Security Challenges for Medical Devices

Johannes Sametinger[1], Jerzy Rozenblit[2], Roman Lysecky[3], Peter Ott[4]

[1] Dept. of Information Systems, Johannes Kepler University Linz, Austria, johannes.sametinger@jku.at
[2] Dept. of Electrical and Computer Engineering/Dept. of Surgery, University of Arizona, USA, jr@ece.arizona.edu
[3] Dept. of Electrical and Computer Engineering, University of Arizona, USA, rlysecky@ece.arizona.edu
[4] College of Medicine, Sarver Heart Center, University of Arizona, USA, ottp@email.arizona.edu

Abstract—**Information Technology (IT) security is essential for any business or organization, including healthcare. This sector poses additional challenges due to the sensitivity of health records, the increasing interoperability of medical devices, and simply the fact that human well-being and life are at stake. Implantable devices are especially critical, as they may potentially put patients in life-threatening situations when not properly secured. Medical devices are becoming noticeably important for millions of patients worldwide. Their increasing dependence on software and interoperability with other devices via wireless communication and the Internet has increasingly put security at the forefront. In this paper, the key issues that motivate research in medical device security are identified. Major challenges are presented along with an illustrative example. A stage is thus set to spur research and development in this life-critical area of technology.**

Keywords–security; medical devices; cardiac pacemakers; security risk.

I. INTRODUCTION

Security and safety issues in the medical domain take many different forms. Examples range from purposely-contaminated medicine to recalls of vascular stents, and health data breaches. Risks resulting from unintentional threats have long been known, e.g., interference from electromagnetic energy. Security risks resulting from intentional threats have only recently been confirmed, as medical devices increasingly use newer technologies such as wireless communication and Internet access. Intentional threats include unauthorized access of a medical device or unauthorized change of settings of such a device. A senior official at the FDA's device unit has often been cited with the following statement: "*We are aware of hundreds of medical devices that have been infected by malware.*" [34]. Even though deaths and injuries have not yet been reported from such intrusions, it is not hard to imagine that someday they will. There is no doubt that health care will increasingly be digitized in the future. Medical devices will increasingly become smarter and more interconnected. The risk of computer viruses in hospitals and clinics is one side effect of this trend. More data breaches and even malicious attacks threatening the lives of patients may result without suitable countermeasures.

Security is about protecting information and information systems from unauthorized access and use. As mentioned above, medical devices have more and more embedded software with communication mechanisms that now qualify them as *information systems*. Confidentiality, integrity and availability of information are core design and operational goals. Secure software is supposed to continue to function correctly under a malicious attack [25]. In this sense, medical device security is the idea of engineering these devices so that they continue to function correctly even if under a malicious attack. This includes internal hardware and software aspects as well as intentional and unintentional external threats. Medical devices comprise a broad range of instruments and implements. For our considerations, only devices with hardware, software and some form of interoperability are of interest. Artificial joints, for example, do not do any processing, i.e., there is no software involved. Thus, we can ignore them from a security perspective. However, they may indeed be critical from a safety point-of-view.

At this point, we emphasize the importance of secure medical devices. It is not really about preventing someone from killing someone else by means of a medical device. However remote and unlikely this scenario might sound, it is not completely implausible. Securing medical devices is securing a critical infrastructure. It is about preventing malicious people from taking control of this infrastructure, about preventing a potential blackmail of device manufacturers or health institutions, and about the sense of well-being of any person who needs to use any such device.

II. MOTIVATION

Major IT security incidents that affect the general public are almost regularly reported in the media. Examples include stolen passwords, stolen credit card information, or website availability problems. The loss, theft, or exposure of personally identifiable information is one major problem that is also widespread in the healthcare sector, which accounts for one fifth of all these reported issues [33]. The FDA collects information regarding reportable issues with medical devices to capture and identify adverse and unexpected events for a particular device or device type. Each year, several hundred thousand medical device reports are received about suspected device-associated deaths, serious injuries and malfunctions [6]. An analysis of these recalls and events has shown that both the number of recalls and adverse events have increased over the years. The major reason for recalls involves devices' malfunctions. Computer-related recalls account for about 20% to 25%, and counting. The numbers show that computer-related recalls are caused mainly by software [1]. More than 90% of device recalls mentioned the word 'software' as the reason for the corrective action. Less than 3% mentioned that an upgrade would be available online [23]. Kramer et al. also tested FDA's adverse event reporting by notifying a device's vulnerability, only to find out that it took

several months before the event showed up in the corresponding database [23]. This time-span is definitely much too long to respond to software-related malfunctions.

Successful *hacking* of medical devices has been demonstrated on several occasions. For example, commands have been sent wirelessly to an insulin pump (raise or lower the levels of insulin) and to disable it. This could be done within a distance of up to 150 feet [20]. The FDA's safety communication has issued a warning to device makers and healthcare providers to put safeguards in place to prevent cyber-attacks [9]. Deaths or injuries are not yet known, but the hypothetical ramifications are obvious. The non-medical IT landscape can also pose a threat to medical operations. For example, when computers around the world came to a halt after an antivirus program identified a normal system file as a virus, hospitals had to postpone elective surgeries and to stop treating patients [11].

III. Medical Devices

Medical devices include everything from simple wooden tongue depressors and stethoscopes to highly sophisticated computerized medical equipment [37]. According to the World Health Organization (WHO), a medical device is "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article" intended for use in the diagnosis, prevention, monitoring, treatment, etc. of disease or other conditions [37]. The FDA uses a similar definition [7]. Classes of medical devices have been defined differently in, e.g., the United States, Canada, Europe or Australia. The FDA has established classifications for approximately 1,700 different generic types of devices. These devices are grouped into medical specialties, called panels. Examples for FDA's specialty panels include cardiovascular devices, dental, orthopedic, as well as ear, nose and throat devices. Active devices may or may not involve software, hardware, and interfaces, which are important when considering security issues. These devices can do some processing, receive inputs from outside the device (sensors), output values to the outer world (actuators), and communicate with other devices.

A. Device Safety

Each of the FDA's generic device types is assigned to one of three regulatory classes: I, II and III. The classes are based on the level of control that is necessary to assure the safety and effectiveness of a device; the higher the risk, the higher the class [8]. For example, class III devices have to be approved by a premarket approval process. This class contains devices that are permanently implanted into human bodies and may be necessary to sustain life, e.g., artificial hearts or an automated external defibrillator. The classification is based on the risk that a device poses to the patient or the user. Class I includes devices with the lowest risk, class III those with the greatest risk.

According to the WHO, optimum safety and performance of medical devices requires risk management with the cooperation among all involved in the device's life span, i.e., the government, the manufacturer, the importer/vendor, the user and the public [37]. The international standard ISO 14971:

2007 provides a framework for medical device manufacturers including risk analysis, risk evaluation and risk control for risk management in a device's design, development, manufacturing, and after sale monitoring of a device's safety and performance [18].

B. Device Security

We consider a medical device to be security-critical if it does some form of processing and communicating, typically by running some form of software on specialized hardware, and often, employing a range of sensors [7]. Sensing devices constitute a security threat, because wrong sensor values may later induce therapeutically wrong decisions by doctors or devices. Safety-critical information has an influence on the safety of a person or her environment. Examples include parameter settings or commands for devices such as implanted defibrillators or x-ray machines. Both malicious and unintentional modification of such information may lead to safety-critical situations. Sensitive information includes anything that is about a patient, e.g., medical records as well as values from sensing devices that report information about a person's or her device's state, e.g., glucose level, ID, or parameter settings of a pacemaker. It is interesting to note that all medical devices as defined by the WHO or by the FDA have aspects that are inherently safety related. Some have a higher risk, some a lower one, cf. FDA's classes I, II and III. However, not all of these devices are relevant from a security point of view; remember the above-mentioned artificial joint. Typically, security is an issue as soon as software is involved. But there are also security-relevant devices that are not considered to be medical devices by the WHO or the FDA. Examples include smartphones that run medical apps handling sensitive information, or regular PCs in a hospital for processing medical records.

The difference between safety and security is not always obvious, because security can clearly have an effect on safety. Generally speaking, safety is about the protection of a device's environment, i.e., mainly the patient, from the device itself. The manufacturer has to make sure that the device does not harm the patient, e.g., by not using toxic substances in implants or by careful development of an insulin pump's software. Security is about the protection of the device from its environment, i.e., just the opposite to safety. As long as a device is operating in a stand-alone mode, this is not an issue. But if a device communicates with its environment or is connected to the Internet or other systems, then someone may get access to data on the device or even gain control over it. A security issue becomes a safety issue when a malicous attacker gains control of a device and harms the patient.

Non-communicating but processing devices can be critical to security when attackers have managed to implant malicious hardware or software before the device gets installed. Examples include hardware or software Trojans that might be installed in heart pacemakers to be activated upon a specific event. Precautions have to be taken at the design and development processes in order to avoid such attacks. Communicating devices, of course, provide a broader attack "surface." We suggest a security classification of medical devic-

es depending on whether they process or communicate sensitive information and on whether they process or communicate safety-critical information. Table 1 summarizes our proposed levels for devices that are security-relevant. Note that this set is an initial classification. While not yet fully elaborated, it is as a first step towards developing a more comprehensive taxonomy of security levels.

Health care professionals increasingly improve and facilitate patient care with mobile medical applications. Patients more and more manage their health and wellness with such applications. Such apps may promote healthy living and provide access to useful health information. Mobile medical apps can be used for a plethora of uses. They can extend medical devices by connecting to them for the purpose of displaying, storing, analyzing, or transmitting patient-specific data. Not every mobile medical application necessarily poses a security risk. However, as soon as it processes or transmits sensitive information or even controls the medical device, security precautions have to be taken.

IV.   PACEMAKER SCENARIO

We will illustrate security issues through an example of pacemakers, i.e., medical devices that are implanted in patients to regulate the patient's heart rate. The purpose of such a device is to maintain an adequate heart rate of a patient whose heart would not be able to do so otherwise. Pacemakers are classified as Class III, the highest safety category.

A. Clinical Perspective

Implantable medical devices are prevalent in many medical specialties. The implantable cardiac pacemakers and defibrillators can be especially critical for the patient's health and welfare. These devices are implanted in hundreds of thousands of patients every year; many of these patients would not be able to live without a fully functional device. Patients with these types of implantable devices are typically seen in a follow-up on a regular basis, in an outpatient clinic or hospital setting, where the device is interrogated and adjustments are made as needed. Trained staff or physicians perform these functions using a vendor specific programming system, which communicates with the device by means of a wand or wireless technology. In addition, over the last several years essentially all device vendors have established a home-based device follow-up system. For this purpose, a data module is located at the patient's home, typically at the bedside. Once the patient is in proximity to the data module, wireless contact is established and the data module interrogates the device. This information is sent (typically through a telephone landline) to an Internet-based repository. Authorized health care professionals can view this information.

Implantable cardiac pacemakers and defibrillators are highly reliable. Nevertheless, failure of device components has occurred and highlighted the potential medical and legal implications. These failures have largely been due to problems with manufacturing processes and/or materials and have typically been limited to certain device batches. Almost always, however, such device failures require surgical device replacement. With the increasing prevalence of web-based wireless remote device follow-up systems, concerns about

Table 1: Security levels of medical devices

Security level	Description	Device examples
Low	Neither sensitive nor safety-critical activity	PC in hospital used for administrative work Heart rate watch
Medium	Sensitive activity	PC processing EHRs Smartphone communicating glucose levels
High	Safety-critical activity	Device controlling insulin pump or sending parameters to pacemaker
Very High	Safety-critical activity, input from elsewhere	Pacemaker receiving external parameters

device security have arisen. At this time these remote follow-up systems are in read-only mode. However, device programming through remote follow-up systems is being investigated. Incorrect programming either by error, technical failure or malicious intent could have potentially life-threatening implications for the patient.

B. Risk Assessment

In our pacemaker scenario, we distinguish different risks according to the CIA triad, i.e., confidentiality, integrity and availability. First, confidentiality, i.e., sensitive data about the patient and her pacemaker may be disclosed. Second, integrity, i.e., data on a device may be altered, resulting in a range of slightly to highly severe impacts on the patient. Third, availability, i.e., a device may become inoperable. An architectural overview of the pacemaker environment is given in Figure 1. While the pacemaker itself is communicating wirelessly, other communication is done via the Internet, a phone line, and sometimes by means of an USB stick. Even if programming devices may not yet have a direct connection to the clinic, sooner or later, they will.

Information disclosure and tampering may happen on any connection between devices. On the Internet, a man-in-the-middle attack can occur, unless appropriate measures such as encryption mechanisms have been used. Wireless communication additionally allows attackers to listen to the traffic with a separate device, i.e., another programming device, another home monitor, or a different device specifically for an attack. Such devices can be used not only for listening but also to pretend being an authorized communication partner. Denial of service attacks may occur as well. In our scenario, the biggest threat stems from the pacemaker's interop-
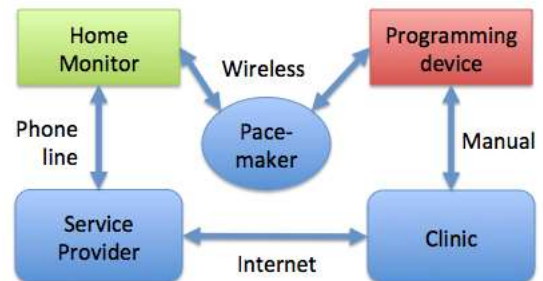

Figure 1: Pacemaker environment

erability. The purpose of an assessment of a device's risks is a determination of risks, their degree of harm as well as the likelihood of harm occurring [27]. Based on this information, countermeasures have to be identified and selected.

C. Software

Software vulnerabilities are bugs or flaws in software that can directly be used by attackers to gain access to a system or network. Software for pacemakers is confidential and proprietary. A system specification is available for academic purposes [2]. It demonstrates the complexity of these seemingly simple devices. There are many programmable parameters, e.g., lower and upper rate limit, as well as various delays and periods. Functionality includes device monitoring, lead support, pulse pacing, various operation modes and states as well as extensive diagnostic features. Software is not only needed on the pacemaker itself, but also on the programming device and on the home monitor. Software on the programming device is needed to non-invasively re-program a pacemaker, e.g., to modify the pacemaker rate, to monitor specific functions, and to process data obtained from the pacemaker. Such software can work with one or a few models of devices, typically from the same manufacturer. Software on the home monitor has to communicate with the pacemaker and to mainly upload important information to a specific server, where personnel from the clinic can later access it. Installing updates may be necessary on both the programming and the home device, but also on the pacemaker itself. A compromised pacemaker can directly do harm to its patient. A compromised programming device can do so indirectly. It may just send other parameters to the device than the ones the cardiologist has chosen. A compromised home monitor also poses a serious threat. If it uploads incorrect values to the server, then these values may lead the cardiologist to wrong conclusions and eventually to wrong device settings that may harm the patient. Last but not least, a compromised server that stores all these values poses a similar threat.

D. Hardware

Hidden malicious circuits provide attackers with stealthy attack vectors [21]. Various potential attacks like privilege escalation, login backdoor, and password stealing have been demonstrated. The hardware of pacemakers is, like its software, confidential and proprietary. A hardware reference platform is available at the University of Minnesota. It is based upon an 8-bit microcontroller [26]. Hardware for programming devices and home monitors is less constrained. These devices have no space and power constraints and are comparable to regular PCs. Similarly to software, malicious hardware circuits can be placed on the medical device itself, but also on other devices it communicates with, i.e., the programming device and the home device in our pacemaker scenario. Malicious hardware on the web server, where pacemaker data are stored, also poses a threat by either revealing sensitive medical data or by even modifying these data and, thus, misleading the treating physician.

E. Interoperability

Security issues of pacemakers have also been raised due to their capability of wireless communication. Concerns include unauthorized access to patient data on the device as well as unauthorized modifications of the device's parameters. Needless to say, modified settings may harm patients' well-being, cause severe damages to their hearts and even cause their deaths. Device integrity is at stake when its wireless communication is attacked. The crucial question is whether it is possible for unauthorized third parties to change device settings, to change or disable therapies, or even to deliver command shocks. Halperin et al. have partially reverse engineered a pacemaker's communications protocol with an oscilloscope and a software radio and have then implemented several attacks able to compromise the safety and privacy of patients [15].

Even if hardware and software of all devices in our pacemaker scenario are free of malware, an attacker may still pose a threat by communicating with either one of these devices, i.e., the home monitor, the programming device, the service provider's web server or the pacemaker itself. Interoperability requires protocols that define sequences of operations between the two communicating parties. These sequences have to ensure the protection of data. Network protocols have often suffered from vulnerabilities, thus, allowing attackers to pretend being someone else. Attackers may use a modified programming device with stronger antennas that allow them to communicate with a pacemaker from a longer distance. They may then pretend to be the authorized cardiologist and modify settings of the device. Similarly, they may act as the home device and read out sensitive data, or communicate with the home device, pretending to be the pacemaker, and relay wrong values.

V.   CHALLENGES

Critical assets deserving strong protection in healthcare include medical records, a plethora of medical sensors and devices, and last but not least, human health and life. The security of medical devices is different and more challenging vis-à-vis regular IT security for several reasons, not just because of the fact that human life is at stake. Clearly, non-medical devices like automobiles can also endanger human life if their safety is compromised through a security breach. One can imagine a scenario where malware is implanted into a dynamic stability control system to intentionally cause an accident. But many medical devices impact the patients' physiology and, thus, pose a permanent threat. Resource constraints are present not for all, but for many, most notably implanted medical devices. Little memory, processing power, physical size limitations and battery life limit the options that are available for security countermeasures. Emergency situations provide an additional challenge that is not present in other domains. Medical devices must prevent unauthorized access, yet may need to allow for a quick and simple access in emergency situations. Another problem is reproducibility. Security researchers often lack access to proprietary devices and are, thus, limited in their ability to study attacks and defenses.

Several countermeasures to vulnerabilities in medical devices have been described [4][14]. They can be protective, corrective, or detective. Examples are auditing, notification, trusted external or internal devices, and cryptographic protections [16]. In what follows, we enumerate various challenges and postulate a means of tackling them.

A. Software Security

Besides the functionality, software developers of medical devices have to take measures to ensure the safety as well as the security of their code. Both *secure development* and *secure update mechanisms* are needed. Risks of medical device software have also been described in [12].

1) Secure Development

Security is a volatile property. A system is never 100% secure. As long as vulnerabilities are unknown, this is not a problem. When attackers know a specific vulnerability, the target system is at risk. The engineering of secure medical software is not radically different from the development of other types of software. It is a common misconception that only bad programmers write insecure code. Besides the underlying complexity of writing code, it takes detailed knowledge, extra training and additional development activities in order to write secure code [17]. Thus, economic and sometimes social factors often play against security quality.

In medical device software we must make sure that both safety and security have top priority and that there is a defined process to report and fix vulnerabilities. The challenge for medical devices includes the fact that additional code for security must not interfere with real-time constraints and other resource constraints like limited battery power.

2) Update Mechanisms

When manufacturers of a system know about vulnerabilities, they will address and correct the problems. A fix must then be distributed to the systems with that vulnerability. The update mechanism itself may be misused for an attack. Updates and patches are (still) much less frequent for medical devices than they are for personal computers and smartphones. However, sometimes they will be necessary.

We need user-friendly update processes for medical devices and take precautions such that malware is not involved in the update process itself. In addition, the update must not break the device or halt its proper functioning.

3) Off-the-shelf software

Off-the-shelf software often "powers" medical technology. On medical devices, software patches or updates are often delayed or are even missing all together. Missing patches may also be an organizational problem. Delays may result from the fact that device manufacturers must approve upgrades to software as well as any security installations [36]. The problem with old software versions is that they often contain known vulnerabilities.

Old software in medical devices was not an issue as long as these devices operated stand-alone. Increasing interconnection makes these devices vulnerable even with old malware [12]. For medical devices, it is important that the production lifecycles of embedded software must match the devices' production lifecycles. Manufacturers have to make sure that software is not used on medical devices after its support has expired.

B. Hardware Security

Safety issues are more prevalent in hardware than the security concerns. An example includes the electromagnetic interference of non-medical devices with pacemakers. Hardware Trojans on medical devices seem unrealistic today, but precautions have to be taken to reduce attack vectors wherever possible. Backdoors in military chips have already been documented, where attackers could extract configuration data from the chip, reprogram crypto and access keys, modify low-level silicon features, and also permanently damage the device [30]. An approach for automatic embedding of customizable hardware Trojan horses into arbitrary finite state machines has been demonstrated. These Trojan horses are undetectable and improvable [35]. Radio pathways have been embedded into computers, where computers could be remotely controlled and provided with malware even when they were not connected to the Internet [29].

We must keep in mind, that hardware Trojans can be an attack vector for medical devices, too. It is important to make sure that such malware not be installed in the manufacturing process. Given the reliance on computer aided design tools, it is further necessary to ensure hardware Trojans are not inserted in the design by these tools. Verification methods utilized in designing hardware should ensure that the resulting output designs match the inputs and do not contain additional circuitry. Outside of using trusted manufactures for each stage of design, ensuring Trojan free hardware is not practical. Thus, *detection and mitigation* capabilities will still be needed. Once malicious hardware is detected and its behavior is understood, research on how to mitigate the affects of the malicious hardware to ensure safety of medical devices will be of critical importance.

C. Interoperability

Increasingly, medical devices rely on wireless connectivity, be it for remote monitoring, or for remote updates of settings or even for an update of the software itself. Interoperability challenges include secure protocols, authentication, authorization, encryption, and key management. Interoperability of medical devices is especially tricky due to medical emergency situations. In case of an emergency, health personnel may need to access not only medical records, but also medical devices of a person in need, perhaps in a life-threatening situation. Authentication and authorization mechanisms must have a bypass or shortcut for such circumstances. However, these bypasses and shortcuts should not provide a means that enable attackers to gain access to the device.

Initiatives to secure the interoperability of medical devices include externally worn devices [3], e.g., a trustworthy wrist-worn amulet [31], and software radio shields [13]. Researchers have also created a prototype firewall to block hackers from interfering with wireless medical devices [32] and to authenticate via physical contact and the comparison of ECG readings [28].

D. Organizational

Security is most effective when designed into the system from the very initial development cycle. It is important to develop and maintain threat models and to assess risks during device development. A systematic plan for the provision of software updates and patches is needed. Last but not least, a security response team has to permanently identify, monitor, and resolve security incidents and security vulnerabilities.

For that purpose, user facilities such as hospitals and clinics should be incentivized to report security occurrences. These reports can provide valuable insights into security problems of medical devices. In addition, we propose the definition of security and threat levels for medical devices with defined rules of action and an audit guideline for all involved stakeholders. The levels defined in Table 1 are a small first step in that direction. We imagine simple scores for medical devices that summarize their sensitivity, their impact as well as their exposure and their current threat level. Rule-based actions could then trigger needed actions to react to security-related incidents.

E. Regulations

It is important to know at any time the level of danger and to take appropriate countermeasures. Design and distribution of medical devices is tightly regulated. In the US, the FDA has the authority over medical device distribution. A device manufacturer has the responsibility for the approved configuration of the device. Device users, such as hospitals and patients, do not have access to a device's software environment and cannot install additional security measures. Any upgrade or update – either added functionality or security measures – typically needs to be approved by the manufacturer. Thus, deployment of security-relevant upgrades typically gets delayed [36]. Manufacturers, importers, and device user facilities are required to report specific device-related adverse events and product problems.

Surveillance strategies have to be reconsidered in order to effectively and efficiently collect data on security and privacy problems in medical devices [23]. Some regulation aspects as well as the role of standards bodies, manufacturers, and clinical facilities have been discussed in [12]. We see a demand for action to adjust the increasing need for software updates for medical devices with the need to redo clinical trials after major changes.

F. Malware detection

Vulnerabilities are often unknown until malware exploiting those vulnerabilities is detected. We need methods to detect the presence of malware. Malware detection techniques include control-flow integrity verification, call stack monitoring, dataflow analysis, and multisource hash based verification. Although software-based malware detection methods are suitable for traditional computing systems, the performance overhead may be prohibitive for medical devices with strict time constraints. Hardware-based detection methods can reduce or eliminate the performance overhead, but power consumption remains a challenge.

For medical devices, we need malware detection methods that are non-intrusive with very low power consumption, as power is a precious resource, especially in implantable devices. In order to provide resilience to zero-day exploits, anomaly-based malware detection methods will be needed. These methods rely on accurate models of normal system behavior, which will require both formal methods for modeling this behavior and tight integration with system design tasks. The importance of timing requirements in medical devices may provide a unique system feature that can be exploited to better detect malware.

G. Malware reaction

Detecting malware only addresses half of the problems. Once malware is detected, how should the medical device respond? Notification is a straightforward option, but it allows the malware to remain active until the device can be inspected or replaced. Automatically re-installing the software may be feasible if halting the device temporarily is safe for the patient. We live in an interconnected world. Unplugging from the Internet may cause a bit of distress but is unlikely to harm one physically. However, life-critical medical devices present a much more complex set of challenges. Clearly, any reprogramming, resetting, or disconnecting a device such as a demand pacemaker, which paces the heart only if the rhythm is abnormal, is less disruptive than it would be in a permanent pacemaker. Trade-off decisions must be considered in such situations. Replacing the device might be an option, but what about the time until the device gets replaced? Being able to turn off any communication to the device is at least a first step, which had been taken by a former US Vice President to avoid a potential terroristic attack [22]. It has to be clear, though, that this step may come too late if malware had already been planted onto the device before terminating the communication capabilities. Resetting the device may be an option in this scenario.

Notifications alert patients to potentially malicious activities [15]. However, notifications of security breaches would rather unnerve worried patients. We imagine different device modes that may be switched when malware is suspected or even known. One such mode, for example, could switch off any communication and use predefined, safe parameter settings. Critically, the design of alterative safe modes must ensure that various software implementations are isolated, both through software safeguards and secure hardware architectures, such that malware cannot alter the operation of the safe modes. Fail-safe features have to protect a device's critical functionality, even when security has been compromised [10].

H. Formal Methods

Finding vulnerabilities in software and hardware before being deployed within a medical device can significantly increase security. In practice, eliminating all security vulnerabilities is infeasible and impractical. Formal verification methods can be applied to analyze temporal behavior and to detect potential vulnerabilities [24]. Guaranteeing timing properties is an important issue when developing safety-critical real-time systems like cardiac pacemakers. Jee et al. have

presented a safety assured development approach of real-time software using a pacemaker as a case study [19]. They followed model-driven development techniques and used measurement-based timing analysis to guarantee timing properties both in their implementation and in the formal model.

Formal methods play an important role in ensuring the hardware and software for medical devices operate as designed. We further believe that formal methods should be utilized to verify correctness of software updates, malware reaction methods, and other runtime system reconfigurations. Formal modeling and verification are essential to ensuring that changes to the system at runtime can be accomplished without impacting device behavior.

I. Resource constraints

Limited power/energy and limited sizes may make known security solutions impractical. For example, an implanted defibrillator may not have the resources to run commercial anti-virus software. Even if it could do so, it may drain the battery too much. In addition, such software would have to connect to the Internet to keep virus information up-to-date and, thus, open up yet another attack vector. Limited memory may necessitate the use of scaled back versions of operating systems. It also makes it more difficult to utilize common security software [36].

Recent research has shown tiny power generators that can convert the motion of a beating heart into electrical energy and implantable devices that can be wirelessly recharged. Zero-power notification and authentication with induced RF energy at no cost to the battery has also been shown, e.g., to audibly alert patients of security-sensitive events [15]. But limited resources will still confine security measures in many medical devices.

J. Non-technical aspects

In addition to technical security aspects of medical devices, we have to consider non-technical issues as well. Security awareness is one major aspect. Technical security measures are useless, when people, for example, provide log-in credentials to unauthorized people. Technically viable systems may nonetheless be undesirable to patients.

The general population is increasingly concerned about the misuse of the Internet in many aspects of their daily life, e.g., banking frauds or identity theft. As a cardiologist and electro-physiologist, one of the authors (P. Ott, MD) has observed an increase in patients' awareness of security issues by questioning the safety of implanted devices in the digital realm. We expect that such concerns will become more and more pressing. A small study has shown that perceived security, safety, freedom from unwanted cultural and historical associations, and self-image has to be taken into account when designing countermeasures for medical devices [5]. We need more information about how concerned patients are about the security of the devices they are using. A user study could reveal what specific, additional steps patients are willing to take in order to increase security. This will give manufacturers valuable information. We will need to increase security awareness of all stakeholders, i.e., manufacturers, patients, doctors, and medical institutions. Additionally, the devices' security states have to be more visible, understandable, and accessible for all stakeholders.

K. IT Infrastructure

In order to protect medical devices, the surrounding IT environment has to be secured as well. Focusing on medical devices, we will refrain from enumerating regular countermeasures found in IT security. These are appropriate for healthcare security or medical device security as well, e.g., erasing hard disks before disposing of them, backing up data, or BYOD (bring your own device) policies. Off-the-shelf devices like smartphones or tablets also increasingly store, process, and transmit sensitive medical data. This data has to be protected from malware on these devices.

IT infrastructure has to guarantee privacy of medical data according to the Health Insurance Portability and Accountability Act (HIPAA). However, safety is at stake as well. For medical devices, it is important to keep in mind that regular IT devices pose a threat to medical devices also when they interoperate directly or indirectly. Most importantly, medical devices should always assume that their surrounding might have been compromised.

VI. CONCLUSION

Securing medical devices means protecting human life, human health, and human well-being. It is also about protecting health information and securing the privacy of sensitive health information. We see an increase in the use of mobile medical applications as well as an increase in medical devices that use wireless communication and utilize Internet connections. New sensing technology provides opportunities for telemedicine with the promise to make healthcare more cost-effective. Unless appropriate countermeasures are taken, the doors stand wide open for the misuse of sensitive medical data and even for malware and attacks that put human life in danger.

REFERENCES

[1] Alemzadeh H., Iyer R.K., Kalbarczyk Z. Analysis of Safety-Critical Computer Failures in Medical Devices. IEEE Security & Privacy. Vol. 11, no. 4, pp. 14-26, July-Aug. 2013.

[2] Boston Scientific. PACEMAKER System Specification. 2007.

[3] Denning T., Fu K., Kohno T. Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security. Proceedings of USENIX Workshop on Hot Topics in Security (HotSec), July 2008.

[4] Denning T., Matsuoka Y., Kohno T. Neurosecurity: security and privacy for neural devices. Neurosurgical Focus, 27(1), July 2009.

[5] Denning T. et al. Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Devices. Proceedings of the 28th International Conference on Human Factors in Computing Systems (CHI '10), 2010.

[6] FDA. MAUDE - Manufacturer and User Facility Device Experience. http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/search. CFM

[7] FDA. Is The Product A Medical Device? http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/ Overview/ClassifyYourDevice/ucm051512.htm

[8] FDA. Medical Devices – Classify Your Medical Device. http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/ Overview/ClassifyYourDevice/default.htm

[9] FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks. June 2013. http://www.fda.gov/ MedicalDevices/ Safety/AlertsandNotices/ucm356423.htm

[10] FDA. Content of premarket submissions for management of cyber-security in medical devices—Draft guidance for industry and Food and Drug administration staff, June 14, 2013. http://www.fda.gov/medicalDevices/Deviceregulationandguidance/guidanceDocuments/ucm356186.htm

[11] Fox News. Antivirus Program Goes Berserk, Freezes PCs. April 22, 2010.

[12] Fu K., Blum J. Controlling for Cybersecurity Risks of Medical Device Software. Communications of the ACM, Vol. 56 No. 10, Pages 35-37, Oct. 2013.

[13] Gollakota S. et al. They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices. SIGCOMM'11, August 15–19, 2011, Toronto, Ontario, Canada.

[14] Halperin D. et al. Security and privacy for implantable medical devices. IEEE Pervasive Computing, Special Issue on Implantable Electronics, January 2008.

[15] Halperin, D. et al. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses, IEEE Symposium on Security and Privacy, May 2008.

[16] Hansen J.A., Hansen N.M. A Taxonomy of Vulnerabilities in Implantable Medical Devices. SPIMACS'10, October 8, 2010, Chicago, Illinois USA.

[17] Howard M., Lipner S. "The Security Development Lifecycle", Microsoft Press, 2006.

[18] International Standards Organization. Medical devices -- Application of risk management to medical devices. ISO 14971:2007.

[19] Jee E. et al. A safety-assured development approach for real-time software, Proc. IEEE Int. Conf. Embed. Real-time Comput. Syst. Appl., Aug. 2010, pp. 133–142.

[20] Kaplan D. Black Hat: Insulin pumps can be hacked. SC Magazine, August 04, 2011.

[21] King S.T. et al. Designing and implementing malicious hardware. In Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET'08), Fabian Monrose (Ed.). USENIX Association, Berkeley, CA, USA, Article 5.

[22] Kolata G. Of Fact, Fiction and Cheney's Defibrillator. The New York Times, October 27, 2013.

[23] Kramer D.B. et al. (2012) Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. PLoS ONE 7(7): e40200. doi:10.1371/journal.pone.0040200

[24] Li C., Raghunathan A., Jha N.K. Improving the Trustworthiness of Medical Device Software with Formal Verification Methods, IEEE Embedded Systems Letters, Vol. 5, No. 3, pp. 50-53, Sept. 2013.

[25] McGraw G. Software Security, IEEE Security & Privacy, vol. 2, no. 2, pp. 80-83, March-April 2004.

[26] Nixon C. et al. Academic Dual Chamber Pacemaker, University of Minnesota, 2008.

[27] Ross R.S. Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1, September 2012.

[28] Rostami M., Juels A., Koushanfar F. Heart-to-Heart (H2H): Authentication for Implanted Medical Devices, CCS '13, ACM SIGSAC Conference on Computer & Communications Security, pp 1099-1112, ACM New York, 2013.

[29] Sanger D.E., Shanker T. N.S.A. Devises Radio Pathway Into Computers, The New York Times, Jan. 14, 2014.

[30] Skorobogatov S., Woods C. Breakthrough Silicon Scanning Discovers Backdoor in Military Chip, Cryptographic Hardware and Embedded Systems – CHES 2012, Lecture Notes in Computer Science Volume 7428, 2012, pp 23-40.

[31] Sorber J. et al. An amulet for trustworthy wearable mHealth. Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications (HotMobile '12). ACM, New York, NY, USA, Article 7.

[32] Venere E. New firewall to safeguard against medical-device hacking, Purdue University News Service, April 12, 2012.

[33] Vockley M. Safe and Secure? Healthcare in The Cyberworld. AAMI (Advancing Safety in Medical Technology) BI&T – Biomedical Instrumentation & Technology, May/June 2012.

[34] Weaver C. Patients put at risk by computer viruses. The Wall Street Journal, June 13, 2013.

[35] Wei S., Potkonjak M. The Undetectable and Unprovable Hardware Trojan Horse, Design Automation Conference DAC'13, May 29 - June 07 2013, Austin, TX, USA.

[36] Wirth A. Cybercrimes pose growing threat to medical devices. Biomed Instrum Technol. 2011 Jan-Feb;45(1):26-34.

[37] World Health Organization. Medical device regulations: global overview and guiding principles. 2003.