Journal of Diabetes Science and Technology
Volume 5, Issue 6, November 2011
© Diabetes Technology Society

REVIEW ARTICLE

A Review of the Security of Insulin Pump Infusion Systems

Nathanael Paul, Ph.D.,[1] Tadayoshi Kohno, Ph.D.,[2] David C. Klonoff, M.D., FACP[3]

Abstract

Insulin therapy has enabled patients with diabetes to maintain blood glucose control to lead healthier lives. Today, rather than injecting insulin manually using syringes, a patient can use a device such as an insulin pump to deliver insulin programmatically. This allows for more granular insulin delivery while attaining blood glucose control. Insulin pump system features have increasingly benefited patients, but the complexity of the resulting system has grown in parallel. As a result, security breaches that can negatively affect patient health are now possible.

Rather than focus on the security of a single device, we concentrate on protecting the security of the entire system. In this article, we describe the security issues as they pertain to an insulin pump system that includes an embedded system of components, which include the insulin pump, continuous glucose management system, blood glucose monitor, and other associated devices (e.g., a mobile phone or personal computer). We detail not only the growing wireless communication threat in each system component, but also describe additional threats to the system (e.g., availability and integrity). Our goal is to help create a trustworthy infusion pump system that will ultimately strengthen pump safety, and we describe mitigating solutions to address identified security issues.

J Diabetes Sci Technol 2011;5(6):1557-1562

Introduction

Since 2000, numerous pump features have helped significantly in attaining better glycemic control, including immediate and longer duration boluses, continuous glucose monitors (CGMs), tighter programmatic basal rate control, and increased connectivity with other insulin pump system components. All these features help achieve better hemoglobin A1c values, and patients have greatly benefited. Unfortunately, while the clinical benefits of these devices have increased, new safety risks have also emerged. New features bring increased complexity to the system, and it is becoming more difficult to assess safety and information security. From 2005 to 2009, there were 56,000 adverse events in infusion pump systems (the total number of affected systems is unknown), with 45% of those adverse events attributed to insulin pumps.[1,2]

Author Affiliations: [1]Oak Ridge National Laboratory, University of Tennessee, Oak Ridge, Tennessee; [2]University of Washington, Computer Science and Engineering, Seattle, Washington; and [3]Diabetes Research Institute, Mills-Peninsula Health Services, San Mateo, California

Abbreviations: (BGM) blood glucose monitor, (CGM) continuous glucose monitor, (FDA) Food and Drug Administration, (PC) personal computer

Keywords: communication, integrity, privacy, safety, security, wireless

Corresponding Author: Nathanael Paul, Ph.D., Oak Ridge National Laboratory, University of Tennessee, 1 Bethel Valley Rd., P.O. Box 2008, Building 5300, MS-6418, Oak Ridge, TN 37831-6418; email address npaul@ornl.gov

The rest of this article addresses the security of insulin pump systems in order to avoid more problematic issues. Our approach is motivated by the patient's goal: to maintain a euglycemic blood glucose level. We wish to protect against a breach in insulin pump system security that could result in hyperglycemia or hypoglycemia. While patients should continue to use their systems, as the benefits far outweigh the risks, as with other classes of medical devices,[3] secure insulin pump system designs are needed. There exists evidence of willful harm to patients (e.g., Tylenol bottles contaminated with cyanide and animated, seizure-inducing images posted on epilepsy support websites). We must ensure that similar risks do not arise for insulin pump system patients.

We define an insulin pump system in this article as a Food and Drug Administration (FDA) class II system of components that contains an insulin pump and any other device that may interact directly with or be used indirectly with the insulin pump device. This definition differs from the FDA's definition of an infusion pump system (e.g., issued in April 2010 concerning infusion pump premarket notification[4]) in that it includes devices that do not directly connect with the insulin pump, and it does not include any part of the infusion set. In some insulin pump systems, there is an insulin pump, a wireless insulin pump remote control, a (wireless) glucose monitor that is used to check the patient's blood glucose, and a CGM system that continuously provides glucose data to the insulin pump.

Figure 1 depicts an example of an insulin pump system. Older systems had isolated devices that were incapable of wireless communication, but with time, newer systems added communication features to components. Once-isolated noncommunicating components can now bidirectionally communicate with the insulin pump or with each other.

There are essentially two types of deployed insulin pump system models: tubed and tubeless (i.e., "patch pumps"). Tubed pumps have the insulin pump worn external to the body, not necessarily in contact with the body; the pump contains a reservoir of insulin that is pumped through a tube that connects to the body subcutaneously via a cannula. Patch pump architecture[5,6] has been introduced and eliminates the long tubing of the tubed architecture with its direct attachment to the body. We differentiate between these two designs because their architectural differences fundamentally affect the way one approaches security.

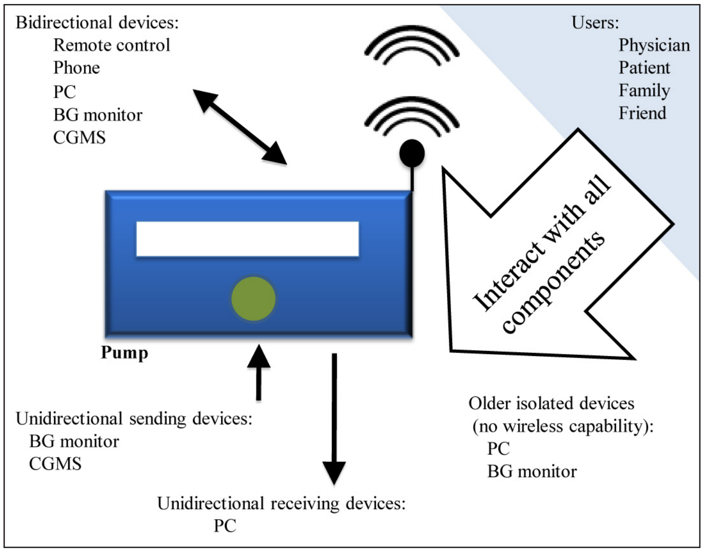
Bidirectional devices:
Remote control
Phone
PC
BG monitor
CGMS
Users:
Physician
Patient
Family
Friend
Interact with all components
Pump
Unidirectional sending devices:
BG monitor
CGMS
Older isolated devices (no wireless capability):
PC
BG monitor
Unidirectional receiving devices:
PC

Figure 1. Insulin pump system

Solutions Under a Risk-Management Approach

In February 2010, we discovered certain insulin pump system vulnerabilities stemming from unauthorized wireless access, and notified the FDA. Since that time, we have been working to solve the identified problem areas: (1) ensuring remote control is done by preapproved individuals (i.e., the patient or patient's physician); (2) maintaining the integrity of glucose data (i.e., detecting changes to measured glucose results); (3) maintaining integrity of system settings; (4) addressing system communication availability; (5) ensuring software has not been undetectably altered; and (6) enhancing safety of new wireless consumer devices (e.g., a mobile phone). While many problem areas can be addressed with existing security mechanisms, adequately addressing identified threats for all stakeholders is challenging. In some cases, novel research is needed to mitigate the risk. In each proposed solution, our goal is not only to design a secure technical solution but also to avoid impeding safety and effectiveness. In addition to safety and security, other factors that must be addressed are:

User acceptance. Patient and health care workers should be able to use the system in a way that derives its full clinical benefit while maximizing the quality of life for the patient. Any hindrance to the patient's or physician's use of a component of the system must be carefully analyzed for its impact on the patient.

User environment. The insulin pump system is made unique by the patient's high amount of interaction with the system. Different user environments directly affect patient interactions in safety and device effectiveness. A solution must account for these environments (e.g., public transit versus home environment).

Resource constraints. As we miniaturize system components, power and computational constraints become more important. Because current insulin pump systems are external to the body and can easily receive renewable power (e.g., change the battery), they are not as resource constrained as other medical device systems. Using resources judiciously can affect the patient's quality of life (e.g., not having to recharge a battery as often), and every system must balance these constraints for patient security and safety.

Effectiveness. A security feature should strengthen safety, but it could affect the clinical effectiveness of the device. There may be a less secure solution that increases device effectiveness with acceptable risk.

Inadequately addressing any of these factors can negatively affect safety. Thus, a derived requirement is that the system meets these criteria adequately while balancing safety. For instance, any change to an existing system should be as usable as a current system.

Categorized Security Challenges Through a Risk-Based Analysis

In this section we detail some of the potential security vulnerabilities posed in insulin pump systems and recommend approaches to mitigate these issues. We note that each vulnerability affects key security properties including availability, confidentiality, integrity, authentication, and authorization (see **Table 1**). Data integrity, which means to ensure that all changes (both unintentional and intentional) to data are detected, was a main focus of a presentation by FDA at the Tenth Annual Diabetes Technology Meeting in Bethesda, Maryland.[7] During his presentation, Paul Jones explained how addressing integrity of wireless communications addresses a main security issue. Similarly, we focus on areas that present the most risk to patient safety when one of these key security properties is compromised.

We highlight security issues in each specific device category by describing how we have reached our current state and then detailing where we are now. We will end by describing where future security challenges exist and detail some steps to mitigate these issues.

Table 1.
Insulin pump key security properties

Availability	To uphold safety, the system must be able to respond according to its specification and design. An insulin pump system should remain available to its user at all times.
Confidentiality	Data is knowable to only the intended parties. Patient information and system data should remain secret to unauthorized third parties.
Integrity	Data cannot be undetectable altered. All system data that can affect patient treatment must no be altered without the patient's knowledge.
Authentication	Only authorized parties or components should be able to act as a more trusted user of the system (i.e., allowed privileged access).
Authorization	Certain authorized subjects's actions must be verified before execution.

Category 1: Insulin pumps. Wireless features of insulin pump systems have introduced additional complexity and potential vulnerabilities. Security challenges posed by wireless connectivity are of particular concern. An unauthorized third party can interfere with pump communication and undermine patient safety (we confirmed this through laboratory experiments by sending commands to an insulin pump using an unauthorized remote programmer at a distance of 100 ft.[8]). In addition to the wireless pump communication, the device's software integrity is equally important (software should not be altered undetectably). Thus, the specifically identified issues are a security breach that could result in: (1) changing already-issued wireless pump commands; (2) generating unauthorized wireless pump commands; (3) remotely changing the software or settings on the device; and (4) denying communication with the pump device.

Category 2: Blood Glucose Monitor. Blood glucose monitors (BGMs) have been typically used as a way of telling a patient their current blood glucose level. Today, they are additionally used to wirelessly transmit a blood glucose value to the pump or, although not as widespread, to calibrate the continuous blood glucose monitor. Through the additional features of calibration and communication, BGMs are an increasingly important and trusted component of the insulin pump system. Currently, deployed systems enable pump and BGM interaction and BGM and personal computer (PC) interaction. Consequences of a security breach may include: (1) changes of glucose levels from the BGM to the pump via the communication channel; (2) changes of glucose levels from the BGM to the PC via the communication channel; and (3) changes to the BGM software by a PC.

Changing the BGM software is more speculative. BGMs currently interact with desktop computers on a regular basis to allow a patient to use data analysis tools on their blood glucose values. Unfortunately, the interface between a BGM and PC could be compromised (e.g., through a computer virus). This particular communication sheds light on a different interface: the interface between two peripheral components (i.e., the BGM and PC), and this interface shows the increased complexity and associated security issue between these components.

Category 3: Continuous Glucose Monitor. By including wireless functionality in the insulin pump system, many pump patients have a network of devices on their person throughout the day. One of the most important devices within the insulin pump system is the CGM. Because insulin dosage may be changed based on monitor-reported blood glucose measurements, similar security challenges exist in this device, including the possibility that there could be a security break that would: (1) alter wirelessly transmitted blood glucose values; or 2) generate records of new glucose values *de novo* and then transmit them wirelessly.

Category 4: Peripheral components. While we have already addressed some of the issues about mobile devices[9], peripheral component risk is increasing. Currently deployed peripheral devices that are being integrated increasingly into the insulin pump system include the PC and mobile phone. A new concept car that displays real-time blood glucose values in its dash shows that any device could be included in an insulin pump system;[10,11] we note that each device presents a potential threat to safety and security. For the PC, we must protect against a breach in: (1) changed insulin pump settings; (2) alteration of existing blood glucose data values; (3) insertion of new blood glucose data values; and (4) transmission of blood glucose data values. The PC is an integral part of a patient's toolset to understanding their glycemic values. Patient benefits outweigh the risks of using such a device, but changes are necessary to increase patient safety from both intentional and unintentional harm.

We note that the described areas do not apply to all insulin pump systems, but they are representative of deployed systems. Future insulin pump systems including closed-loop artificial-pancreas systems are susceptible to similar issues and present new challenges, but we omit those systems for brevity. Fortunately, many of the identified areas have solutions that may simply need vetting by relevant stakeholders (i.e., primarily patients and physicians), while some are more difficult and require novel research. The FDA has already begun encouraging insulin pump manufacturers to start addressing security in their product designs,[7,12,13] and we look forward to the FDA's future guidance in insulin pump system security. We now detail mitigating ways to address security in deployed systems.

Mitigating solutions

For faster deployment of potential solutions, we highlight some approaches here.

Pump and component interaction. Wireless functionality is a key feature that has introduced much of the identified issues. While this is a necessary and important feature (for current CGMs, the artificial pancreas, and general improvement on the quality of the patient's life), simple changes can greatly increase patient safety.

For example, if a pump always has a fail-safe physical interface for the patient (e.g., programming can be done without a remote), then the patient will retain pump control if a remote programmer is lost, stolen, or wireless communication is interrupted. For a patch pump, a simple tactile button on the device itself could be used to enable wireless communication for a short period of time. When that period of time expires, the pump can no longer communicate wirelessly with the programmer. Temporarily disabling wireless communication protects against abuses where the battery is intentionally drained through its wireless communication interface.

To augment this safety feature, one could additionally use a physical feature to completely disable remote-control wireless communication. This would require a physical interface on the pump to allow control until wireless communication could be restored (e.g., at a minimum, allow the starting and stoppage of insulin delivery and immediate insulin delivery). This may be useful to avoid unintentional message interference in environments with heavy wireless activity.

Continuous wireless communication presents a more challenging issue, and presents a new problem for the artificial pancreas. This device will rely on continuous reliable CGM transmission of glucose levels. Interruption of CGM data transmission would be highly problematic.

An unaddressed aspect of patient therapy is system alarms—an issue that affects patient acceptance and is influenced by the patient's environment. An alarm event should be able to attain the patient's attention. Hypoglycemic patients do not respond well to auditory alarms,[14] and a dual-mode alarm may be necessary (e.g., auditory and vibratory). One possibility for future pumps is to have the phone listen to system communication (e.g., CGM to pump). Even if messages were encrypted, certain data transmission patterns may indicate a problem, and the phone could alert the user. This assumes that the phone cannot understand but can detect system communication, and it assumes an acceptable level of risk. Additional risk lies in using the phone as an alarm where rogue software could intentionally mute alarms or raise spurious alarms. To increase safety, an alarm system may need two independent components (e.g., phone plus pump).

Confidentiality. In addition to wireless communication and device service interruption, confidentiality remains an issue. Common encryption standards such as the Advanced Encryption Standard provide a foothold for an acceptable solution. While issues with key management exist within a specific vendor's system (e.g., initial device pairings and pairing new devices), this requires that vendors work more closely together. An insulin pump system may involve several companies and their associated devices, and manufacturers will need to share keys without overburdening patients. This should be an easier technical problem, but it should be vetted for usability.

While encryption helps provide a solution, it could inhibit emergency medical staff needing access to patient data.[15] An easy solution is to provide a physical pump interface (e.g., a physician presses a physical tactile button for the needed data). If a physical pump interface is not acceptable, then a novel solution will be needed for accessing this information (e.g., using an infrared port that interfaces to a reader).

Peripheral components. We now discuss potential solutions for peripheral components by considering a PC. The PC can now change insulin pump settings, and many patients use a computer to graph their data. Unfortunately, although maintaining PC integrity is the goal of a multibillion dollar antivirus industry, this goal has been (yet) unrealized. Ensuring integrity may require novel computer science research to provide a safe environment for patients.

Use of an untrustworthy peripheral component presents a more recent challenge in a medical device system. We are now tasked with building a safe system from less safe parts. The unsafe system may perform undesired actions, and we must both detect and address those actions performed by many peripheral devices including a desktop PC, smartphone, or lightweight tablet PC. Dependable logs for both unintentional errors and intentional issues become more important as complexity within the system increases. We leave this topic for a future paper.

Device classification

This article has highlighted many security issues within an insulin pump system. Research[16] has shown similar issues in cardiac devices. We envision that future medical device security research will fall into different device classes that partition the medical device system. These classes align well with the FDA's device classes.

Device classification may be done differently for security purposes, and the primary factor is how the device is used by the patient. In this sense, devices that are completely implanted and not physically accessible externally belong to class III; examples include pacemakers, internal cardiac defibrillators, and neurostimulators. Devices that are implanted but external to the body form class II; this includes infusion pumps. Another class, class I, includes devices that are completely external to the body but are still considered to be part of the system; this includes BGMs, mobile phones, and personal computers.

We claim that device interactions with these atypical class I medical device system components constitutes risk and may need closer scrutiny. Because the classes are associated with different regulatory burdens, we anticipate that faster but effective regulatory examination will be needed. In the future, based on the system's complexity from interactions within different components, this class may need subclasses based on the device's interaction and safety implications from those system interactions.

Conclusion

Insulin pump systems have continually incorporated new components that have greatly benefited patients, including CGMs and wireless remote programmers. In the future, new devices including automobiles, watches, clocks, beds, and exercise equipment are all viable devices for inclusion (while phones may be adopted more, they are already a part of insulin pump system therapy). The resulting complexity makes security and safety analysis more difficult. We recommend a cautious approach to adopting these new devices, as their impact on patient safety is not well understood.

Device miniaturization and commercialization of an artificial pancreas may soon result in new approaches to system design. As sensors and pumps grow smaller, decreasing computational and power resources can affect the security architecture. Engineers are working to make these new architectures safe and secure both now and in the future.

Funding:

Prepared in part 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. This publication was also made possible in part by Grant Number HHS 90TR0003/01. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the HHS.

Acknowledgements:

The authors would like to thank Lawrence MacIntyre, Chris Rathgeb, and Ben Huey for helping implement the initial security breach of using an unauthorized programmer with an insulin pump system. We thank Apurv Kamath of DexCom for his valuable comments in earlier drafts of this paper.

References:

1. LCDR Alan Stevens, FDA Infusion Pump Team Leader. Insulin Pumps. Public Workshop: Innovations in Technology for the Treatment of Diabetes: Clinical Development of the Artificial Pancreas (an Autonomous System); 2010 Nov 10; available from: http://fda.yorkcast.com/webcast/Viewer/?peid=c99b98eac96d45dd90de77c6e359f139.
2. White Paper: Infusion Pump Improvement Initiative. April 22, 2010. Available from: http://www.fda.gov/medicaldevices/productsandmedicalprocedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm205424.htm. Accessed on October 31, 2011.
3. Maisel WH, Kohno T. Improving the security and privacy of implantable medical devices. N Engl J Med. 2010;362(13);1164–6.
4. Guidance for Industry and FDA Staff—Total Product Life Cycle: Infusion Pump—Premarket Notification [510(k)] Submissions Draft Guidance. April 23, 2010. Available from: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm206153.htm. Accessed on October 31, 2011.
5. Senesh G, Bushi D, Neta A, Yodfat O. Compatibility of insulin Lispro, Aspart, and Glulisine with the Solo MicroPump, a novel miniature insulin pump. J Diabetes Sci Technol. 2010:4(1):104–10.
6. Zisser HC. The OmniPod Insulin Management System: the latest innovation in insulin pump therapy. Diabetes Therapy. 2010:1(1);10–24.
7. Jones PL. Regulatory considerations for insulin pump safety and security. Proceedings of Insulin Pump Safety and Security Workshop, 10th Annual Diabetes Technology Meeting; 2010 Nov 11–13; Bethesda, Maryland.
8. Paul N. Insulin pump security and reliability: past, present, and future. Proceedings of Oak Ridge National Laboratory JDRF meeting; 2010 Apr; Oak Ridge, Tennessee.
9. Paul N, Klonoff D. Insulin pump system security. Proceedings of First USENIX Workshop on Health Security and Privacy; 2010 Aug. 10; Washington, District of Columbia.
10. Kerr D, Olateju T. Driving with diabetes in the future: in-vehicle medical monitoring. J Diabetes Sci Technol. 2010:4(2);464–9.
11. Fruhlinger J. Medtronic Diabetes concept car monitors glucose levels in-dash. endgadget. June 12, 2008. Available from: http://www.engadget.com/2008/06/12/medtronic-diabetes-concept-car-monitors-glucose-levels-in-dash/. Accessed on October 31, 2011.
12. Klonoff DC, Reyes JS. Insulin pump safety panel: summary report. J Diabetes Sci Technol. 2009:3(2);396–402.
13. Zhang Y, Jones PL, Klonoff DC. Second insulin pump safety meeting: summary report. J Diabetes Sci Technol. 2010:4(2);488–93.
14. Schultes B, Jauch-Chara K, Gais S, Hallschmid M, Reiprich E, Kern W, Oltmanns KM, Peters A, Fehm HL, Born J. Defective awakening response to nocturnal hypoglycemia in patients with type 1 diabetes mellitus. PLoS Med. 2007:4(2);e69.
15. Klonoff DC. Designing an artificial pancreas to be compatible with other medical devices. J Diabetes Sci Technol. 2008:2(5);741–5.
16. Halperin D, Heydt-Benjamin TS, Fu K, Kohno T, Maisel WH. Security and privacy for implantable medical devices. IEEE Pervasive Computing. 2008:7(1);30–9.