

# Insulin Pump System Security and Privacy

Nathanael Paul, Ph.D.  
CSIIR<sup>\*†</sup>

Oak Ridge National Laboratory  
npaul@ornl.gov

David C. Klonoff, M.D., FACP  
Mills-Peninsula Health Services  
Diabetes Research Institute  
dklonoff@yahoo.com

## Abstract

Physicians are using medical devices to treat an array of sicknesses including Parkinson's, Alzheimer's, pain, gastroparesis, diabetes, and heart disease. Among other features, many of these devices now include the ability to wirelessly interface with a patient or other devices. To address threats on data integrity and privacy, secure solutions in medical device systems, particularly insulin pump systems, are needed.

In this paper we discuss issues including peripheral component threats, their usability, and their regulation. These issues are important to a safe and effective medical device system deployment.

## 1. Introduction

With the introduction of wireless capabilities in medical devices for improved and more convenient treatment, vulnerabilities have emerged. Through our current research, we have noted developing areas that need attention in medical device security. In this paper we focus on insulin pump systems. In particular, we focus on peripheral system devices, usability, and regulation. While medical researchers do not typically focus on these areas, they could pose obstacles to the safety and effectiveness of these medical devices.

In February, 2010 we notified the FDA of vulnerabilities in insulin pump systems (direct attacks were implemented at our lab) and other potential security problems. We note that malicious intent is needed for these problems, and we are currently working to better understand the problems with these devices. This experience has given us additional insight into medical device security challenges. In a future paper, we will explicitly detail our results and solutions.

## 2. Insulin Pump System Threat Model

Based on our current research and experience with insulin pumps, certain areas of interest are especially important. While some of these have been discussed in previous research literature [Halperin08, Klonoff08], our experience has taught us lessons that certain medical device system threats remain unnoticed. In this section we present a medical device system model within the context of an insulin pump system.

A *medical device system* includes the patient, the physician, the medical device hardware, its software, its data, and any component (hardware or software) or accessory that is designed to be indirectly used with or directly interact with a medical device. We consider components and accessories, because they can influ-

ence the medical device's operation both directly and indirectly.

For an insulin pump, the medical device is the pump itself. Components that can directly interact with the insulin pump include patients, physicians (i.e., healthcare assistants), blood glucose monitors, continuous glucose monitors, and insulin pump remote controls. These mechanical devices now directly interface via radio frequency communication to the insulin pump. The patient and physician interact with each and every device.

Indirectly used components include smartphones [Apple09] and non-wireless blood glucose monitors. While no one has used a smartphone as an insulin pump remote control, this type of device can be used to check blood glucose and help calculate insulin boluses (A pump delivers a *bolus* of insulin in response to a patient command).

In the rest of this section, we discuss peripheral component threats, and our motivating example is the use of a smartphone to control or monitor an insulin pump system. By analyzing a component of insulin pump systems that has not yet been widely deployed, we wish to highlight potential attacks on data integrity and privacy.

**Indirect Attack.** If malware were installed on the phone, then the malware could cause harm by changing stored glucose values or bolus calculations. A physician or patient may use these values in programming a patient's insulin pump. If these values were maliciously or unintentionally changed, then either the physician or patient could unwittingly endanger the patient's life by delivering an incorrect dose of insulin which would result in hyperglycemia, or worse, hypoglycemia.

Many smartphone applications can help physicians remember normal population lab measurement values (e.g., typical blood glucose values). While helpful, if malware could change these values, then a physician's subsequent treatment based on these incorrect lab values could harm a patient (e.g., a physician using blood glucose values of 50-100 mg/dl instead of 80-120 mg/dl might order too much insulin and inadvertently induce hypoglycemia).

In addition to data integrity, privacy is another difficult problem. By storing blood glucose values on a smartphone, any software could have access to this data. To satisfy integrity and privacy requirements, this data needs very strict protection.

In this threat model, we have detailed what malware could accomplish, but the same is true of any

\* Cyberspace Sciences and Information Intelligence Research Group

† Prepared by Oak Ridge National Laboratory, P.O. Box 2008, Oak Ridge, Tennessee 37831-6285, managed by UTBattelle, LLC, for the U.S. Department of Energy under contract DE-AC05-00OR22725.

installed smartphone application. Any application could have similar, although unintentional, effects. There is potential risk if a smartphone is part of a medical device system. Components that have not been designed for direct interaction with a medical device might be insecure, and system designers must take care in the design of an entire medical device system.

**Direct Attack.** In addition to using a smartphone as a peripheral device, there are those implantable medical devices that can receive direct wireless communication [Halperin08]. Similar to the described indirect attacks, malware could use a smartphone to control an insulin pump if a phone was used for controlling a medical device.

Currently, there is little need for remote control of insulin pumps over a great distance, but protocol implementations do exist that allow remote control from greater distances (e.g., well outside of the patient's arm length). Although some medical devices may need more powerful communication between system components, we argue for near-field communication. While near-field communication does not make a device secure, remote attacks become more difficult.

If there is a need for communication over longer distances, an additional device may be used, but care must be taken to not overburden the patient with this additional device requirement. An example in an insulin pump system is a patient in a hospital setting. As a nurse walks down the hall, she could remotely communicate with each patient's device. If near-field communication were enforced with any patient's insulin pump, an additional proxy device could enable the nurse's communication without burdening the patient.

At this time, there is no central system which communicates with a network system of medical devices such as a set of insulin pumps or continuous glucose monitors, but such a network could be created in the future.

### 3. Usability and Regulatory Aspects

As we attempt to solve these insulin pump system threats, many peripheral issues are equally important. If a device were secure but unusable because of user-unfriendly security features, then the product would not be commercially viable.

**Usability.** Recently, there has been productive research in both medical devices and radio frequency systems to help secure these devices. One technically successful approach is the addition of an extra security device to a system [Denning08, Rieback05]. However, many patients already dislike the burden of insulin pump therapy, and carrying or wearing an additional device would be a difficult proposition. A secure solution must account for patient acceptance.

**Regulation.** The problems presented in this paper are new, because they pose intentional attacks rather

than unintentional interference. Because little regulatory guidance currently exists for manufacturers in making secure medical devices, additional guidance from the FDA will be very helpful to deal with these security challenges [Zhang10].

### 4. Conclusion

With the addition of new data and control capabilities in medical device systems, these devices are becoming more susceptible to attack. As secure devices are developed, both direct and indirect attacks should be considered. We have introduced a model of an insulin pump system and described attacks on peripheral components that are designed to interact both directly and indirectly with insulin pumps. Future insulin pump system designs should defend against these threats.

In securing devices against malicious threats, other challenging issues including usability and regulation play an important part in making these devices safe and effective. We believe these issues need to be solved in parallel for an effective solution.

### 5. References.

- [Apple09] Tim Gee. Apple Targets Health Care with iPhone. Mar. 19, 2009. <http://medicalconnectivity.com/2009/03/19/apple-targets-health-care-with-iphone-30-os/>.
- [Denning08] Tamara Denning, Kevin Fu, Tadayoshi Kohno. Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security. In *Proceedings of the 3rd USENIX Workshop on Hot Topics in Security*. July 29, 2008.
- [Halperin08] Daniel Halperin, et al. Security and Privacy for Implantable Medical Devices. *IEEE Pervasive Computing*. 7(1):30-39. Jan.-Mar. 2008.
- [Klonoff08] David C. Klonoff. Designing an Artificial Pancreas System to Be Compatible with Other Medical Devices. In *Proceedings of the Journal of Diabetes and Technology*. 2(5):741-745. Sept. 2008.
- [Rieback05] Melanie R. Rieback, Bruno Crispo, Andrew S. Tanenbaum. RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. In *Proceedings of the 10th Australasian Conference on Information Security and Privacy*. July 2005.
- [Zhang10] Yi Zhang, Paul L. Jones, and David C. Klonoff. Second Insulin Pump Safety Meeting: Summary Report. 4(2):488-493. Mar. 2010.