Security Scores for Medical Devices

Johannes Sametinger[1] and Jerzy Rozenblit[2]
[1]*Department of Business Informatics - Software Engineering, Johannes Kepler University Linz, Altenbergerstraße 69, 4040 Linz, Austria*
[2]*Department of Electrical and Computer Engineering, University of Arizona, 1230 E Speedway Blvd, 85718 Tucson AZ, U.S.A.*
johannes.sametinger@jku.at, jr@ece.arizona.edu

Keywords: Security, Security Score, Medical Devices, Sensitivity, Impact, Safety, Vulnerability, Security Risk.

Abstract: Medical devices are indispensable for millions of patients worldwide. They increasingly depend on software and hardware components, and interoperate with other devices wirelessly and through the Internet. The sensitive nature of health records, the increasing interoperability of medical devices, and the fact that human well-being and life are at stake, puts medical device security at the forefront in healthcare technology. In this paper, we contrast medical devices' safety with their security and introduce a stratification of security scores. We need such a grading to increase security awareness in the medical domain and as a guideline for designers and developers who will have to act appropriately to ensure devices' trustworthiness and as a basis for stakeholders' course of action when devices pose risks. We motivate and illustrate the scores by examples.

1 INTRODUCTION

Medical devices have more and more embedded software with communication mechanisms that now qualify them as information systems. Security is about protecting information and information systems from unauthorized access and use. Confidentiality, integrity, and availability of information are core design and operational goals. Software security is "the idea of engineering software so that it continues to function correctly under malicious attack" (McGraw, 2004). In this sense, medical device security is quite similar. Its goal is to engineer such devices so that they ideally would be immune to malware implantation or if a breach occurred, they would continue to function correctly. Medical devices comprise a broad range of instruments and utensils. In this paper, we discuss only devices with hardware, software, and some form of interoperability. For example, most artificial joints are not "powered" by software (yet). Thus, we can ignore them from a security perspective. However, they are indeed critical from a safety point of view. Researchers have demonstrated successful hacking of medical devices on several occasions. For example, Jay Radcliffe was able to send commands to his insulin pump (raise or lower insulin levels) and to disable it wirelessly within a distance of up to 150 feet (Kaplan, 2011). Chunxiao et al., (2012) have shown security attacks and defenses for a diabetes therapy system. FDA's safety division has issued a warning to device makers and healthcare providers to put safeguards in place to prevent cyber-attacks (FDA, 2013). We do not know about any deaths or injuries yet, but hypothetical ramifications, e.g., ransomware on medical devices, are obvious. The 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 Windows file as a virus, hospitals had to postpone elective surgeries and stop treating non-critical patients in emergency rooms (Fox, 2010). The fact that there are still many medical devices based on an old version of the Windows operating system is another problem (Fu and Blum, 2013).

People increasingly manage their health and wellness with mobile medical applications (FDA, 2015). Such apps may promote healthy living and provide access to useful health information. Mobile apps can extend medical devices by connecting to them for the purpose of displaying, storing, analyzing, or transmitting patient-specific data (FDA, 2013b). 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, we have to take security precautions. Mobile and cloud frontiers pose new

challenges, where designers and developers of healthcare IT must address pre-existing security vulnerabilities and undiagnosed future threats (Kotz et al., 2011).

Over the last years, wearable devices have become popular. With sensors attached to the body, they detect and monitor changes in body signatures of various areas. Athletes, people aware of personal fitness, but also patients use wearable devices. For our discussion, it is not relevant whether a medical device is wearable. Many consumer-acquired wearable devices like fitness trackers or heart rate monitors do not qualify as medical devices. They cannot have a direct negative effect on their wearers, but they may contain sensitive information. Therefore, they are not completely out of our scope even though we concentrate on medical devices. We propose security scores for medical devices in order to increase security awareness and, thus, to motivate stakeholders to plan countermeasures accordingly. Someone's security awareness is her knowledge and attitude regarding the protection of a device's information system. In the context of medical devices, it is important that all stakeholders, not just device manufacturers, display this knowledge and attitude and, most of all, work together to explicitly know a device's security status and improve it when needed.

In Section 2, we briefly introduce medical devices and contrast safety to security. In Section 3, we discuss levels of concern comprising sensitivity, impact and exposure of medical devices. Vulnerabilities and the suggested security scores follow in Section 4. In Section 5, we give a discussion of the proposed scores. A conclusion follows in Section 6.

2 MEDICAL DEVICES

Medical devices include everything from simple wooden tongue depressors to highly sophisticated computerized medical equipment (World Health Organization, 2003). According to the 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 a disease or other conditions (World Health Organization, 2003). The FDA uses a similar definition (FDA, 2014). Classes of medical devices are different in various countries. In the US, FDA's Center for Devices and Radiological Health is responsible for regulating firms, which manufacture, repackage, relabel, or import medical devices. The FDA has established classifications for about 1,700 different generic types of devices. They further group them into medical specialties, called panels. Examples for FDA's specialty panels include cardiovascular, dental, and orthopedic devices (FDA, 2014).

A more general classification divides medical devices into everyday use, diagnostic, therapeutic, and life-supporting equipment (Smith, 2012). Doctors and nurses use such equipment daily during routine medical procedures. Examples include needles, latex gloves, syringes and stethoscopes. The main purpose of diagnostic equipment is to help doctors detect and diagnose diseases. Examples include ultrasound machines, positron emission tomography (PET) scanners, computer tomography (CT) scanners, and magnetic resonance imagery (MRI) machines. Therapeutic equipment helps patients to recover and improve their health after surgeries and other medical treatments. Examples are devices such as infusion pumps and medical lasers. Life-support equipment is helpful in cases of physiological organ failure or major trauma. Examples include heart-lung machines, medical ventilators, and dialysis machines.

What makes medical devices stand out is not just the fact that they may potentially threaten life. We also need to secure our IT infrastructure. This infrastructure comprises not only physical devices but also personnel, security companies, emergency response teams, etc. We typically rely upon these entities, should IT-related problems occur. Patients and healthcare providers are not IT experts and are very much at the mercy of the devices' manufacturers who only now are beginning to take security seriously. The goal of our suggested security scores is to fill this gap and to make devices' security states better accessible, visible, and understandable to all stakeholders.

2.1 Device Safety

The FDA has assigned generic device types to the regulatory classes I, II or III, which are based on the level of control that is necessary to assure the safety and effectiveness of a device. The higher a device's risk, the higher its class (FDA, 2014). Class I includes devices with the lowest risk, class III those with the highest risk. Class III devices need a pre-market approval process. Examples include implanted devices and devices that may be necessary to sustain life like artificial hearts or automated external defibrillators.

2.2 Device Security

Whether a medical device is active or passive is important in many respects. Passive devices do nothing by themselves, e.g., a stethoscope or a simple artifi-

cial joint. Active devices may or may not involve software, hardware, and interfaces, which are crucial when considering security issues. These devices can do some processing, receive inputs outside of the device (sensors), output values to the outer world (actuators), and communicate with other devices. Medical devices are security-critical if they do some form of processing and communicating, typically by running software on specialized hardware, and often, by employing a range of sensors (Sametinger et al., 2015). The devices do not need to be re-configurable in order to be security-relevant. All medical devices as defined by the WHO or by the FDA have aspects that are inherently safety related. 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. There are, however, security-relevant instruments and appliances that the WHO or the FDA do not consider medical. Examples include smartphones that run fitness apps handling sensitive information, or regular PCs in a hospital for processing medical records.

Paul et al., have proposed a security-based classification of medical devices where the primary factor is how patients use the device (Paul et al., 2011). Class I includes devices that are completely external to the body. Examples include smartphones and personal computers. Naturally, devices in class I are also a part of the medical enterprise. Class II contains devices that are implanted but external to the body. Examples include infusion pumps. Finally, class III contains devices that are completely implanted and are not physically, externally accessible. Examples are pacemakers and internal cardiac defibrillators.

2.3 Interoperability

According to a study by the West Health Institute, device interoperability with electronic medical records (EHRs) could save the U.S. healthcare industry $30B annually (Versel, 2013). In fact, medical devices are increasingly communicating health information, e.g., insulin pumps or pacemakers may transmit logs directly to physicians or hospitals, or receive modified settings and commands (Kramer et al., 2012). Storing and transmitting patients' medical information requires state-of-the-art technology. Networked mobile devices enable individuals and their physicians or hospital personnel to better monitor and manage their medical conditions (Kotz, 2011). If device communication is wireless or over the Internet, then transmitted information is at risk of exposure. We can wirelessly connect devices with mobile medical applications to wearable, portable, and even embeddable sensors (Kotz, 2011). They enable effortless continuous medical monitoring. Examples of monitored values are glucose levels in diabetic patients or the weight of individuals seeking to lose it. In such settings, people involved need subtle control over the collection, recording, dissemination, and access to monitored data. When patients use new sensing devices, they add a new dimension to the confidentiality challenge. In the near future, it is likely that we will witness the proliferation of tiny sensors that detect a widening range of compounds and report it to our mobile devices like smartphones. We may then transmit the collected values to healthcare institutions or to public clouds, enabling the powerful and cost-effective screening, diagnosing, monitoring, and tracking of people's health. Sensors and microelectronics integrated into the sole of running shoes are one recent example. They measure the biomechanical data of the runner and evaluate her form with real-time measurements, which they then transmit to a smartphone and to an external server for further evaluation. Google's proposed smart contact lenses to monitor diabetics provide another example with a hint of how the future might look like. Increased use of sensors may one day allow us to monitor medical conditions and help develop individualized treatments. Clearly, the increased interoperability of devices leads to increased security risks and, hence, requires increased security measures in order to protect these devices from attacks.

3 LEVELS OF CONCERN

The FDA has introduced the level of concern for medical devices. It is a measure referring "to an estimate of the severity of injury that a device could permit or inflict, either directly or indirectly, on a patient or operator as a result of device failures, design flaws, or simply by virtue of employing the device for its intended use" (FDA, 2005). The FDA's severity of injury distinguishes death, minor and serious injury. We will consider device failures or design flaws in Section 4. In addition to the impact of a device, we suggest to also consider the fact whether devices store and process sensitive information and how much a device is exposed to its environment.

Thus, we propose a level of concern for medical devices based on whether they process or communicate sensitive information, whether they process or communicate safety-critical information, and how exposed they are to their environment. To keep things

simple, we have chosen to use four levels for all categories, i.e., low, moderate, high, and very high.

3.1 Sensitivity

In a medical context, sensitive information includes anything about a patient, e.g., medical records, and 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. We introduce a medical device's sensitivity to indicate the amount of sensitive information on that device. There are several approaches to define sensitive information in the health domain, e.g., HIV test results, information from reproductive health clinics, and information about celebrities' medical issues. At this point, we emphasize that we typically do not categorize information as slightly or highly sensitive. Either it is sensitive or it is not. We propose a pragmatic approach for scoring the sensitivity and use an estimate of the amount of sensitive information on a device, and an estimate of how easily we can attribute this information to a specific patient. Thus, we categorize the information to be slightly sensitive, sensitive, or highly sensitive. Table 1 summarizes our suggested sensitivity levels. We will later use the numbers in parentheses for calculations. We make the distinction between high and very high based on the fact whether sensitive information is stored of a single person or of multiple persons. We refrain from using a finer granularity for the sake of simplicity.

3.2 Impact

Medical devices differ in the degree of impact that they can have on a patient. Typically, devices with a high benefit (utility) also pose a high potential harm. For example, a cardiac pacemaker can save the life of patients, but it can also threaten the life of a patient if it malfunctions. A pacemaker has a direct impact on the patient as it can directly influence the heart rate. Other devices can have indirect impact. Determining the indirect impact of a device is much more difficult than determining its direct impact. For example, a blood glucose meter has no direct impact, but the values it provides indirectly influence the insulin dose a patient delivers to herself. This dose influences the patient's health. If a BGM displays wrong values, then it may influence the amount of insulin its user will deliver. In a worst-case scenario, this may even result in the death of that person.

We introduce a device's impact to indicate the influence a device has on a patient, i.e., the potential benefit and the potential harm a device can do to a patient, be it directly or indirectly. Table 2 summarizes medical devices' impact. Again, the coarse granularity may sometimes prohibit an easy assignment to one of the values. For example, well-being may affect health and the other way round. Generally, we can say that the higher the level, the higher the impact. When one device has a higher impact than another device, then we assign the former to a higher level than the latter, even though both may influence well-being or health.

Table 1: Sensitivity of medical devices.

Sensitivity	Description	Examples
Low (0)	No sensitive information on device	Dental laser
Moderate (1)	Moderately sensitive information (sensor values, no personal info)	Insulin pump storing glucose levels, Blood glucose meter
High (2)	Sensitive information	PC storing individual health records
Very High (3)	Highly sensitive information (personal information, health information)	Server storing many health records

3.3 Exposure

Modern devices tend to increase interoperability. Interoperability refers to the mode in which devices work with one another. Medical devices can operate as stand-alone (low exposure) or they can interoperate with other devices and even connect to the Internet (high exposure). High exposure offers a big attack surface for potential intrusions. However, it also provides flexibility and benefits. For example, a cardiologist may save a patient's life by remotely controlling her pacemaker in a medical emergency. An information security exposure is "a system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network" (MITRE).

Table 2: Impact of medical devices.

Impact	Description	Examples
Low (0)	No impact	Administrative PC in hospital Heart rate watch
Moderate (1)	Impact on well-being	Drug dispensing device, Dental laser
High (2)	Impact on health	Blood glucose meter
Very High (3)	Impact on life	Pacemaker, X-ray, Insulin pump, Heart-lung machine

A system's attack surface is the set of ways in which an adversary can enter the system and potentially cause damage (Manadhata, 2008). Every feature of a system adds a certain amount of risk. A large attack surface provides potential for intrusions. Nevertheless, it also provides flexibility and benefits.

Table 3 summarizes medical devices' exposure levels. Devices connected to the Internet may have an IP address, but they may also be accessible through an intermediate device that connects to the Internet and allows access to the medical device in some form. Please note that this level is independent from any security measures that we may have taken to protect the device. If a medical device has a high exposure, then it is possible to control its impact and to access sensitive information externally. This can be done by authorized parties, e.g., medical doctors in charge, or, if the device is not properly secured, by malicious attackers. Needless to say that we need safeguards too to prevent voluntary or involuntary harm by authorized parties.

Table 3: Exposure of medical devices.

Exposure	Description	Examples
Low (0)	Stand-alone device without communication features	Dental laser, Bone growth stimulator
Moderate (1)	Device with near-field communication	Pacemaker
High (2)	Device with "plug-and-play" interoperability or distant wireless communication	Tablets used by physicians
Very High (3)	Device with Internet connection	Server with health records

3.4 Privacy and Safety Concerns

When we combine exposure with sensitivity, then we obtain the degree of exposure of sensitive information. If a highly exposed device stores highly sensitive information, then the exposure of the sensitive information is high. We introduce a simple formula to calculate numerical values. By multiplying sensitivity or impact with exposure, we get values between zero and nine. The result is zero when either sensitivity or exposure is zero, i.e., there neither is sensitive information on the device nor does it interoperate with other devices. Multiplying the values 0...3 by 0...3 yields values in the range 0,1,2,3,4,6,9. The resulting values can be classified as low (0, 1), moderate (2, 3), high (4, 6) and very high (9).

From a privacy perspective, we do not have to be concerned about devices that do not store or process sensitive information. In addition, there is no need to be worried if the device is not exposed. From a safety perspective, we do not have to be concerned about devices without an impact on patients. Again, no need to worry if there is no exposure of the device. From a security perspective, devices not exposed to their environment are not an issue. At this point, we refrain from considering situations where malware may infect devices during the manufacturing process (Sametinger et al., 2015). Privacy is at stake if there is sensitive information and we can access it from outside the device. Safety is at stake if there is an impact on patients and we can control this impact from outside the device.

3.5 Examples

We discuss a blood glucose meter (BGM), a cardiac pacemaker (CPM), an ultrasound imaging device (USI), a magnetic resonance imagery machine (MRI), and a diabetes logbook app (DLA) as illustrative examples. A stand-alone blood glucose meter allows its user to read blood glucose values from the device's display. The device does not have any information about the patient who uses it but may store several historic values. An implanted cardiac pacemaker enables a cardiologist to program it via wireless communication. The device stores some basic information about its wearer. An ultrasound-imaging device provides a LAN connection to store patients' images in an in-house database. The same is true for the magnetic resonance imagery machine. The diabetes logbook app runs on a smartphone and allows its user to log information about meals, blood glucose values (from the BGM) as well as insulin levels and dosages. If the app is a registered (class 1) medical device, patients' doctors can use generated reports to make medical decisions. The app stores backup data on the manufacturer's cloud infrastructure.

Table 4 shows all the levels of concern we have defined for these devices. We can see at a glance where we need security countermeasures. Please note that the devices we have chosen as examples exist in many different forms from various vendors. These devices will vary in the levels of concern also. A device can store more or less sensitive information and interoperate with its environment to a greater or lesser extent. Therefore, it is important to define the levels of concern for specific devices of a specific manufacturer, rather than for a group of devices. We have chosen the numbers in Table 4 to represent a specific device category. It is interesting to see that the blood glucose meter does not need any security precautions even though there is an indirect impact on patients. Missing

exposure makes it impossible for attackers to manipulate the device. We have rated the impact of the diabetes logbook app higher than the impact of the blood glucose meter, because the logbook may contain a much longer history of values that, if manipulated, may have more serious consequences if used for therapeutic decisions. We have specified different sensitivity and impact levels for the two imaging devices USI and MRI, simply to demonstrate different level combinations. Not surprisingly, Table 4 shows that our MRI needs more security precautions than our BGM.

Table 4: Levels of concern for sample medical devices.

Device	Sn	Im	Ex	PLC	SLC
BGM	0	1	0	0	0
CPM	1	3	1	1	3
USI	1	1	3	3	3
MRI	3	2	3	9	6
DLA	3	2	3	9	6

Sn … Sensitivity, Im … Impact, Ex … Exposure
PLC … Privacy level of concern, SLC … Safety level of concern

BGM … Blood glucose meter, CPM … Cardiac pacemaker
USI … Ultrasound imaging device, MRI … Magnetic resonance imagery
DLA … Diabetes logbook app

4 SECURITY SCORES

Regardless of a device's level of concern, i.e., its sensitivity, impact, and exposure, it can be secure or insecure depending on whether there are vulnerabilities and on whether somebody knows these. "100% secure" devices are as unlikely as zero-fault software. We will have to find a way to manage insecure devices. Devices with high exposure of sensitive information pose a higher privacy risk, but if we have taken proper security countermeasures, then the privacy threat may still be low. The same holds for devices with a high exposure of impact and a higher safety risk. Whether a device is actually at risk depends on whether there are security vulnerabilities and potential exploits. Thus, we have to define the current vulnerability level and then calculate the privacy and safety scores depending on a device's sensitivity and impact, respectively.

4.1 Vulnerability

We have stated in the introduction that secure devices have to continue to function correctly even if under a malicious attack. Vulnerabilities are errors in devices, typically in software, which we can directly use to gain unauthorized access to the device. They pose a threat to the device itself, to the information it contains, to other devices it communicates with, and to its environment. Today, most stakeholders are concerned about the safety of medical devices. They pay less attention to the devices' vulnerabilities. These can be quite volatile. When we detect vulnerabilities, our rating of the device's threat may increase rapidly. It is important for everyone involved to have a clear picture of the current security status and to make reasoned decisions about necessary steps in order to decrease the threat, if needed. We propose vulnerability levels as described in Table 5.

At this point, we clearly have to distinguish between two different perspectives, i.e., the attacker's and the risk analyst's perspective. If a potential attacker detects vulnerabilities, then the actual threat, but not necessarily the analyst's assessment of it, will increase. Thus, a device's vulnerability level represents a person's knowledge about this device's vulnerabilities. Not knowing any vulnerability does not necessarily mean that none exists. A device's vulnerability provides a dynamic property, as found vulnerabilities and exploits increase the risk, and later patches and updates reduce the risk.

Table 5: Vulnerability of medical devices.

Security	Description	Examples
Low (0)	Neither vulnerabilities nor malware on device	New device Device with upgraded software version
Moderate (1)	Vulnerabilities on device, no exploits yet	Weakness in protocol Potential buffer overflow
High (2)	Vulnerabilities on device with known exploits	Protocol weakness or buffer overflow can be used for unauthorized access
Very High (3)	Malware on device	Hardware Trojan or software backdoor on device

Both software and hardware take time to mature. Therefore, a five year old product may potentially be safer than a new product out in the market. However, we argue that it is reasonable to assume that a new device or software upgrade is low on the vulnerability scale, cf. Table 5. At that time, vulnerabilities are not yet known and, for software upgrades, known vulnerabilities have usually been fixed.

4.2 Privacy and Safety Scores

A medical device is at risk when it is vulnerable and stores sensitive information. It also poses a risk when it is vulnerable and it has an impact on a patient. Privacy concerns exist when personally identifiable in-

formation or other sensitive information is processed or stored. Insufficient access control or inappropriate sharing are often the cause of privacy issues. Privacy is about the ability to conceal information about a patient. Disclosure of sensitive information may result in negative consequences. For example, an employer may not be willing to employ people with HIV. Sensitive information may also constitute a threat, because wrong values may later induce therapeutically wrong decisions by doctors or devices. We calculate privacy and safety scores again by using multiplication. Sensitivity multiplied by the vulnerability yields the privacy score; impact multiplied by vulnerability yields the safety score.

The levels of concern provide general information about how important security precautions are for a device. Vulnerability levels and security scores, i.e., privacy and safety score, indicate a device's current security status. The higher it is, the more we have to expect security breaches.

4.3 Examples

In Table 6, we present different vulnerability levels for the devices introduced in the previous section. If we assume that there are no known vulnerabilities, then we set the appropriate level to zero. This is the case, for example, when a new device comes to market. There is no risk yet at that time. Later, when we know about vulnerabilities, risk increases. In Table 6, we show devices as defined above with various vulnerability levels and the resulting privacy and safety scores. A quick glance at the table reveals that privacy and safety are at risk in the logbook app, and that the cardiac pacemaker's safety is at risk. We will discuss consequences from that information below. Please note that we use values for sample devices in Table 6. These devices may have different values than specified in our table. The values depend on the specific implementation and equipment by the manufacturers.

Table 6: Privacy and safety scores for sample devices.

Device	Sn	Im	Vu	Priv	Saf
BGM	0	1	3	0	3
CPM	1	3	2	2	6
USI	1	1	1	1	1
MRI	3	2	0	0	0
DLA	3	2	3	9	6

Sn … Sensitivity, Im … Impact, Vu … Vulnerability
Priv … Privacy Score, Saf … Safety Score

BGM … Blood glucose meter, CPM … Cardiac pacemaker
USI … Ultrasound imaging device, MRI … Magnetic resonance imagery
DLA … Diabetes logbook app

We have to mention at this point that knowledge about the existence or non-existence of vulnerabilities may differ among different persons. It is always possible that only malicious attackers are aware of vulnerabilities. In this case, we may assume a low score even though the danger of an attack is indeed high. The malicious attackers who know about the vulnerability are able to determine the appropriate score.

5 DISCUSSION

We imagine having levels of concern as well as privacy and safety scores defined for any medical device. Levels of concern include sensitivity, impact, and exposure. Manufacturer can define them for the approval process. The vulnerability level as well as privacy and safety scores of a device are dynamic properties; we have to maintain them in order to describe the current risk associated with using a device. It should be mandatory that they be maintained and publicly available. Thus, doctors and patients would be able to check out both the levels of concern and security scores of a specific device. As manufacturers may be hesitant to admit increased vulnerability, we imagine a neutral third-party organization to be in charge, e.g., the MITRE Corporation that operates CVE, a dictionary of publicly known information security vulnerabilities and exposures. We may deduct a device's vulnerability level from the number and severity of its CVEs.

Risk management includes risk framing, risk assessment, risk response and risk monitoring (Ross, 2011). Our suggested security scores contribute to the assessment and to the monitoring of risks of medical devices. The number of entry points that an attacker may use to access the device defines the attack surface. The exposure we have suggested does not differentiate between devices with big or small attack surfaces. Minimizing the attack surface can reduce the risk of attacks, but it does not change the general exposure of a device. Proper authentication and authorization also makes a huge difference in securing a device. If a device's manufacturer has chosen to implement adequate security measures like authentication or encryption, then the level of concern will be unchanged. However, these measures will affect privacy and safety scores, because proper security mechanisms will have an effect on the emergence of vulnerabilities.

We definitely need mandatory security analyses for devices that may threaten human life. Our proposed scores and levels of concern provide a black-box view to medical devices. If manufacturers ana-

lyze security properly, it will later have a positive effect on the number of vulnerabilities that we will get to know. We will see positive effects in low values for our privacy and safety scores. Threat analysis is another activity that we need to evaluate security risks posed to a device. Such analysis is important in order to plan for countermeasures. A device manufacturer should include such activities into the development of the devices. The results will not be publicly available, as it would provide valuable information to attackers. We do not use such information to characterize medical devices, but they will have a positive effect to their security scores.

We have presented a numerical system that still represents work in progress. As a next step, we plan to perform a proof of concept. The fundamental principle of design science research is that we acquire knowledge of a design problem and its solution in the creation and application of design artifacts (Hevner, 2007). The research outcome not only includes the design artifact itself but also a clearly defined contribution to scientific knowledge. Another next step is to define rules of action, such that stakeholders have defined process models as guidance for further action. Further action can be manifold and depends on the device. For example, if we have a safety score of nine in a pacemaker, then one option is to remove the pacemaker from the patient and replace it with another model. A less expensive and less time-consuming alternative is to provide future medical devices with an option to cut off communication features. Whatever the response to an increased risk of a device might be, we should have predefined courses of action in order to act quickly. The security scores described in this paper are a first step in this direction.

6 CONCLUSIONS

Medical devices increasingly use wireless communication and Internet connections. Additionally, we see an increased use of mobile medical applications in connection with a plethora of medical sensors still to come. We have introduced security scores in an effort to increase the security awareness of all involved parties and to provide a knowledge base that makes it possible to make sound decisions in different security situations. Sensitivity, impact, and exposure are static properties of devices. They reflect whether a device handles sensitive or safety-critical information and how exposed it is to its environment. Vulnerability and risk are dynamic. If they increase, we have to take appropriate countermeasures, or the doors will stand wide open for the misuse of sensitive medical data and for malware and attacks that put human life in danger.

We have not provided any information on how to implement effective defense mechanisms. It is the manufacturer's task to pay due attention to the development of secure devices. Our suggested scores can provide information about how concerned we have to be in general about security precautions of specific devices and about security and safety risks at specific points of time. The consequences may be manifold. Manufacturers may fix problems or patients and hospitals may decide to refrain from using these devices.

REFERENCES

Chunxiao, L., Raghunathan, A., Jha, N. K., 2011. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. *13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom)*, pp 150-156. https://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6026732

FDA, 2005. Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 11, 2005. http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089543.htm

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

FDA, 2013b. Mobile Medical Applications – Guidance for Industry and Food and Drug Administration Staff. Sept. 2013. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf

FDA, 2014. Medical Devices – Classify Your Medical Device. http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/default.htm

FDA, 2015. Mobile Medical Applications – Guidance for Industry and Food and Drug Administration Staff, Feb. 09. http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf.

Fox News, 2010. Antivirus Program Goes Berserk, Freezes PCs. April 22. http://www.foxnews.com/tech/2010/04/22/antivirus-program-goes-berserk-freezes-pcs/

Hevner, A. R., 2007. A Three Cycle View of Design Science Research, *Scandinavian Journal of Information Systems*, Vol. 19: Issue 2, Article 4. http://aisel.aisnet.org/sjis/vol19/iss2/4

Fu K. and Blum J., 2013. Controlling for cybersecurity risks of medical device software, *Communications of the ACM*, vol. 56, no. 10, p. 35.

Kaplan D., 2011. Black Hat: Insulin pumps can be hacked. *SC Magazine*, August 04. http://www.scmagazine.com/black-hat-insulin-pumps-can-be-hacked/article/209106

Kotz, D., Fu, K., Gunter, C., and Rubin, A., 2015. Security for mobile and cloud frontiers in healthcare, *Communications of the ACM*, vol. 58, no. 8, pp. 21–23.

Kramer, D. B., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K., Reynolds, M. R., 2012. Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. http://www.plosone.org/article/info:doi/10.1371/journal.pone.0040200

McGraw, G., 2004. Software Security, *IEEE Security & Privacy*, vol. 2, no. 2, pp. 80-83, March-April. doi:10.1109/MSECP.2004.1281254

Kotz, D., 2011. A threat taxonomy for mHealth privacy, *Workshop on Networked Healthcare Technology (NetHealth)*, January. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5716518

Paul, N., Kohno, T., Klonoff, D. C., 2011. A Review of the Security of Insulin Pump Infusion Systems, *Journal of Diabetes Science and Technology*, vol. 5, Issue 6. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3262727

Manadhata, P., 2008. An Attack Surface Metric, *CMU-CS-08-152*. http://reports-archive.adm.cs.cmu.edu/anon/2008/CMU-CS-08-152.pdf

MITRE. The MITRE Corporation: Common Vulnerabilities and Exposures – The Standard for Information Security Vulnerability Names. https://cve.mitre.org

Ross, R. S., 2012. Guide for Conducting Risk Assessments, *NIST Special Publication 800-30 Revision 1*. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Sametinger, J., Rozenblit, J., Lysecky, R., and Ott, P., 2015. Security Challenges for Medical Devices, *Communications of the ACM*, vol. 58, no. 4, pp. 74–82.

Smith, E., 2012. Types of Medical Equipment. *HIVE Health Media*. January 22. http://www.hivehealthmedia.com/types-medical-equipment/

Versel, N., 2013. West: Device interoperability with EHRs could save $30B annually. *Mobihealthnews*. http://mobihealthnews.com/21120/west-device-interoperability-with-ehrs-could-save-30b-annually/

World Health Organization, 2003. Medical device regulations: global overview and guiding principles, ISBN 92-4-154618-2. http://whqlibdoc.who.int/publications/2003/9241546182.pdf