Protecting Global Medical Telemetry Infrastructure

Benessa Defend, Mastooreh Salajegheh, Kevin Fu, and Sozo Inoue
University of Massachusetts Amherst and Kyushu University
{defend,negin,kevinfu}@cs.umass.edu, sozo@lib.kyushu-u.ac.jp

January 7, 2008

Acknowledgment:
This work was supported under grant number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

Executive Summary

Implantable medical devices (IMDs) such as heart rate sensors, pacemakers, and drug delivery systems can save lives and greatly improve a patient's quality of life. As the use of wireless IMDs becomes more ubiquitous, the need to address security and patient privacy concerns under adversarial conditions increases. Challenges in addressing these issues arise due to the resource limitations of medical devices, characteristics of wireless communication, and the distinguishing features of transmitted data. In this paper, we discuss possible threats to the privacy and security of a medical telemetry infrastructure. We define four main security goals for the system: privacy, availability, integrity and authentication. We also present multiple realistic scenarios to show the necessity of these four security goals in collecting, transmitting, and analyzing medical data. Moreover, we introduce potential solutions for preventing or detecting the problems we identify.

1. Introduction

Medical devices allow patients to lead longer and more active lives through monitoring, relaying data to medical professionals, and providing treatment in times of crisis. Devices capable of wireless communication are increasingly used for patient monitoring in hospitals and homes. Examples include heart rate sensors, pacemakers, drug delivery systems, neurostimulators, and wireless identification bracelets. Some of these devices, such as pacemakers and insulin pumps, are surgically implanted inside the body and have long battery lives of around 10 years in order to prevent the potential surgical complications of physically replacing the devices. Other devices are worn externally and have shorter battery lives. Some of the medical devices have the ability to communicate wirelessly with a monitoring device in a patient's home, which then relays information to a hospital or doctor's office via the Internet. In addition to transmitting information, medical devices can contain sensitive personal data, such as name, date of birth, illnesses, history of treatment, allergies, and other health-related information. For example, some pacemakers log heart rate data to keep a record of a patient's exercise activities. Drug delivery pumps can be programmed to administer different dosages at preprogrammed times or in the event of a medical emergency. Pacemakers contain therapy information regarding the duration and amount of energy to administer if the heart rate becomes too fast, too slow, or irregular.

Privacy, availability, integrity, and authentication are the four important security goals for medical devices. Privacy entails the disclosure of sensitive personal information. Another security goal for a system of medical devices refers to the availability of the system, with regards to emergency and non-emergency patient situations. It is highly important that medical devices perform accurately when needed and have the ability to communicate information in a timely and efficient manner. Integrity and authentication refer to the validity of the data and the source of the data respectively. That is, the integrity of the contents of the communication and the authenticity of the source of the communication must be verified to ensure secure operation of the system. Failure to verify the integrity of messages could result in improper medical

treatment. These messages must also come from valid, existing medical devices within the network.

To solve pressing problems related to these security goals for medical devices, further research is needed in the following areas:

1. Privacy and security for wireless devices. New algorithms and cryptographic techniques are needed to ensure that medical devices protect the privacy of patient data, including personal, medical, and location information.

2. Traffic analysis. Methods are needed to prevent a third party from analyzing the traffic, or the communication between devices. Using traffic analysis, unauthorized parties can learn sensitive information about patients. This includes preventing information leak- age so that an adversary can obtain no new information by employing traffic analysis techniques.

3. Intrusion detection systems. In addition to prevention mechanisms, detection mechanisms are necessary to determine if an intrusion has occurred. Intrusions can severely disrupt a network, leading to data loss and degradation in patient care. It is important to be able to identify when intrusions have taken place so that any damage may be repaired.

We will consider various scenarios which illustrate the complexity and reality of problems which motivate this research. The first scenario is telemetry spam, which is unsolicited medical telemetry that floods the network and monitoring equipment. We next consider possible means for a third party to deplete a device's battery, to invade a person's privacy, and to disrupt the entire medical device network. We detail the difficulties associated with preventing each of these problems and also present countermeasures. These scenarios show why each of the four goals are necessary in an infrastructure for collecting and storing medical telemetry.

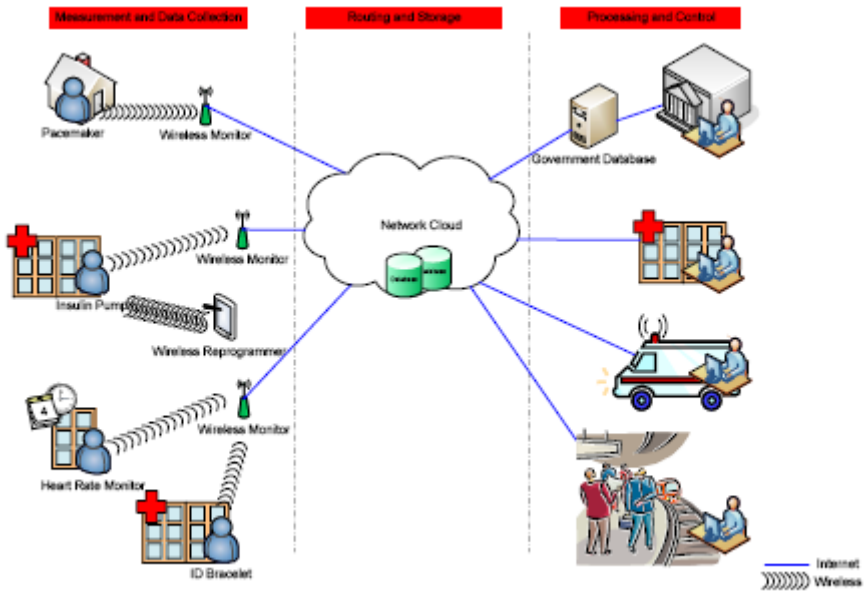

Figure 1: Overview of a medical telemetry infrastructure. Medical devices, such as pacemakers, implantable insulin pumps, and identification bracelets, can communicate with other monitoring devices at hospitals, homes, and other places. Information from these devices can be used by medical professionals in making health care decisions and by government agencies in monitoring public health and compiling statistics.

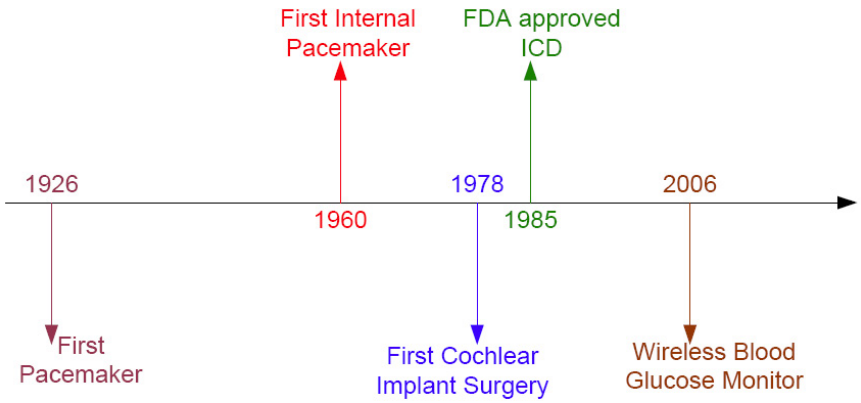

Figure 2: Timeline of significant events in the history of modern medical devices [10, 4, 8, 1].

2. Motivation

Medical telemetry represents a major information infrastructure to secure in the coming years. From 1990 to 2002, about 2.25 million pacemakers and 416,000 Implantable Cardiac Defibrillators (ICDs) were implanted in the United States [9]. The insulin pump market is around $3 billion annually with around 400,000 people worldwide using insulin pumps, and the number of people growing annually at 12-14% [15]. Medtronic, one of the leading companies in medical devices, had $12.3 billion in sales last year [14]. Wireless patient monitoring devices and implanted devices are becoming more ubiquitous as the population ages and technology advances.

Passed by Congress in 1996, the Health Insurance Portability and Accountability Act (HIPAA) regulates health insurance coverage and the privacy and security of medical data [16]. The Privacy Rule of HIPAA took effect in 2003 and controls the utilization and disclosure of Protected Health Information (PHI). For example, when PHI is needed for medical services, only the minimum amount of PHI necessary may be disclosed. Prior to HIPAA, there was no federal law regulating the privacy of medical records. As HIPAA and subsequent medical privacy laws are introduced to handle the growing ways in which information can be shared electronically, hospitals and companies that handle patient data must become more diligent about protecting sensitive information and preventing privacy leaks.

The main function of medical devices is to protect and improve patient health and well-being. They must be able to effectively administer treatment in a timely manner and be able to communicate with external devices. For example, a heart rate monitor must be able to transmit a message to a doctor that a patient is having a heart attack and needs immediate assistance. To fulfill their functions, medical devices, assistive monitoring devices, and the hospital system must operate properly. In addition to proper operation and patient care, the four goals of privacy, availability, integrity, and authentication must be considered. In the following sections, we discuss different challenges that affect the ability for medical devices to perform properly in the context of these goals. We also present various countermeasures and show that this emerging problem area needs further consideration.

3. Scenarios

Medical devices are becoming pervasive in their use in hospitals and homes. In order to provide the highest level of patient care, these devices must operate efficiently and within specific goals related to privacy, availability, integrity, and authentication. Next we explore various scenarios which demonstrate how these goals can be violated and present methods for prevention and detection.

3.1. Telemetry Spam

Problem: Availability, Integrity, and Authentication

Telemetry spam refers to unwanted, fictitious medical telemetry messages. For example, an unauthorized third party could send thousands of fake “I’m having a heart attack” messages. At

the same time, a heart rate monitor could detect that a patient is having a heart attack and sends one “I’m having a heart attack” message to the hospital monitoring device. The monitoring device could become overwhelmed and be unable to handle such a large amount of traffic. Since there are thousands of spam messages and one legitimate message, the legitimate message may become lost, which could have fatal consequences.

	Privacy	Availability	Integrity	Authentication
Telemetry Spam		X	X	X
Dead Battery		X		
Patient Privacy Invasion	X			
Compromised Infrastructure	X	X	X	X

Table 1: Example scenarios and the security goals which are violated.

In a less serious situation, motorists were prevented from driving their cars because a rogue wireless car key transmitter was sending signals that blocked other wireless car keys [11].

Significance

When a network is bombarded with fake messages, there is a possibility that the wireless monitoring device will miss authentic messages. Therefore the patient may not receive medical attention in an emergency. Moreover, these spam messages injected in the network would cause numerous emergency calls to the hospital. These false alarms will reduce the system accuracy and reliability.

Difficulty

What makes the protection of medical devices challenging is that it is not difficult for a malicious user to build a wireless device to transmit fake messages. Therefore, a solution to this threat has to provide the monitoring device with a way to block or ignore fake messages and accept only authenticated messages.

Potential countermeasures

Several techniques from cryptography can be used to provide authentication and integrity in such a system. However, the usual techniques should be optimized according to the characteristics of the medical devices such as memory, energy, or computational constraints. In addition to preventative measures, intrusion detection systems can be used to discover abnormal activities. For example, if 1000 heart attack messages are detected within 5 seconds, this can be defined as abnormal behavior and an alarm can be raised.

3.2. Dead Battery Scenario

Problem: Availability

Some medical devices require batteries for operation. If these devices are used in a predictable manner, then the lifetimes of the batteries are also predictable and replacement can be planned accordingly.

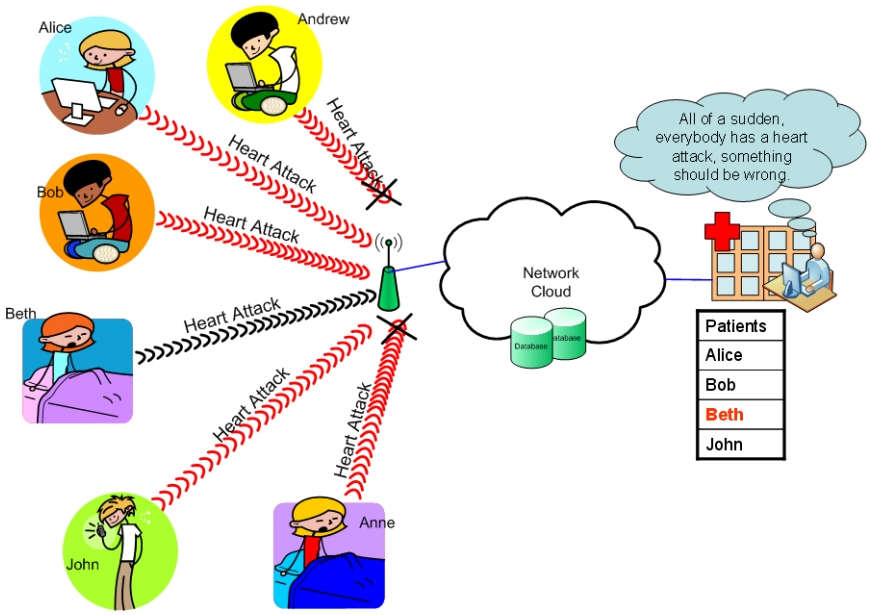

Figure 3: Telemetry spam scenario. When multiple unauthorized individuals send heart attack messages to the wireless reader, the reader may lose some of the messages (Andrew and Anne in the above example). Moreover, among the received heart attack messages, the doctor (or the automatic processing system) could not distinguish the real patient who needs immediate help from the spam senders.

Consider the case when a malicious person sends multiple messages to a medical device to drain its battery. The medical device consumes its energy both to receive the query and to reply to the unauthorized monitor. Another threat to the availability of the medical device is the case when the communication of other wireless devices accidentally interferes. When two wireless devices are communicating in the same radio range as a third medical device, the third may become activated and use some of its battery power in the process.

Significance

When a battery nears depletion, it often requires surgical intervention in the case of implanted medical devices. Since unauthorized access to the medical device results in greater power consumption and therefore premature battery depletion, the patient will require surgery sooner to replace the battery. Also, it could be difficult to predict when the battery will be depleted, and thus hard to determine when replacement surgery will be needed. Unnecessary surgeries pose threats to patients and waste time and money.

Difficulty

To avoid accidental or malicious communication with medical devices, an authentication system can be utilized between the medical device and its wireless monitor. However, the medical device still needs to receive the query from the monitor to be able to authorize the monitor, which results in unnecessary energy consumption. In addition, hospitals cannot realistically prevent all wireless devices from entering or being used within the hospital. Similarly, in a public space a third party could send messages to a person's medical device to cause accelerated battery depletion.

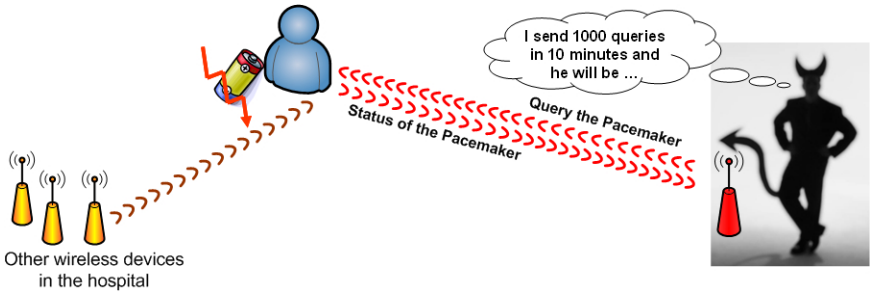

Figure 4: Dead battery scenario. Apart from the valid wireless reader, other wireless devices may communicate with the battery-powered medical device intentionally or accidentally.

Potential Countermeasures

A possible solution to the dead battery problem is to use an RFID (Radio Frequency Identification) tag as a proxy so that no one can talk to the medical device directly. For example, a variant of a device called RFID Guardian [12] could be used as a firewall to prevent and control unauthorized communication to a device. The device which sends a message to the medical device "pays" for the energy to charge the RFID tag before it can communicate directly with the medical device. Thus, the battery of the medical device is not wasted by unauthorized communication.

3.3. Patient Privacy Invasion

Problem: Privacy

Wireless medical devices communicate with other types of monitoring devices within hospitals, homes, and other places. Third parties can eavesdrop on this communication, which can lead to a loss of privacy for patients. For example, an eavesdropper can learn personal information, such as the frequency at which a patient receives medication or the type of medication received, by monitoring the frequency and quantity of communication between the medical device and the monitoring device. Based on the unique characteristics of the communication, one may also be able to learn the type or types of medical devices that a person possesses.

Sometimes patients have one or more medical devices. These devices together can form an identifying pattern, or "wireless fingerprint." Consider that John has a pacemaker and an insulin pump, Mary has only a pacemaker, and Susan has a wireless ID bracelet. By observing only the electronic communication, a third party could distinguish John from Susan and Mary. Distinguishing characteristics that can be used to form a fingerprint include the frequency of communication, the manufacturers and models of medical devices, the strength of the wireless signal, and the quantity of information communicated. John's wireless fingerprint can thus be used to track him in different locations.

Significance

Knowledge by an unauthorized party of a person's medical devices, medications, treatment schedule, etc. is an invasion of privacy. Section 3 discusses in detail the legal issues of protecting patient privacy. Discrimination and patient tracking are additional consequences of

this type of privacy erosion that are not yet covered by legislation. For example, at a job interview an employer could use the techniques described earlier to discover that an applicant has a pacemaker. In a desire to save money in potential insurance costs and sick leave, the employer could then use this information to discriminate against that applicant in favor of hiring a person who does not have any medical devices. This type of discrimination could also be used in housing, insurance coverage, and other situations.

Difficulty

Preventing these types of privacy losses from medical devices presents some unique challenges. Most importantly, these devices are designed to enhance the quality of a person's life and to save lives in the event of emergencies. Therefore, these devices must be able to communicate with external devices. They cannot be turned off or disabled outside of the home or hospital setting in order to prevent unauthorized eavesdropping. Though cryptography can be used to encrypt and authenticate data, encryption alone does not alleviate all privacy concerns in a network. A third party can use a technique called traffic analysis to analyze other characteristics of the communication to identify distinguishing patterns. Encrypted and authenticated communication can leak information about the source of the data and the topology of the network. Analysis of the frequency of communication between two devices, the message length, or even the direction of communication can reveal sensitive patient information, such as diseases and treatments being administered. For example, the encrypted traffic of wireless heart rate monitors could reveal details about the patient's level of stress or monitoring status. A unique packet size and frequency fingerprint may distinguish between a heart murmur and a normal heart rhythm. Treatment information may also be inferred, such as the frequency that medication is taken, e.g. a diabetic's measurements will change after an insulin shot. Also, some patients have multiple types of medical devices, which together form a distinguishable pattern. Thus, a person's medical devices inadvertently broadcast identifying information that cannot be protected with cryptography alone.

Potential Countermeasures

Fortunately, some countermeasures may be applicable to this problem area. Similar to a countermeasure to the dead battery scenario in Section 4.1, one potential is to use an RFID tag or another proxy device to control access to a medical device. For example, a variant of a device called RFID Guardian [12] could be used as a firewall to prevent and control authorized communication to a device. This proxy device would be most beneficial in settings outside the home and hospital, where a medical device would probably normally not be communicating with any other device.

In settings like the home and hospital, a medical device may regularly communicate with monitoring devices. Regardless of whether a proxy device is employed, this communication may be eavesdropped. The next alternative is to modify the characteristics of the communication that are identifying. For example, medical devices could communicate at regular intervals of time and send messages of a fixed length. This countermeasure is difficult because it entails modifying already existing protocols or designing new protocols.

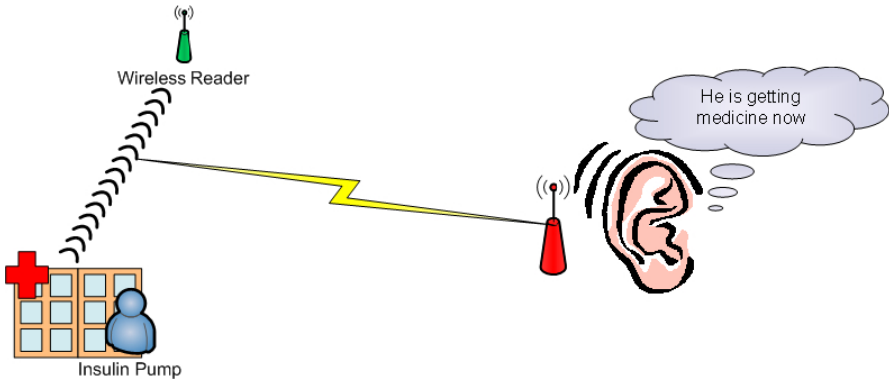

Figure 5: Patient privacy invasion. By eavesdropping on communication between a wireless medical device and a monitoring device, an unauthorized third party could learn when a patient is receiving medication, what kind of medication, and the frequency of medication.

Figure 6: An employer could learn that an applicant has an Implantable Cardiac Device. In an effort to save on potential insurance costs and sick leave, he could choose to hire an applicant without any medical devices.

In the field of Radio Frequency Identification (RFID), which uses small electronic tags to identify objects, there is a similar tracking problem to the one described above regarding medical devices. Multiple countermeasures have been proposed for the RFID tracking problem [3, 2, 6] and may be utilized for medical devices.

For the problem of discrimination, legislation may prove effective or at least serve as a deterrent. Existing anti-discrimination laws for housing, employment, etc. could be modified to include measures protecting people from discrimination based on their implanted or external medical devices.

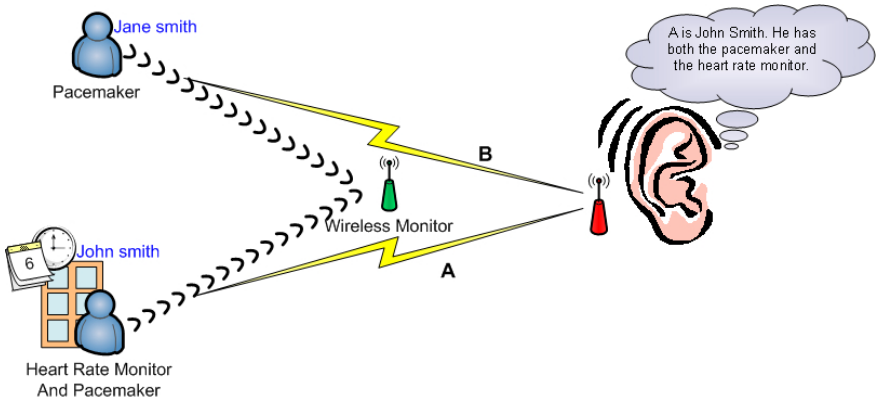

Figure 7: The collection of a person's medical devices can be used for identification and even tracking.

3.4. Compromised Infrastructure

Problem: Privacy, Availability, Integrity, Authentication

In a network with medical devices, privacy and security vulnerabilities are not limited to communication between the devices and monitors. Vulnerabilities can be unintentionally or intentionally introduced and exploited in a network. Poor password management is one way in which vulnerabilities can be introduced. Examples of poor password management include when hospital staff share passwords, reuse the same password for multiple accounts and computers, or write down their passwords. Sometimes private patient information is inadvertently disclosed if someone forgets to log out of a computer, forgets to lock a door, or conducts a sensitive conversation in an open area. Recently, there have been many reports [13, 7] in which backup tapes containing sensitive information have been lost in the mail.

Significance

Intentional threats can also inflict harm to a network. Insider threats from malicious employees and physical break-ins can result in significant losses. Viruses, worms, and trojans can also be intentional threats or result from careless activities by benign employees. Some individuals are skilled at conducting social engineering attacks in which they can obtain private information, such as passwords and patient information, by talking to people who have access to such details [5].

Employee carelessness, both intentional and unintentional, can compromise the integrity of an entire system. Especially in the case of a virus or trojan, the fact that security has been compromised may not become evident until days or months after the intrusion. A compromised network can lead to loss of data, downtime in which the system is unavailable, and disclosure of private information. In a health care setting, system downtime can interfere with patient care and be potentially life-threatening if medical professionals cannot access or receive information from patients' medical devices or the computer system.

Difficulty

Employees must inherently be trusted to some degree by their employer. They are given access to trusted computer systems, secure areas, and information not available to outsiders. Thus, it is very difficult to prevent and sometimes detect compromises that result from insiders.

It is also challenging to control accidental threats resulting from human error or negligence, such as when a door is left unlocked. Also, complete physical security of a system is impossible to obtain. Certain measures, such as physically locking equipment in racks and access controls systems, can make the success of a physical break-in less likely.

Potential Countermeasures

Automatic password checkers can be used to ensure good password habits, e.g. that users pick only "strong" passwords, do not reuse old passwords, and change passwords periodically. Company policies regarding discussing information, giving access to information, etc. can also help prevent compromises. However, it is important to combine prevention techniques with detection and recovery techniques in the event of a compromise. For example, intrusion tolerant systems are designed to be resilient to attacks. Auditing and intrusion detection systems are used to allow detection of compromises by providing audit logs of activities, notifications of unusual activities, etc.

4. Conclusions

Electronic medical devices can provide great assistance for patients and doctors. Each year more and more medical devices are developed with increasing functional capabilities. For example, in the past decade some medical devices have been developed with wireless capabilities. Though advances in technology bring greater flexibility and provide more detailed information for medical professionals, new privacy and security risks are being introduced that did not exist in previous generations of medical systems.

Telemetry spam, while similar in nature to unwanted e-mail spam, could be much more malicious and difficult to prevent. An unauthorized third party could also take actions to drain the battery of an unsuspecting person, resulting in an early or unnecessary surgery. There are also multiple scenarios with regards to privacy, including patient information and medical history, which must now be considered with wireless medical devices. In addition to the medical devices themselves, there are other potential weaknesses in the handling and use of medical data, which could be detrimental to the treatment and care of patients.

History has taught us that it is important to build security into a system during the beginning stages, as it is much more difficult to add security later. In order to prevent or withstand the scenarios discussed above, it is important to consider the four security goals of privacy, availability, integrity, and authentication in a system with medical devices. Patients will need strong security and privacy guarantees in order to instill confidence in a global infrastructure for collecting and storing medical telemetry.

5. References

[1] Diabetes Education and Reseach Center. GlucoTel's BG Meter - First to Support Wire- less Bluetooth. Aug. 28, 2006.
http://diabetescenter.blogspot.com/2006/08/glucotels-bg-meter-first-to-support.html

[2] A. Juels, P. Syverson, and D. Bailey. High-power proxies for enhancing RFID privacy and utility. In G. Danezis and D. Martin, editors, *Privacy Enhancing Technologies (PET)*, 2005.

[3] Ari Juels, Ronald L. Rivest, and Michael Szydlo. The blocker tag: selective blocking of rfid tags for consumer privacy. In *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, pages 103–111, New York, NY, USA, 2003. ACM.

[4] Medtronic. Medtronic timeline of significant events. 2007.
http://www.medtronic.com/corporate/history.html

[5] Kevin D. Mitnick, William L. Simon, and William Simon. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, Inc., New York, NY, USA, 2002.

[6] David Molnar. Security and privacy in two RFID deployments, with new methods for private authentication and RFID pseudonyms. Master thesis, University of California Berkeley, Berkeley, California, USA, 2006.

[7] MSNBC. Bank of America loses customer data. March 1, 2005.
http://www.msnbc.msn.com/id/7032779/

[8] National Academy of Engineering: Greatest Achievements of the 20th Century. Health technologies timeline. 2007.
http://www.greatachievements.org/?id=3824

[9] FDA News. FDA Releases Results of Study on Defibrillator and Pacemaker Malfunctions Part of Agency Drive to Improve Device Safety Monitoring and Public Communications. Sept. 16 2005.
http://www.fda.gov/bbs/topics/NEWS/2005/NEW01231.html

[10] Australian Government Department of Foreign Affairs and Trade. Australia Now: Innovative Australia. Last accessed: Nov. 28, 2007.
http://www.dfat.gov.au/facts/innovative australia.html

[11] The Register. Satanic car key traps 12 motorists in car park of horror. Nov. 2 2007.
http://www.theregister.co.uk/2007/11/02/kent car key/

[12] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. RFID guardian: A battery-powered mobile device for RFID privacy management. In *Proc. 10th Australasian Conf. on Information Security and Privacy (ACISP 2005)*, volume 3574 of LNCS, pages 184–194. Springer-Verlag, July 2005.

[13] The Register. Citibank Admits: We've Lost the Backup Tape. June 7, 2005.
http://www.theregister.co.uk/2005/06/07/citigroup lost tape/

[14] The New York Times. Patients warned as maker halts sale of heart implant part. Oct. 15 2007.
http://www.nytimes.com/2007/10/15/business/15device.html

[15] Medical News Today. New generation of insulin pump - starbridge secures global diabetes contract. Nov. 19 2005.
http://www.medicalnewstoday.com/articles/33847.php

[16] United States Department of Health and Human Services. Office for Civil Rights – HIPAA. 2007.
http://www.hhs.gov/ocr/hipaa/