A Visible Light Channel based Access Control Scheme for Wireless Insulin Pump Systems

Jian Zhao and Kam Kong
Dept. of CIS
Delaware State University
Dover, DE 19901, USA
Email: jzhao16@students.desu.edu, kkong@desu.edu

Xiali Hei and Yazhou Tu
School of Computing and Informatics
University of Louisiana at Lafayette
Lafayette, LA 70503, USA
Email: {xiali.hei,yazhou.tu1}@louisiana.edu

Xiaojiang Du
Dept. of CIS
Temple University
Philadelphia, PA 19122, USA
Email: dxj@ieee.org

***Abstract*—Smart personal insulin pumps have been widely adopted by type 1 diabetes. However, many wireless insulin pump systems lack security mechanisms to protect them from malicious attacks. In previous works, the read-write attacks over RF channels can be launched stealthily and could jeopardize patients' lives. Protecting patients from such attacks is urgent.**

To address this issue, we propose a novel visible light channel based access control scheme for wireless infusion insulin pumps. This scheme employs an infrared photodiode sensor as a receiver in an insulin pump, and an infrared LED as an emitter in a doctor's reader (USB) to transmit a PIN/shared key to authenticate the doctor's USB. The evaluation results demonstrate that our scheme can reliably pass the authentication process with a low false accept rate (0.05% at a distance of 5cm).

***Index Terms*—security; wireless insulin pump; visible light channel; access control; patient safety**

I. Introduction

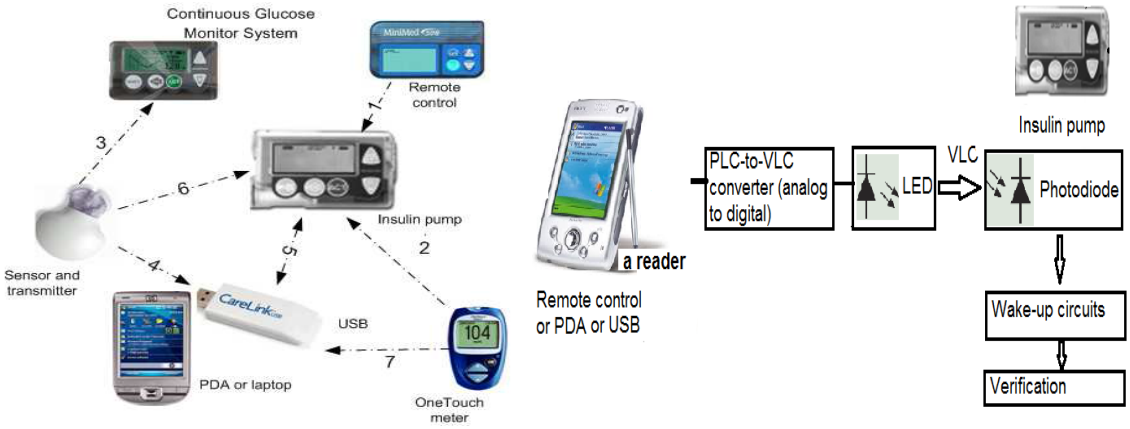
An estimated 30.3 million people of all ages or 9.4% of the U.S. population had diabetes in 2015 [1]. About 5% of people with diabetes are estimated to have type 1 diabetes and need to use insulin pumps. Such devices have security vulnerabilities, and patients all over the world that use such devices may be affected negatively.

These patients deserve a better treatment that employs state-of-the-art technologies to improve their security. Traditionally, the patients with diabetes mellitus use finger-stick to get their blood glucose readings. Currently, the interstitial glucose level can be automatically measured every five minutes via a glucose sensor. Endocrinologists and researchers have attempted to use the wireless insulin pumps with a glucose sensor (see Fig. 1(a)) for the treatment of Type 1 diabetes [4]–[6]. The three components of an insulin pump are 1) a glucose monitor with a glucose sensor, 2) an insulin delivery system, and 3) an algorithm to adjust insulin dosages according to blood glucose levels. In the treatment of Type 1 diabetes, a closed-loop insulin pump system has many advantages over other types of pumps and will become the primary tool in the treatment of diabetes. However, the insulin pump systems (such as MiniMed 640G) with wireless links are vulnerable to read-write attack, jamming attacks, and insulin dosage attacks. Even though FDA [3] guidelines recommend that medical device manufacturers remain vigilant about cybersecurity issues and take the necessary steps to protect patients from potential security risks, most of today's commercial medical devices do not have enough security mechanisms embedded in their hardware/software to mitigate such risks. It is critical to fill the gap and make the wireless insulin pump system highly secure to help the patients.

There exists a wireless link between the pump and the sensor via an insecure channel. Due to oxygenizement, the lifetime of the sensor is one week to one month, and the patient is required to calibrate it every 12 hours. The sensor continually sends the glucose level readings to the pump. If the sensor gets an ultra-low glucose level reading, it will send the commands to stop the infusion of a pump. Figure 1 shows the components of a Medtronic Paradigm real-time insulin pump system. The OneTouch meter obtains blood glucose readings from the patients' manual tests. The blood glucose level is sent from the OneTouch meter to the insulin pump via wireless link 2 (we have numbered each wireless link). The sensor tests the patient's interstitial glucose level and sends the readings to a continuous glucose monitor system (CGMS) via wireless link 3, and to the pump via wireless link 6. Wireless links 2, 3, and 6 are vulnerable to the same attacks. The insulin pump then delivers insulin to the patient. The patient can operate a remote control unit to send instructions (such as suspend and resume basal dosage) to the insulin pump via wireless link 1. Note that wireless links 4 and 7 transmit historical glucose readings to a Carelink USB device. Wireless link 5 allows the Carelink USB device to gather reports on blood glucose readings. Wireless link 6 sends current glucose readings to the pump. Carelink USB device is used by a patient to upload data to a web-based management system. Compromising wireless links 1, 3, 5, and 6 was demonstrated in [8] and [7].

In this paper, we will investigate an innovative approach to secure the link 5 through a visible light communication (VLC) channel. Most conventional wireless security uses 'radio' signals (such as Wi-Fi bands). The radio propagation properties have been well studied, and radio communication can be easily attacked by remote entities. VLC power drops off as d^4 instead of d^2 because VLC uses a square-law receiver instead of a field receiver (RF antenna). Thus, when the power of infrared LED is ultra-low, it makes the communication range very short. Visible light can be controlled to travel extremely short distances (<10cm) and requires the sender and receiver

978-1-5386-3180-5/18/$31.00 ©2018 IEEE



(a) A real time insulin pump system [9]

(b) VLC channel for writing data

Fig. 1. System components

to be facing each other unobstructed. Thus, it is impossible for an attacker to hide 10cm away to launch attacks. Light signals can be modulated to generate unique keys as well. The transmission rate of visible light is 10-100 times higher than the radio signals. Thus, the transmission time of a message between the insulin pump and remote controller is short, which leaves the attacker a much ***shorter attack time*** compared to radio links. Finally, the hardware is easy to add on to the Carelink USB and insulin pumps by adding necessary circuits. When a user/nurse turns on the LED in the USB/reader by pressing a button, he/she will start the authentication and data transmission over the VLC channel. The algorithms in the insulin pump will verify the password/PIN transmitted.

The visible light signals can supplement the well-studied radio channels in conventional wireless medical device access, and can be used for the following crucial case: secure pump access via visible light signals; when a doctor wants to read data from or write commands to an insulin pump, the visible light channel will be used to guarantee secure, short distance, well-aligned communications between a reader/USB and the insulin pump.

Contribution. A wireless insulin pump provides the convenience and reduces the cost of medical care for Type 1 diabetes patients. Currently, these devices have no security schemes in their hardware and software units. The proposed activities aim to overcome typical reader/pump attacks and to protect the scheduling of remote insulin delivery. The mixed visible light and radio signal's secure communication channels can address the security concerns in an implantable insulin pump.

The main contributions of this paper can be summarized as follows:

- We first propose the use of a visible light channel to protect the medical devices.
- We implement a visible light channel prototype on two Arduino Uno-R3 boards.
- The evaluation results demonstrate that our scheme can reliably pass the authentication with a low false accept rate (0.05% at a distance of 5cm).

The remainder of this paper is organized as follows: In Section II, we discuss the related work. In Section III, we describe the background and attack models. We analyze a visible light channel based access control scheme for wireless insulin pumps in Section III. B. In Section IV, we describe our experimental results. We present related discussions in Section V, and we conclude the paper in Section VI.

II. Related Work

A. Attacks on medical devices

In 2008, Halperin et al. found that some IMDs are vulnerable to attacks. They suggested balancing between security and effectiveness [17]. Then, Halperin et al. gave a security analysis of Implantable Cardioverter Defibrillator (ICD). They could use radio-based attacks to comprise the ICD. In 2011, two attacks targeted at wireless insulin pumps were demonstrated [7], [8]. They could deliver lethal dosages by sending malicious commands over the air. In 2013, Li et al. showed different types of attacks on an insulin pump in [16]. They used reverse-engineering technology to attack the insulin pump. Then, in 2016, Eduard Marin extended their attacks by fully reverse-engineering the wireless communication protocol among all of the peripherals of the insulin pump system [33]. Measurements in paper [27] show that intentional EMI under 10W can inhibit pacing and induce defibrillation shocks implantable cardiac electronic devices.

B. Countermeasures

In recent years, some countermeasures have been proposed by researchers to mitigate the vulnerabilities of implantable medical devices (IMDs). Authors of [17], [28], [29] tried to devise energy-aware security techniques. Authors of [18], [19], [21] proposed utilizing an additional external devices. Rasmussen et al. proposed to allow IMDs to emit an acoustic alert when processing a transaction [20]. Our previous work [10], [11], [24], [25] discussed various access control schemes for wireless medical devices. The authors of [23] proposed using friendly jamming to mitigate adversarial accesses to IMDs. We are finalizing another paper that discusses closed-loop control attacks targeting insulin pumps. In 2011, Paul

et al. examined insulin pump system security and privacy in [12]. In 2015, O'Keeffe et al. discussed Cybersecurity in an AP experiment [13]. A cryptographic solution (rolling code) and body-coupled communication were used to protect the wireless links in [16], [26]. However, the attack in [7] exploited a vulnerability between the Carelink USB and the pump. Authors of [32] built a generic insulin infusion pump model and presented a corresponding hazard analysis. Authors of [31] identified a set of safety requirements that can be formally verified against pump software. Li et al. issued the use of rolling codes to protect against unauthorized access [16]. First, some rolling codes do not offer strong authentication. Second, there was no detailed introduction for how to update and revoke the shared encryption key between the remote control and insulin pump. Key management [34]–[36] is also essential for wireless security. In 2011, Gollakota et al. proposed a solution with an external device, known as "shield." However, the "shield" has not been tested for the insulin pumps. In 2013, Hei et al. proposed anomalous detection to solve the problem. They recorded the glucose log to detect anomalous behaviors. Unfortunately, a false alarm resulted at times from a frequent detection rate.

All of those works are based on general well-studied radio signal channels and can be easily attacked by remote entities that have sound knowledge of the radio propagation patterns. Komine et al. conducted a fundamental analysis for VLC systems in [14] and opened this area. Rajagopal et al. demonstrated a VLC channel using LEDs and a device with cameras in [15]. Those schemes are primarily based on digital security that uses interpretable digital signals to deliver information. This paper will use special analog signals (visible light signals) that have not been popularly used in security fields, as well as analog security technologies to enhance IMD security. Those special analog signals do not have easy-to-interpret patterns and are built on unique analog modulations, and thus can better protect patient medical information.

III. System and Attack Models

Our main hypothesis is that we can establish the communication channel and maintain its security against jamming and safety for the patient by utilizing the optical channel. Regarding the threat model, we assume that the attacker can use Carelink USB to remotely control the insulin pump by forging the radio signals. Also, we assume that the attacker cannot be within a range of 10cm from the patient.

A. Read/Write Attack over Wireless

Given the wireless insulin pump system, we discuss potential attacks. A serial number of an insulin pump need to be manually entered to connect it to a Carelink USB device wirelessly. After establishing the wireless connections among all components, the insulin pump can display blood glucose (BG) readings from sensors and adjust dosages accordingly.

Since all the wireless links in the system are not encrypted, attackers can compromise the wireless links easily. By compromising the wireless links, attackers can conduct various malicious actions. For instance, attackers could display incorrect BG readings on the insulin pump via link 2 as Radcliffe demonstrated. Also, an attacker can suspend the basal rate delivery using link 1. We do not discuss such kind of attack in our paper because it can be noticed by patients.

The pump settings could be modified by insulin pump users via Carelink Pro software on a computing device. The new settings could be uploaded to the pump using the attached Carelink USB device via wireless link 5. As a result, attackers may use customized software and a wireless sniffer to obtain the serial number of all pumps within 300 feet, and can, therefore, compromise wireless link 5 to change the settings of the pump without being noticed. Using this security flaw, an attacker can 1) disable the alarms of the pump, 2) change the maximum allowable dosage of the pump, and 3) deliver a fatal dose to the insulin pump user [7], [8]. The delivery of a lethal dose is life-threatening and must be prevented.

In this paper, we focus on the attacks that are based on the compromised wireless link 5. The authentication scheme is critical. However, the existing authentication with a passcode is not secure because the attackers can eavesdrop the radio signals from a long distance. Right now, there is no authentication scheme over wireless link 5. In this paper, we build a visible light channel based authentication scheme for wireless link 5.

B. Visible light channel (VLC) based access control

Over wireless link 5 (see Figure 1(a)), the attacker can remotely change settings and schedule dosages on the pump. Our previous infusion-based detection scheme cannot be applied in the wireless insulin pumps with closed-loop control because it requires the patient to manually enter the glucose level. Although the pump has efficient resources, such as rechargeable battery and high power microcomputer, the processor speed that the pump uses is low. This leads us to investigating other ways of making wireless link 5 secure without using a fixed shared key.

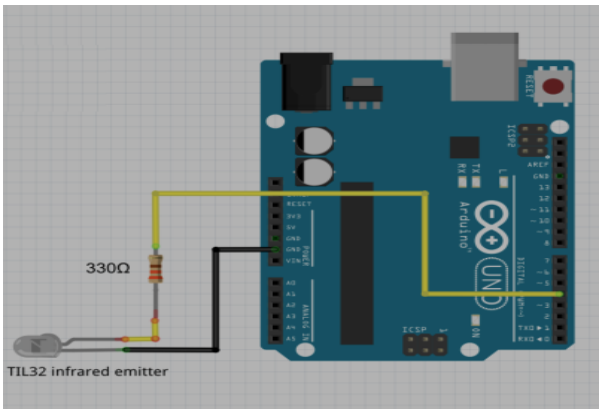
To solve the above issues, we propose a human-aware, visible light based insulin pump access control scheme. The visible light can be controlled to travel within an extremely short distance (<15cm), and requires non-blocking direct sender-receiver facing. This makes it impossible for an attacker to hide somewhere 15cm away to launch jamming attacks. Fig. 1(b) illustrates the idea of the VLC channel for an insulin pump and a remote reader. It shows the secure pump writing operation. The wireless channel is based on VLC. When the nurse wants to send a dosage to the pump, he or she can press a button on the USB or remote control and powers the LED. The external reader sends the LED signals by properly facing the pump, and the pump verifies the PINs or a shared key. For the secure pump data writing (such as sending an external control command to the pump), we add a small LED wake-up circuit (simpler than general RF circuit) to the remote reader and pump. When the visible light signal wakes up the receiver, and the receiver in the insulin pump recognizes the

PINs or shared key, the authentication is completed. Fig. 1(b) illustrates an authentication process.

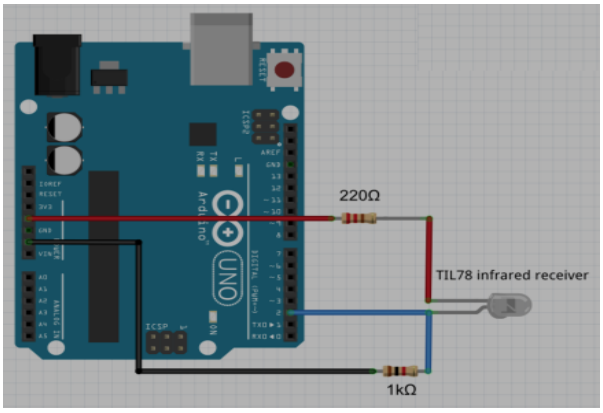
We propose one approach to conduct the access control for a wireless insulin pump. It is to transmit the pre-configured PIN/key to authenticate because the visible light of low-power LED can guarantee the directionality and range of communication. [30] shows that when the communication range is 100cm, and the transmission power is 5W, the attacker at a distance of 15cm cannot successfully eavesdrop on the transmitted message. In our work, the power used is far lower than 5W, making it extremely difficult for an attacker to eavesdrop within a 10 cm radius around the patient. Visible light propagation is different from the multi-path fading model of conventional radio signals. It depends on the angle, transmitted power, luminous intensity, dimming, shadowing, photometric and radiometric parameters, and other parameters as well as the patient's circuitry. We build a visible light prototype to simulate the mutual authentication between medical devices.

IV. Experiments for VLC-based Access Control

A. Experimental Results



(a) Circuits to send the visible light signals



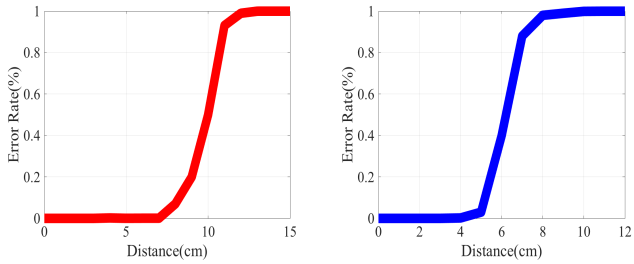
(b) Circuits to receive the visible light signals

Fig. 2. Circuits of VLC channel

In our experiments, we use two Arduino Uno-R3 boards with ATmega328 (8-bit 1M CPU), a photodiode TIL 32, a photodiode TIL 78, a 220 Ohm resistor, a 330 Ohm resistor, and a 1k Ohm resistor to build a proof-of-concept VLC secure channel prototype and conduct the experiments. Fig. 2(a) and Fig.2(b) show the circuits we use. Implementation of the VLC secure channel on pumps is challenging. In this project, we choose Arduino Uno R3 as the microcontroller, and we choose an infrared LED to save the energy and space. When using an infrared LED as an emitter in a doctor's reader, there are three challenging problems: (1) Customization of the LED work frequency using a low consumption circuit; (2) Extraction of the features of the LED signals; (3) Adjustment of the LED signals. To use the infrared photodiode as a receiver in the insulin pump, there are also two challenging problems to be solved: (1) Extraction of the features of the LED signals; (2) Quantification of the energy consumption. Besides these challenges, we also develop the threshold adjustment method in the receiver. During the daytime and nighttime, the thresholds are different. They vary with the light intensity of the LED and environmental light.

TABLE I
False Accept Rate and False Reject Rate

Distance(cm)	FAR(%)	FRR(%)
1	0.00	0.00
2	0.00	0.00
3	0.00	0.00
4	0.01	0.01
5	0.05	0.05
6	0.06	0.06
7	0.07	0.07
8	7	7
9	20	20
10	50	50



(a) Daylight Result (b) Night Result

Fig. 3. Experimental Results

We sent 3000 10-letter passwords through the visible light for each distance to test the visible light channel. From Table I, we can find the false accept rate (FAR) and false reject rate (FRR) of different distances. When the distance is 5 cm, the FAR and FRR are 0.05%. We think this is a usable distance for the USB/reader and insulin pump. When the distance is 10 cm, the FAR and FRR are 50%. This makes the eavesdropping difficult when the attacker is farther than 10 cm away from the patient. The password error rates have the same trend. As demonstrated in Fig. 3, within a distance of 5 cm, the password error rate is 0. Then, during the day, the password error rate increases sharply when the distance is 7 cm, while during the

night, the bit error rate increases sharply when the distance is 5 cm. In both cases, when the distance is longer than 12 cm, the password error rate is 100%. This means that the VLC communication will fail when the distance is longer than 12 cm. Thus, it is very difficult for the attacker to eavesdrop the messages if he/she is not be very close to the patient.

V. Discussions

A. Overhead Analysis

Our prototype requires approximately 0.5ms to finish the visible light channel based PIN/key authentication. The energy consumed is negligible compared with ordinary therapy or communication. Furthermore, the verification time of our scheme is short, which is very important in regards to the patient's convenience. Our scheme needs to store two algorithms for visible light wake-up and PIN verification in the insulin pump. All of the storage requirements are acceptable to today's insulin pumps. According to the datasheet of ATmega328, when the microcontroller actively works at 1Mhz, the power consumption is 0.5ms*1.8V*0.2mA=0.18μJ, which is insignificant cost compared the main cost of a pump's other operations.

B. Security Analysis

1) Defending Against the Read/Write Attack: If a hacker wants to remotely send a dosage to the insulin pump, he or she should be within 10 cm of a patient and have an LED built-in his/her reader and know the pre-configured PIN/key. 10 cm is an offensive distance for most people. Besides, he/she has to be in the line of LED and pump. This condition makes the eavesdropping is extremely difficult. Therefore, our communication distance-bound access control can defend against this attack. We checked various visible light channels and found that VLC power drops off as d^4 instead of d^2 as wireless radio because VLC uses a square-law receiver instead of a field receiver (RF antenna). Thus, when the power of infrared LED is ultra-low, it makes the eavesdropping even harder. The simulation and rigorous analysis are out of the paper's scope.

C. Emergency Situations

Many researchers suggested using open access operated by clinical staff during emergencies, e.g., in [18], [19], and [20]. To handle the emergency situation, we also can deactivate our scheme. Some literatures (e.g. in [11] and [22]) focused on the emergency case. Thus, in this paper, we can deactivate the visible light channel based access control scheme to allow open access to wireless insulin pumps.

VI. Conclusion

For wireless insulin pump systems, there are several read/write attacks that are related to remote dosage setting, and the vulnerability comes from no authentication on wireless link 5. In this paper, we proposed a visible light channel based access control scheme that can defend against these attacks. Our scheme leverages the user's involvement to push the button, turn on the LED, send the visible light signals to a pump's reader, and conduct the authentication. The evaluation results demonstrate that our scheme can reliably pass the authentication with a low false accept rate (0.05% at a distance of 5 cm). Our scheme can be generalized to other infusion systems as well. VLC channel also provides an alternative approach to transmit critical data between the insulin pump and readers. Working on a general out-of-band VLC channel is our future work.

Acknowledgment

This work was supported in part by US NSF under grants CNS-1812553.

References

[1] Centers for Disease Control and Prevention, "National Diabetes Statistics Report: Estimates of Diabetes and Its Burden in the United States, 2017". https://www.cdc.gov/diabetes/pdfs/data/statistics/national-diabetes-statistics-report.pdf.

[2] http://www.computerworld.com/article/2981527/cybercrime-hacking/researchers-hack-a-pacemaker-kill-a-man-nequin.html

[3] http://news.medterasolutions.com/pharmaceutical-medical-devices/manufacturers-face-new-restrictions-on-medical-devices/

[4] G. M. Steil, K. Rebrin, C. Darwin C, F. Hariri, and M. F. Saad, "Feasibility of automating insulin delivery for the treatment of type 1 diabetes," *Diabetes* vol.55, pp: 3344-3350, 2006.

[5] G. M. Steil, K. Rebrin, R. Janowski, C. Darwin , and F. Saad, "Modeling β-cell insulin secretion: implications for closed-loop glucose homeostasis," *Diabetes Technol Ther*, vol.5, pp: 953-964, 2003.

[6] G. M. Steil, A. E. Panteleon, and K. Rebrin, "Closed-loop insulin delivery: the path to physiological glucose control," *Adv Drug Deliv Rev*, vol. 56, pp: 125-144, 2004.

[7] http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack.

[8] J. Radcliffe. https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf

[9] X. Hei, X. Du, S. Lin, and I. Lee, "PIPAC: Patient Infusion Pattern based Access Control Scheme for Wireless Insulin Pump System," in *Proc. of IEEE INFOCOM 2013*, Turin, Italy, Apr. 2013.

[10] X. Hei, X. Du, J. Wu, and F. Hu, "Defending Resource Depletion Attacks on Implantable Medical Devices," in *Proc. of IEEE Globecom'10*, pp. 1-5, 2010.

[11] X. Hei and X. Du, "Biometric-based Two-level Secure Access Control for Implantable Medical Devices during Emergencies," in *Proc. of IEEE INFOCOM'11*, pp. 346-350, 2011.

[12] N. Paul and T. Kohno, "Security Risks, Low-tech User Interfaces, and Implantable Medical Devices: A Case Study with Insulin Pump Infusion Systems", in the proceeding of Usenix Conference Healthsec'12, 2012. https://www.usenix.org/system/files/conference/healthsec12/healthsec12-final17.pdf

[13] D. T. O'Keeffe, S. Maraka, A. Basu, P. Keith-Hynes, and Y. C. Kudva, "Cybersecurity in Artificial Pancreas Experiments", Diabetes Technol Ther. 2015 Sep, vol. 17, no. 9, pp. 664-666, doi: 10.1089/dia.2014.0328, Epub 2015 Apr 29.

[14] T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights", *IEEE Transactions on Cosumer Electronics*, vol. 50, no. 1, pp. 100-107, Feb. 2004.

[15] N. Rajagopal, P. Lazik, and A. Rowe, "Hybrid visible light communication for cameras and low-power embedded devices", in *Proc. of ACM VLCS'14*, Maui, Hawaii, USA, Sep. 2014.

[16] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System", in *Proc. of the 13th IEEE Intl. Conf. on e-Health NAS*, pp. 150-156, 2011.

[17] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses," in *Proc. of the 2008 IEEE Symp. on SP'08*, pp. 129-142, 2008.

[18] P. Inchingolo, S. Bergamasco, and M. Bon, "Medical data protection with a new generation of hardware authentication tokens," in *Proc. of Mediterranean Conf. on Medical and Biological Engineering and Computing*, 2001.
[19] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: new directions for implantable medical device security," in *Proc. of the 3rd Conf. on Hot topics on security*, pp. 1-7, 2008.
[20] K. B. Rasmussen, C. Castelluccia, T. Heydt-benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. of ACM CCS '09*, pp. 410-419, 2009.
[21] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *Proc. ACM Conf. SIGCOMM'11*, pp. 2-13, 2011.
[22] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: Cryptography Based Secure EHR System for Patient Privacy and Emergency Healthcare," in *Proc. of ICDCS'11*, pp. 373-382, 2011.
[23] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. of IEEE INFOCOM'11*, Shanghai, China, Apr. 2011.
[24] X. Hei, X. Du, "Security in Wireless Implantable Medical Devices," Springer, hardcopy ISBN 978-1-4614-7152-3, online ISBN 978-1-4614-7153-0, published in April 2013.
[25] X. Hei, X. Du, and S. Lin, "Poster: Near Field Communication based Access Control for Wireless Medical Devices", in *Proc. of ACM MobiHoC 2014*.
[26] Ch. Li, "System design and verification methodologies for secure computing", *PhD Thesis*, 2012.
[27] D. F. Kune, J. Backes, S. S. Clark, D. B. Kramer, M. R. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors", in *Proc. of the 34th IEEE Symp. on SP'13*, pp. 1-15, May 2013.
[28] S. Hosseini-Khayat, "A lightweight security protocol for ultra-low power asic implementation for wireless implantable medical devices", in *Proc. of IEEE ISMICT'11*, pp. 6-9, 2011.
[29] C. Beck, D. Masny, W. Geiselmann, and G. Bretthauer, "Block Cipher Based Security for Severely Resource-constrained Implantable Medical Devices", in *Proc. of ACM ISABEL'11*, pp. 62:1-62:5, 2011.
[30] C. Chow, Y. Liu, C. Yeh, C. Chen, C. Lin, and D. Hsu, "Secure communication zone for white-light LED visibe light communication", Optics Communications, vol. 344, pp. 81-85, 2015.
[31] R. Jetley and P. Jones, "Safety Requirements based Analysis of Infusion Pump Software," in *Proc. of the Workshop on Software and Systems for Medical Devices and Services*, pp. 21-24, 2007.
[32] Y. Zhang, P. Jones, and R. Jetley, "A Hazard Analysis for a Generic Insulin Infusion Pump," *J. of Diabetes Sci. and Technol.*, vol. 4, no. 2, pp. 263-283, 2010.
[33] E. Marin, D. Singelée, B. Yang, I. Verbauwhede and B. Preneel, "On the feasibility of cryptography for a wireless insulin pump system," in *ACM Proc. of the Sixth ACM Conference on Data and Application Security and Privacy*, pp. 113-120, 2016.
[34] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, "An Effective Key Management Scheme for Heterogeneous Sensor Networks," *Ad Hoc Networks, Elsevier*, Vol. 5, Issue 1, pp 24C34, Jan. 2007.
[35] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks," *Journal of Computer Communications*, Vol. 30, Issue 11-12, pp. 2314-2341, Sept. 2007.
[36] X. Du, M. Guizani, Y. Xiao and H. H. Chen, "A Routing-Driven Elliptic Curve Cryptography based Key Management Scheme for Heterogeneous Sensor Networks," *IEEE Transactions on Wireless Communications*, Vol. 8, No. 3, pp. 1223 - 1229, March 2009.