33rd Annual International Conference of the IEEE EMBS
Boston, Massachusetts USA, August 30 - September 3, 2011

Biomedical Devices and Systems Security

David Arney, Krishna K. Venkatasubramanian, Oleg Sokolsky and Insup Lee*
Department of Computer and Information Science,
University of Pennsylvania, Philadelphia, PA, 19104
{arney, vkris, sokolsky, lee}@cis.upenn.edu

Abstract— **Medical devices have been changing in revolutionary ways in recent years. One is in their form-factor. Increasing miniaturization of medical devices has made them wearable, light-weight, and ubiquitous; they are available for continuous care and not restricted to clinical settings. Further, devices are increasingly becoming connected to external entities through both wired and wireless channels. These two developments have tremendous potential to make healthcare accessible to everyone and reduce costs. However, they also provide increased opportunity for technology savvy criminals to exploit them for fun and profit. Consequently, it is essential to consider medical device security issues.**

In this paper, we focused on the challenges involved in securing networked medical devices. We provide an overview of a generic networked medical device system model, a comprehensive attack and adversary model, and describe some of the challenges present in building security solutions to manage the attacks. Finally, we provide an overview of two areas of research that we believe will be crucial for making medical device system security solutions more viable in the long run: forensic data logging, and building security assurance cases.

I. Introduction

Medical devices are articles that are used in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease in humans or animals [1]. They are essential for modern medicine as they provide the ability to automate many patient monitoring and management functions. This allows caregivers (doctors/nurses) to be able to focus on their primary task of patient care.

As medical devices collect and exchange personal health data, *securing* them is very important. Lack of security may not only lead to loss of patients' privacy, but may also physically harm the patient by allowing adversaries to introduce bogus data or modifying/suppressing legitimate data, inducing erroneous diagnosis. Indeed, protecting health data is a legal requirement as well. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), specifies, among other things, a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information [2].

Medical devices can be broadly classified into two categories: stand-alone and interoperable. Stand-alone medical devices are designed to perform monitoring and actuation tasks without directly interacting with other medical devices or other equipment. These are by far the most common type of medical devices available today. Recent years, however, have seen medical devices move away from their traditional stand-alone organization. Devices now have considerable communication capabilities, which allows them to interact with entities around them. The proliferation of short distance wireless communication technologies has also opened up the possibility for the devices to communicate using the wireless channel. Examples include wireless pulse oximeters [3], defibrillators and pacemakers [4], and patient monitors [5]. Note that, interactions between devices can be both intermittent (*e.g.* store and forward ECG monitors [6]) and continuous in nature [5]. Each presents its own set of security and privacy issues. In this paper, our focus is on networked devices with continuous connectivity.

Both stand-alone and networked medical devices present security problems. In the case of the former, devices may be subject to tampering, reprogramming by unauthorized persons, and device-specific hazards. Device firmware may be upgraded opening additional hazards. When medical devices are connected to a network, the network interface provides another avenue for attack. It enables remote attacks from outside the hospital as well as attacks that originate locally. For example, researchers working with an implantable cardiac defibrillator were able to remotely read telemetry data and reprogram the device [7]. It can be seen that besides the obvious physical hazards, there are also privacy implications for such attacks. The network itself may also be a target of attacks, and the more devices there are on the Hospital Information System (HIS), the more attractive it is as a target.

Besides malicious attacks, there are also likely to be unexpected interactions between devices and systems. Wireless technologies such as WiFi are particularly prone to interference, including interference from medical devices such as electro-surgical units, and invite tampering simply by making it easier for malicious persons inside or outside the hospital to access the network. Many of these devices currently have no safeguards beyond an unpublished, proprietary interface and are susceptible to buffer overflows and other problems when unexpected signals are received on their interfaces. For example, electromagnetic interference by two RFID systems (active and passive) in the proximity of medical devices demonstrated the presence of hazards such as: total switch-off and change in set ventilation rate of mechanical ventilators; complete stoppage of syringe pumps; malfunction of external pacemakers; complete stoppage of renal replacement devices and so on [8].

In this paper, we present an overview of some of the principal aspects of medical device security, especially when the devices are networked. Particularly, the focus is on identifying security requirements, the principal threats and the challenges involved in addressing them. In [9], the

POC: Insup Lee, lee@cis.upenn.edu

978-1-4244-4122-8/11/$26.00 ©2011 IEEE

authors present a taxonomy of vulnerabilities of implantable medical devices. They classify them based on the cause of vulnerabilities and the effect the vulnerabilities have on the system. In this work, we look at a much broader class of medical devices. The focus is not only attack models, but also on a model for networked medical devices, along with the challenges involved in securing this model. Further, we motivate the need for two new areas of research — forensic data logging and assurance cases for security, that will nicely complement the aforementioned security improvements that are already being proposed with respect to medical devices.

II. Medical Device System Model

Figure 1 depicts the patient-centric medical device system. The model is based on the ICE standard for medical device interoperability [10]. It has been designed to act as a middleware enabling interaction of legacy stand-alone medical devices and an architecture for applications using medical devices, including closed-loop physiological control. The system consists of: (1) *Collection of Medical and Other Devices* placed on or around a single patient that can perform monitoring and actuation. The devices have an adapter that allows them to communicate with the Network Controller; (2) *Network Controller* interfaces with the medical devices. It is responsible for collecting data from the individual devices. It also connects the entire setup to an external network, *e.g.*, HIS. The network controller also records all the actions of the entire system in a data logger or black box recorder (BBR) for future analysis; (3) *Supervisor* receives data from the various medical devices, process it, and initiate action from the medical devices. The Supervisor runs clinical applications that use the connected devices to support a clinical scenario selected by the caregiver; and (4) *Caregiver* is responsible for configuring the system, selecting an appropriate program on the Supervisor, and then monitoring the patient's well-being using an user-interface provided by the Supervisor. The caregiver can control various parameters of the system such as alarm thresholds and so on as permitted by the application they choose.

The entire system is designed to facilitate interaction between the medical devices available today. It has the potential to provide closed-loop control over patient's health. For example, the Supervisor could run an application that receives data from a glucose monitor, processes the data to analyze the level of blood sugar in the patient, and commands the infusion pump to administer a dose of insulin chosen by the caregiver.

III. Attack Model

Adversaries attacking a medical device system, such as that of Figure 1, can be classified into two sources: active and passive. *Active attackers* have the capability to eavesdrop on traffic between the devices, network controller and the supervisor, inject messages, replay old messages, spoof, and ultimately compromise the integrity of device operation. Active attackers, if successful, can not only invade a patient's privacy but can also suppress legitimate data or insert bogus data into the network leading to unwanted actions (drug delivery) or prevent legitimate actions (notifying doctor in case of an emergency). *Passive attackers*, on the other hand, are attackers who eavesdrop on the messages exchanged within the system and use off-line cryptanalytic attacks to access confidential data being communicated (invading a patient's privacy). This type of attack does not try to interfere with the operation of the medical devices.

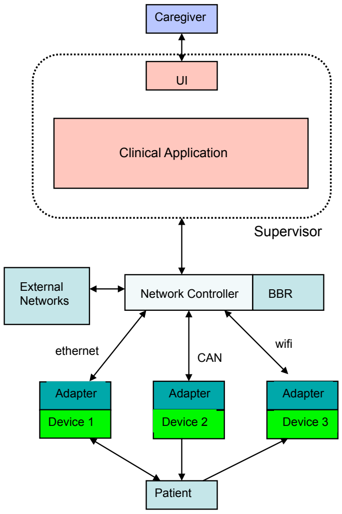

Fig. 1. Patient-centric view of the device environment

There are four broad classes of targets that adversaries can choose to attack within medical device systems. They include: patient physical security, patient data security or privacy, medical device physical security, and data security of the health-care institution that deploys the medical device system. We now describe them in some detail.

Patient's Physical Security: This category includes attacks that directly target the patient's health. The attacker's goal is to cause some form of physical harm to the patient. This can be achieved by targeting various operational aspects of the medical device system such as sensing, processing, communication, and actuation. Sample attacks include: (1) triggering a device to give an additional dose of medication; (2) altering programming of a radiation therapy device, either by corrupting its program directly or by feeding it bad data; (3) interfering with an implanted device; (4) falsifying printed labels on medication between the pharmacy and the patient; (5) tampering with a patient's electronic health records to make it appear that they have- or do not have- a medical condition; (6) changing prescriptions in the hospital's order entry system so the patient receives the wrong dose or medication

Patient's Data Security: This category includes attacks that seek to access an individual patient's health data in an unauthorized manner. The issue with such an attack is that such loss of sensitive medical information could lead to discrimination and abuse. For instance, one could deny services to people with specific medical conditions. Patient's data security can be breached in multiple ways from communication eavesdropping, to physical theft of patient information. Sample attacks include: (1) reading residual device data if not cleared after use; (2) a patient's health records are read by curious hospital staff; and (3) medical records are stolen and used to file a fake insurance claim.

This category involves security of a single patient. The privacy of data pertaining to sets of patients is considered under institutional security.

Medical Device Physical Security: This category includes attacks that seek to target medical devices and the network components. The idea is to mount a Denial of Service (DoS) on the medical devices in some form so that they cannot perform their task. Such attacks could have additional consequences apart from lack of availability including privacy loss, especially in systems designed to fail-open [11], or even physical damage to the device or surrounding infrastructure. Sample attacks include: (1) theft of devices or medication; (2) new firmware is uploaded to infusion pumps using their online update feature that changes the pressure limits causing the pumps to burn out their motors; and (3) a device is engaged in an endless stream of challenge-response message to drain its battery.

Institutional Data Security & Privacy: This category includes attacks that seek to target the medical institution where the medical device system is deployed. The idea is to compromise the interaction between the device system and the medical institution's internal network and access, at a large-scale, patient data or network operational information. Samples attacks include: (1) traffic analysis of the hospital network reveals that patients have a high rate of adverse events; (2) sniffing the wireless network shows that one brand of device is prone to problems; (3) DOS attack on hospital network; and (4) changing the hospital's Dose Error Reduction System information to trigger incorrect alarms.

IV. Challenges

There are numerous challenges that need to be overcome in the course of developing solutions for addressing the various attacks on medical device systems. They are:

- *Overhead:* Security always adds an overhead to any system. Medical devices often have limited computational and communication capabilities. Many devices are battery powered. Even devices such as infusion pumps or ventilators include batteries as a backup source or for use during patient transport. Security solutions that are resource-intensive will seldom be adopted. Therefore computation, memory, and communication resource needs must be carefully considered.
- *Heterogeneity:* Systems of medical device are usually made up of heterogeneous elements with order of magnitude difference in capabilities. A direct consequence of this heterogeneity is that one security solution might not fit the needs of the entire system.
- *Usability*: Security protocols need to be developed with usability in mind. That is, they should in not increase the cognitive load of the users beyond what is needed in learning to operate the device. Essentially, security has to be as transparent as possible to the users (*e.g.*, clinicians). Clinical trials apart from testing devices for efficacy should also test them for the usability aspect of their security. Security solutions that add overhead for clinicians, such as multiple logins or the need to enter a code on each device create safety issues for patients. In many clinical situations, speed is important and systems that delay clinicians' ability to act will not be clinically acceptable.
- *Attitude:* A prevailing attitude in medical device systems community is that of "security through obscurity" [12]. This attitude has been shown to be problematic as hackers, given the right incentives, will always be able to hack into such a system. Further, making the inner workings of the security primitives of the system publicly available, leads to design improvements that serve the system well, in the long run [13].
- *Safety*: Safety has been the primary concern for medical devices for a long time. With the introduction of security, one needs to ensure that system safety does not get compromised in any manner. For example, the addition of cryptographic primitives to a implantable device if not designed properly could lead to excessive computational load causing excessive heating of the tissue surrounding the device or premature battery exhaustion.

V. Developing Secure Medical Devices

Safety has been the fundamental goal of medical device manufacturers. This has lead to the development of a process for ensuring safety properties using tools such as: (1) FMEA: Failure Modes and Effects Analysis, and (2) Safety/assurance cases. Manufacturers must convince the FDA that they have accounted for and mitigated all safety hazards. Safety in the context of security is a growing issue; driven in part by the use of wireless technology. Device manufacturers must now explicitly address these concerns in their submission to the FDA.

Maintaining security for medical devices is not very different from any other cyber-physical system and depends on the maintenance of five basic properties - (1) *Data Integrity*: All information generated and exchanged between the medical devices and the supervisor are accurate and complete without any alterations; (2) *Data Confidentiality*: All information generated during the use of medical devices is only disclosed to those who are authorized to see it; (3) *Availability*: All medical devices are accessible by the supervisor, caregivers and patients as needed; (4) *Authentication*: All devices involved know who they are interacting with; and (5) *Physical/Administrative Security*: All medical devices and associated equipment used by caregivers and others should be protected from tampering. Further, the work-flow of an organization should allow only authorized physical access to equipment.

Recent years have seen much work in securing medical devices [11], [7], [14], [15]. In most of these cases the focus is on secure communication or effective access control, especially for implantable medical devices. Many of the issues discussed in these papers apply to general classes of medical devices as well. In this section, therefore, we provide an overview of two areas of research that we believe will be crucial for building secure medical devices. The first is forensic data logging capabilities and the other is developing formal assurance cases for medical device security.

Forensic Data Logging: Forensic data logging means that patient and device data are logged to a flight-recorder style data logger. These logs assist in uncovering causes of adverse events. They can help to distinguish use error, equipment failure, or abnormal use. Logs also open new hazards. The data logging of the state-of-the-clinical environment usually includes, among other things: (1) technical variables and technical alarm conditions from the medical devices made available to the ICE network controller; (2) patient physiological variables and alarm conditions from medical devices available to the network controller; (3) network controller commands to medical devices; (4) network controller status; (5) supervisor decisions, time the decisions were made and the inputs on which they were made; and (6) any other significant events and errors within the entire system. Fundamentally, data logger designs need to anticipate security risks. For example, data logger memory should be write-only on the device and information identifying the patient encrypted.

Assurance Cases: Assurance cases represent a framework for arguing that evidence justifies a claim. They provide a means for convincing a third party, such as a regulator, that a particular claim is justified. For medical device security, one might claim that the device is adequately secure for its intended use in a particular use environment. Developing assurance cases like their safety counterpart is a three step process: (1) *Claim:* Specifying the claims about certain properties of the system. For example, communication between devices and the network controller is secure; (2) *Argument:* Making arguments about the evidence justifying the claim. Example, use of AES encryption algorithm for hiding (*i.e.*, encrypting) data communicated between the device and network controller; and (3) *Evidence:* Providing evidence to support the arguments made toward the claim. Example, AES algorithm implementation is verified via formal proof documentation or reasoned test cases that are verified via documentation.

Complementary hazard analysis techniques (e.g. FTA, FMEA, Hazop, etc) in combination with formal methods techniques for verifying implementations facilitates the development of secure medical devices and provides a foundation for assurance case presentation. Building assurance cases for individual components of the medical device system is not sufficient. Eventually, the individual assurance cases have to be composed as well, to satisfy security claims of the entire system. Finally, developing assurance cases also involves providing cost-benefit justification for their use. Some of the questions that need addressing in this regard include: how much additional effort is required? Is the effort justified? What are the short and long term benefits from the activity? How are safety cases maintained as systems evolve?

VI. Conclusions

Security is crucial for the long term viability of today's networked medical device systems. In this paper, we focused on the challenges involved in securing networked medical devices in the presence of various classes of adversaries. We presented a generic model for medical device systems, developed a comprehensive attack and adversary model, and described the various challenges in designing security solutions. Further, we provided a short overview of two main areas of research that need to be done to make security solutions more viable in the medical settings. It needs to be noted that security can only be talked about in abstract absent a concrete design. In the future, we therefore plan to focus on developing security solutions for specific clinical applications such as pulmonary management work-flows that involve integrating devices including ventilators, pulse oximeters, blood pressure monitors, and so on. Validation will be done based on actual implementation of the solution in the context of the clinical application.

Acknowledgements

The authors would like to thank Paul L. Jones of the FDA for his insights and help in improving this paper. This research was supported in part by NSF CNS-1035715, NSF CNS-0930647, ONR MURI N00014-07-1-0907, and NIH 1U01EB012470-01.

References

[1] Safe Medical Devices Act. http://www.fda.gov/cdrh/devadvice/312.html.

[2] HIPAA-Report2003. Summary of HIPAA Health Insurance Probability and Accountability Act. US Department of Health and Human Service, May 2003.

[3] K. McCarthy. NONIN Avant 4000 Bluetooth Wireless Oximetry:Increased Safety and Accuracy When Administering the Six-Minute Walk Test. February 2008. White Paper.

[4] Medtronics Inc. http://www.medtronic.com/your-health/bradycardia/device/.

[5] BodyMedia. http://www.bodymedia.com/.

[6] Jocelyne Fayn and Paul Rubel. Toward a personal health society in cardiology. *Trans. Info. Tech. Biomed.*, 14:401–409, March 2010.

[7] 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. 2008. In Proc. of IEEE Symposium on Security and Privacy.

[8] R. van der Togt and E-J. van Lieshout and R. Hensbroek and E. Beinat and J. M. Binnekade and P. J. M. Bakker. Electromagnetic Interference From Radio Frequency Identification Inducing Potentially Hazardous Incidents in Critical Care Medical Equipment. *JAMA*, 299(24):2884–2890, 2008.

[9] J. A. Hansen and N. M. Hansen. A Taxonomy of Vulnerabilities in Implantable Medical Devices. pages 13–20, 2010. In Proc. of Second Security and Privacy in Medical and Home-Care Systems (SPIMACS) Workshop.

[10] ASTM F29.21. Medical devices and medical systems - essential principles of safety and performance for equipment comprising the patient-centric integrated clinical environment (ice). Draft Standard version 160608.

[11] T. Denning, K. Fu, and T. Kohno. Absence makes the heart grow fonder: new directions for implantable medical device security. In *Proceedings of the 3rd conference on Hot topics in security*, pages 5:1–5:7, 2008.

[12] A Heart Device Is Found Vulnerable to Hacker Attacks. http://www.nytimes.com/2008/03/12/business/12heart-web.html?ref=business.

[13] N. Ferguson, B. Schneier, and T. Kohno. *Cryptography Engineering: Design Principles and Practical Applications.* Wiley Publishing, 2010.

[14] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS '09, pages 410–419, 2009.

[15] K. Venkatasubramanian, S. K. S. Gupta, R. P. Jetley, and P. L. Jones. Secure interoperable medical device communication. *IEEE Pulse*, pages 16–27, Sept/Oct 2010.