jeon, and H.-J. Yoo, "The human body characteristics as a signal transmission medium for intrabody communication," *IEEE Trans. Microwave Theory and Techniques*, vol. 55(5), pp. 1080–1086, May 2007.

[19] H. Baldus, S. Corroy, A. Fazzi, K. Klabunde, and T. Schenk, "Human-centric connectivity enabled by body-coupled communications," *IEEE Communications Magazine*, vol. 47, pp. 172–178, June 2009.

[20] T. Schenk, N. Mazloum, L. Tan, and P. Rutten, "Experimental characterization of the body-coupled communications channel," in *Proc. IEEE Int. Symp. Wireless Communication Systems*, Oct. 2008, pp. 234–239.

[21] Y.-T. Huang and R. Rieger, "An OOK body-channel transceiver front-end ASIC for distributed force measurement," *J. Signal Processing Systems*, pp. 1–9, Oct. 2009.

[22] N. Cho, J. Lee, L. Yan, J. Bae, S. Kim, and H.-J. Yoo, "A 60Kb/s-to-10Mb/s 0.37nJ/b adaptive-frequency-hopping transceiver for body-area network," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2008, pp. 132–133.

[23] A. Fazzi, S. Ouzounov, and J. van den Homberg, "A 2.75mW wideband correlation-based transceiver for body-coupled communication," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2009, pp. 204–205.

[24] "USRP." [Online]. Available: http://www.ettus.com/

[25] "GNU radio." [Online]. Available: http://gnuradio.org/

[26] A. Alrabady and S. Mahmud, "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs," *IEEE Trans. Vehicular Technology*, vol. 54, pp. 41–50, Jan. 2005.

[27] M. Novotny and T. Kasper, "Cryptanalysis of KeeLoq with COPACOBANA," in *Proc. Wksp. Special Purpose Hardware for Attacking Cryptographic Systems*, Sept. 2009, pp. 159–164.

[28] H.-J. Yoo, S.-J. Song, N. Cho, and H.-J. Kim, "Low energy on-body communication for BSN," in *Proc. Int. Wksp. Wearable and Implantable Body Sensor Networks*, Mar. 2007, pp. 15–20.