What about security? Medical Applications and Implantable Medical Devices

Inbar Fried

Fall 2014 – Tufts University

COMP 116 – Introduction to Computer Security

December 12, 2014

I. Abstract

Medical applications and implantable medical devices are gaining momentum in the field of healthcare and will begin to play larger roles in the lives of many people. The integration of our healthcare with our personal applications and smart devices holds a lot of promise in convenience and continual care, but the new security challenges generated by this shift in healthcare are demanding and, unfortunately, often neglected. There are a couple major reasons for the absence of security in these devices and applications, and most of them, such as the lack of education, can be easily addressed. The involvement of people with computer systems security knowledge into this emerging field needs to happen while the field is still young and malleable.

II. Introduction

The field of healthcare has developed immensely in recent years, led directly by progress made in fields such as computer science, electrical engineering, and wireless communications. Advancements in these related fields has sparked a new generation of implantable medical devices and has created a new niche for medical applications. The ability of this new technology to address problems that previously had limited solutions, if any at all, has produced a multi-billion dollar market that continues to grow annually [1].

The success of these products can be attributed to their ability to solve customer needs from a wide range of issues. At the forefront of this market are companies with expertise in various fields including pharmaceutical companies, software development startups, micro-electromechanical systems (MEMS) production corporations, and academic research labs. The primary concerns of these companies differ, ranging from device biocompatibility, device size, drug pharmacokinetics, application-interface simplicity and intuitiveness, patient compliance, sampling rates, publications, and funding.

The progress that has been made in the field so far is substantial, especially given the young age of the field and technology. The potential to create new and exciting products and gain a very large profit has driven many people into the field and will continue to recruit more as it gains traction. Unfortunately, in this rapid drive towards fame, profit, and market ownership the security of these devices and applications is often not given appropriate attention.

Building secure systems in general is very difficult, and the systems of phones and tablets are no exception. There are, however, some easily addressable sources of poor security, including implementations by unqualified individuals, careless mistakes by knowledgeable developers, and ambiguous and strict government regulations. The ultimate risks of leaving security as an afterthought are only slowly being realized and often at painful prices. In this paper we will consider each of these hurdles, propose ways in which they may be addressed, and focus on the dire need to involve security experts in this growing market of medical devices and applications.

III. How it Affects Us

Whether or not we have personally been victims of private medical-information theft, we are all at risk. If we have ever required medical attention or have any form of health insurance, our information is being stored along with hundreds of thousands of other patients' information. We want to believe that this information is secured, but it is not uncommon to hear about medical databases being compromised. In February of this year attackers gained unauthorized access to over 400,000 patients' private information from a Texas healthcare system, and in 2012 a similar attack had compromised nearly 800,000 patients' information in the Utah Department of Health [2].

This problem will only increase in gravity with the integration of medical applications to our smart devices such as phones and tablets. Prior to these personal medical applications, companies that stored medical information would dedicate a lot of effort to building secure databases, but the individuals and startups that develop applications are not aware of the security measures they must take.

Even more concerning is the security of implantable medical devices produced by pharmaceutical companies or MEMS companies whose expertise does not entail software security. As of recently there have been no published attacks on implantable medical devices, but a talk in 2011 at the Black Hat Security Conference brought this concern to the public eye. During the presentation an insulin pump was hacked to display a false blood-sugar level reading to the user. Such an attack could result in the user unnecessarily altering the dosage or failing to do so when needed [3]. Similar work had been published in 2008 where an implantable cardiac defibrillator had been hacked to deliver a potentially lethal shock [4]. These demonstrations prove that such attacks are feasible and are not limited to our imaginations. The targets of attacks on implanted drug delivery systems could be to drain the battery life of the device, release lethal amounts of drug, or on the contrary prevent any drug from being released.

As the average population age increases, the number of people requiring medical assistance will grow [5]. The promise of medical applications and implantable medical devices is exciting, and the field of healthcare has already started heading down that path. As we will likely find ourselves at some point in our lives requiring medical care, either personally or for loved ones, it is imperative that we as the security community get involved in the field now while it is still young and malleable.

IV. Causes of Insecurity

The lack of security in these devices and applications is most often not a result of negligence, but a result of naivety and inexperience. There are several major factors that contribute to the lack of security in medical applications and devices, including work by

unqualified individuals, careless mistakes by development teams, and ambiguous government regulations.

a. Lack of Security Expertise

In Implantable Medical Devices

A main contributor to the issue of inadequate security in medical applications and devices is the work performed by unqualified individuals. This is often an issue in companies that deal with implantable medical devices whose expertise lies in drug formulations, drug pharmacokinetics, material biocompatibility, and device miniaturization. The risks posed by this lack of expertise increase as wireless technology is incorporated into implantable devices. When the first pacemaker was successfully implanted in humans in 1960, the concern of wireless security or patient information being stolen was non-existent [6]. However, the advantages that external communication with implantable devices poses have resulted in increasing efforts to incorporate wireless technology into these micro-devices. The hopes of increased patient compliance, more efficient drug delivery, and safer drug dosing blind these companies to the looming security risks.

Recent work carried out by Robert Langer at MIT and MicroCHIPS successfully completed the first-in-human trial of a wirelessly controlled implanted drug delivery device [7]. The trial consisted of twenty dose deliveries of human parathyroid hormone fragment (1-34) [hPTH(1-34)] to seven post-menopausal women suffering from osteoporosis. The existing delivery method requires self-administered injections, making patient compliance a challenge, and making implantable externally regulated drug delivery devices an appealing alternative.

A wireless controller in the microchip set up a bidirectional communication link between the device and an external computer operated by a qualified programmer. The programmer could communicate to the *in vivo* device a specific well to open, either immediately or at a scheduled time. The device could relay information back to the computer with a confirmation on the dose delivery, as well as remaining device battery life. The trial as a whole received very positive results.

This work is very promising, and is a great example of the benefits that implantable drug delivery systems can provide, however, the important area of device security seems to receive very little attention in the published paper. Currently the communication with such devices, such as the microchip system, requires the device and computer to be within ten feet of one another, making interception of the signal difficult. Despite the current security benefits this limitation provides, it is not hard to imagine that for the sake of a more profitable and convenient feature, such as remote care, a solution to this perceived limitation could be devised without fully considering its present advantages.

The shift towards long-range wireless communication set up between the device and a remote controller would need to be served over a network where all the information is relayed. Precautions, such as encrypting data, would need to be taken to secure the information passed over the network, but the packets of information being sent may still be intercepted and potentially decrypted. The issue will get more complicated when technicians with little security background may try to invent their own cryptographic algorithms, instead of using existing cryptographic algorithms that have mathematical proofs behind their encryption methods. Packet sniffing and similar attacks pose a real

threat and are often the topics of public headlines involving computer systems in banks, retail stores, and online service providers. The integration of wireless communication with the implantable device will generate the same vulnerabilities for the device.

Following the success of the first-in-human microchip trial, there is little doubt that this technology will be incorporated into many other drug-delivery domains. Already Langer and MicroCHIPS are looking to apply the wireless microchip technology as a contraceptive, producing what can be referred to as the "digital-pill" [8]. The area of device security is a challenging topic even for more computer-oriented companies, so it is not a topic that should be overlooked. Hopefully there does not need to be some crisis with an implanted drug delivery system to prove to everyone the seriousness and difficulty of efficient device security and the need for involving experts.

In Medical Applications

Unfortunately, issues of improper security are not unique to medical devices and pharmaceutical companies, but exist in many software-oriented companies as well. The cause of poor security is not negligence, but improper education. Often inexperienced developers either do not understand the extent to which they need to secure their code's functionality or believe that their security methods are superior to published methods. A thought somewhere along the lines of "no one will be able to crack my code because it's original and has never been studied" can lead to very costly outcomes.

In the field of medical applications, all of the data relayed to-and-from the device with the app goes over a wireless network. If all of the devices, including the app's device and the receiver of the data are on the same secure network, as is often the case in hospital settings, the risks of an attacker sniffing the network and intercepting packages are reduced.

However, the involvement of personal smart devices in the market has led to information being passed over multiple networks, possibly going through insecure networks. The risks this insecure transmission poses are strengthened by some common mistakes made by inexperienced developers. These mistakes include passwords that are hardcoded into the system or set to common passphrases, self-generated cryptographic protocols, sending unencrypted data, and permitting user input without size restrictions or input filtering. Even a little knowledge on methods to avoid these common mistakes could provide a substantial amount of security.

b. Failing to Prioritize

Even with working knowledge of all of these potential pitfalls, medical application developers are often mesmerized by the potential to add some new and exciting feature or perfect the graphical user interface that they leave security as a final task.

Having recently finished a project for a medical applications class, I am aware of the ease with which security is left as an afterthought. As a team of five students, we designed and implemented a mobile patient monitor for the iPad that would serve as a supplement to an existing patient monitor. The iPad received information from an Arduino that read patient information from ECG, temperature, and blood pressure sensors. Throughout the development process security had been brought up, but due to strict deadlines and a long list of desired features we had left the topic of security untouched. We presented our final product on December 4th, having finished most of the features we set to implement and leaving a place for security in the "Future Work" slide, a recurring pattern throughout the semester.

Out of interest I packaged the application for a static analysis on the Veracode website. The scan gave the app a perfect score of 100 and reported that the app had passed all of the tests and that no security issues, neither "very low" nor "very high", had been found. I was extremely surprised to receive such results, being aware of various areas where safety could be a concern in the app. Based on my insider knowledge I know that some security issues in the app's code include the transfer of unencrypted data from the Arduino over a Wi-Fi network to the iPad, the lack of user-input filtering or size-restrictions upon password entry, and the lack of input verification on the input from the Wi-Fi network. Fortunately for us this application was never sending sensitive patient data or storing a patient identifier.

This personal experience demonstrates the importance of performing further security analysis past a static scan. The limitations of a static scan are known, mainly its inability to detect errors that occur in the runtime environment, but the issues listed above would not be revealed through a dynamic scan either. Review of the code by security experts is necessary for a more conclusive evaluation of code security, and most importantly, security cannot be left on the back burner and placed on a "Future Work" slide. Strict deadlines and required features are challenges that every product team faces, but prioritizing security throughout the development process is necessary.

c. Ambiguous Regulations

Of the barriers to better security, the most complicated and confusing are the government regulations. In 1996 President Clinton signed the Health Insurance Portability and Accountability Act (HIPAA) in order to establish federal standards for the security of electronic health information [9]. This act set clear guidelines for health

systems in companies and hospitals, but since 1996 a lot has changed and continues to change. The U.S. Food and Drug Administration (FDA) regulate medical devices and applications, but their standards on the technology and features of these products are not clear, possibly due to their own lack of understanding of the field and its future projection.

In September of 2013 the FDA released a document they announced as their final guidance for medical applications, titled "Guidance for Industry and Food and Drug Administration Staff" [10]. Without even reading through the document, which is filled with ambiguous definitions and links to other federal laws, the use of the words "final" and "guidance" already raise questions; not to mention the "contains nonbinding recommendations" title on the front cover. How can this be the final document pertaining to the regulation of medical applications if the field is still in its infancy? And if this document is just "guidance", how enforced is its content? Too many doors are left open and too many questions regarding security are left unanswered, contributing to the mess of security in the current system.

Although many of the laws are ambiguous and deciphering their meaning is left in the hands of companies, there are basic requirements that every device or application should meet in order to ensure consumer safety. Some of these features include: strong user authentication, data confidentiality, data accuracy, data accessibility, data wiping, encrypted network protocols, and extensive testing [11]. These requirements are known and are very clear, meaning that the ambiguity of the FDA is no excuse for insecure systems in these domains. By addressing these basic security measures, we can set an

example to others and to the FDA; helping both parties make the confusing guidelines more transparent.

V. Conclusion

The research and products in the field of medical applications and implantable medical devices are very interesting, exciting, promising, and profitable. The issues that the products address are very real and will continue to persist as more and more people reach elderly years of age. The thrill of implementing a sexy new feature or designing a drug with perfect efficacy are all valid goals, but they should not come on top of building secure systems. Up until now we have been able to squeeze by while leaving security as an afterthought, but the attacks described by Radcliffe and Halperin et al. will become more of a reality if left untreated. Chances are that medical applications or implantable medical devices in some way will impact most of us, and we do not want to wait to address the problem for a time when it is too late. We as the security community need to educate others and get involved in these products, offering our expertise and domain knowledge. Building very secure systems is difficult, but there are steps we can take now towards ensuring a basic level of security in this field.

References

1. "MHealth Market Is Expected to Reach $58.8 Billion Globally by 2020 According to Allied Market Research Projections." PR Newswire. Allied Market Research, 14 Nov. 2013. Web. 10 Dec. 2014. < http://www.prnewswire.com/news-releases/mhealth-market-is-expected-to-reach-588-billion-globally-by-2020-according-to-allied-market-research-projections-231971081.html>
2. McCann, Erin. "Hackers Swipe Health Data of 405K." Healthcare IT News. Healthcare IT News, 5 Feb. 2014. Web. 10 Dec. 2014. < http://www.healthcareitnews.com/news/hackers-swipe-health-data-405k>
3. Radcliffe, Jerome. "Hacking medical devices for fun and insulin: Breaking the human SCADA system." Black Hat Conference presentation slides. Vol. 2011. 2011.
4. Halperin, Daniel, et al. "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses." Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE, 2008.
5. Ortman, Jennifer M., Victoria A. Velkoff, and Howard Hogan. "An aging nation: the older population in the United States." Proc. Economics and Statistics Administration, US Department of Commerce (2014).
6. Greatbotch, Wdson, and Curtis F. Holmes. "History of implantable devices." (1991).
7. Farra, Robert, et al. "First-in-human testing of a wirelessly controlled drug delivery microchip." Science Translational Medicine 4.122 (2012): 122ra21-122ra21.
8. Dockterman, Eliana. "The Future of Birth Control: Remote Control Fertility." TIME: Health. TIME, 7 July 2014. Web. 10 Dec. 2014. < http://time.com/2963130/the-future-of-birth-control-remote-control-fertility/>.
9. "Health Insurance Portability and Accountability Act." California Department of Health Care Services. N.p., n.d. Web. 08 Dec. 2014. <http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx>.
10. "Guidance for Industry and Food and Drug Administration Staff." Mobile Medical Applications. US Food and Drug Administration, 25 Sept. 2013. Web. 10 Dec. 2014. <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm359130.htm>.
11. Kobes, Shelby David. "Security implications of implantable medical devices." (2014).

The Mobile Patient Monitor I built as part of the team is available at:
https://github.com/ifried01/MMD/tree/master/Project2-ECG
and the Veracode scan results are included in this directory.