Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Devices

Tamara Denning[†], Alan Borning[†], Batya Friedman[‡], Brian T. Gill[*], Tadayoshi Kohno[†], and William H. Maisel[+]

[†] Department of Computer Science & Engineering and [‡] The Information School
University of Washington
[*] Department of Mathematics, Seattle Pacific University
[+] Medical Device Safety Institute, Beth Israel Deaconess Medical Center
Harvard Medical School

ABSTRACT

Implantable medical devices (IMDs) improve patients' quality of life and help sustain their lives. In this study, we explore patient views and values regarding their devices to inform the design of computer security for wireless IMDs. We interviewed 13 individuals with implanted cardiac devices. Key questions concerned the evaluation of 8 mockups of IMD security systems. Our results suggest that some systems that are technically viable are nonetheless undesirable to patients. Patients called out a number of values that affected their attitudes towards the systems, including perceived security, safety, freedom from unwanted cultural and historical associations, and self-image. In our analysis, we extend the Value Sensitive Design value dams and flows technique in order to suggest multiple, complementary systems; in our discussion, we highlight some of the usability, regulatory, and economic complexities that arise from offering multiple options. We conclude by offering design guidelines for future security systems for IMDs.

Author Keywords

Defibrillators, embodied technologies, implantable medical devices, medical device security, pacemakers, safety, security, value dams and flows, Value Sensitive Design.

ACM Classification Keywords

J.3 Life and Medical Sciences: Health

General Terms

Design, Human Factors, Security.

INTRODUCTION

Implantable medical devices (IMDs), such as pacemakers and implantable cardioverter-defibrillators (ICDs), are electronic devices designed to treat abnormal physiological conditions within the body. A 2001 report estimated that over 25 million US citizens depend upon IMDs for life-critical functions [13]. Some current-generation devices now have the ability to communicate wirelessly with external equipment from distances up to 5 meters away. There are numerous reasons for making IMDs wireless. For example, wireless IMDs can be configured ("programmed") by doctors in the operating room from farther away, which avoids the need to bring programming equipment into the sterile operating area. Wireless technology also allows the IMD to send alerts to a home monitoring station—which can then send a report to the patient's physician for analysis—without causing interruption to the patient's activities.

Despite these clear advantages, a new class of risks has recently come to light. In 2008, researchers—including some of the authors—showed that one model of (short-range) wireless ICD currently in use is vulnerable to unauthorized tampering [12]. The authors showed that someone using low-cost, home-made equipment could wirelessly communicate with the ICD to modify settings on the ICD, cause the device to issue a large shock, or learn private information about the patient.

Despite the vulnerabilities identified, the authors were careful to note that the risks to patients today are low; for example, the ICD model they studied, which was introduced into the US market in 2003, is only capable of short-range wireless communication. Nevertheless, they also warned that—unless suitable defenses are developed soon—the risks to patients with medium- or long-range wireless devices could be much greater in the future. Past examples give evidence that some people are willing to use technology to cause physical harm to patients. In November 2007 and again in March 2008 hackers compromised epilepsy support websites by posting animated images on these websites that caused photosensitive epilepsy patients to experience pain and seizures [8, 21].

Motivated by this situation, the computer security research community has begun to develop new technical security

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
CHI 2010, April 10 – 15, 2010, Atlanta, Georgia, USA
Copyright 2010 ACM 978-1-60558-929-9/10/04...$10.00.

mechanisms for warding off the potential security risks to future wireless IMDs [6, 12, 22]. Developing strong technical security defenses is, however, only part of the solution. There is a fundamental gap between developing technical mechanisms that *could* protect the security of future wireless medical devices if deployed and developing security defenses that *will* be accepted (even welcomed) by patients, doctors, and other stakeholders. We seek to bridge this gap between technical systems and effective deployments by initiating an analysis of how potential security systems for IMDs interact with one of the most critical stakeholder groups: the patients themselves.

We used the Value Sensitive Design (VSD) framework [9] and semi-structured interviews to explore the values and experiences of patients with implanted cardiac devices and solicit their feedback on a range of security approaches. We developed our interview based on a conceptual investigation of the problem space and informed by our experience as security researchers, as HCI researchers and social scientists, and as a cardiologist. In the course of the interview, we present participants with 8 different security systems that embody different approaches to security for IMDs: passwords, body modifications, behavior changes, and patient-passive. Not all of these systems are well-developed or even desirable as solutions for IMD security; instead, we solicited feedback on them in order to investigate the ways in which participants' values and priorities interact with the security systems' properties. We conclude with 11 criteria that we advise researchers and designers to satisfy in order to make their security systems more acceptable to patients with IMDs. By studying how patients' views and values interact with security systems for wireless implantable medical devices, this paper can serve as a foundation for informing the design of future IMD systems that not only have desirable technical security properties, but that also address the values and needs of patients. Looking beyond IMDs, this paper also provides contributions to Value Sensitive Design and HCI by studying patient perceptions about embodied (implanted) devices and their security.

IMPLANTABLE MEDICAL DEVICES AND SECURITY

Implantable Cardiac Devices

Current electronic implantable medical devices (IMDs) prevent or treat conditions ranging from heart failure to diabetes to Parkinson's Disease. This study focuses on patients with implanted cardiac devices—pacemakers and implantable cardioverter-defibrillators (ICDs). Pacemakers in some patients might improve their lives, while in others might be life-sustaining. Patients with ICDs depend upon their devices to treat potentially fatal heart rhythms.

Implantable cardiac devices store information such as the patient's name and records of irregular heart rhythms that occurred since the last checkup. Patients visit cardiology clinics periodically so that medical staff can download information about these episodes and adjust settings on the patient's device. Newer models incorporate medium-range (2–5 meters) wireless capabilities to add convenience and in-home monitoring to the device's functioning.

Security for Implantable Cardiac Devices

There are numerous important properties for IMDs. The three most relevant to our study are:

- **Authorized clinical access.** The patient's cardiologist and the cardiologist's staff should always be able to change settings on the patient's IMD when the patient is in the clinic.
- **Emergency access.** Medical staff and staff at *other* hospitals should be able to change settings on the patient's IMD if the patient is taken to that hospital in an emergency situation. For example, if the patient requires an emergency operation and has an ICD, the ICD must be deactivated before the operation in order to prevent unintentional shocks to the patient.
- **Security.** No unauthorized person should be able to change settings or view information on the patient's IMD.

All security systems for wireless IMDs should satisfy these requirements to some degree in order to ensure the patient's safety and security; but as noted above, this is not the case for all systems in current use. However, protection against individuals with prolonged physical control over the patient is not a necessary goal for most of these systems, since there are other ways to harm a person in those circumstances and patients are likely to notice prolonged physical contact.

Technical Approaches

It is not obvious how best to provide security for IMDs. In particular, it is inappropriate to apply security measures indiscriminately: while it is important to secure devices against unauthorized access, it can be equally or more dangerous to a patient if a strong security policy prevents medical staff from accessing the patient's IMD in an emergency. The following (non-orthogonal) security approaches have emerged as potential strategies for addressing the value tensions between *security* for IMDs and *safety* for the patient in an emergency.

Passwords. The use of passwords and passphrases to protect access to information systems is a long-standing tradition in the security community. Therefore, it is very natural to investigate the potential use of passphrases for IMD security. Unfortunately, it is unclear how to convey passphrases to emergency medical staff in a timely and reliable manner. For example, if patients carry the passphrases for their IMDs on cards in their wallets, their wallets may be forgotten, lost, stolen, or destroyed in an emergency situation; a missing wallet would prevent medical staff from accessing the patient's IMD, which is potentially serious for patients.

Additional patient body modifications. When the authors discussed the problem of carrying passphrases with members of the computer security community, multiple individuals suggested that tattooed passwords would be a way to circumvent the problem. This suggestion brings up another potential category of security solutions: system designs that require a patient to make additional body modifications (aside from the patient's implanted IMD).

Patient behavior changes. In this security approach, patients are asked to make some modification to their behavior. A canonical example of this approach is asking users to carry an access card. The Cloaker, discussed later in this paper, is a security system that requires patients to wear an external, computational wristband [6].

Passive with respect to the patient. This security approach represents technologies and system designs that do not require patients to wear anything, do anything, or make any additional changes to their bodies. A canonical example of this approach in traditional security is biometrics (e.g., face recognition). In the domain of IMD security, researchers have investigated the viability of a proximity-based access system for IMDs [3, 22].

HUMAN-COMPUTER INTERACTION

Security and Privacy

There has been extensive work in the HCI community on both security and privacy issues. The collection edited by Cranor and Garfinkle [4] includes many of the classic papers on security and usability. Regarding privacy, some of this work has focused on understanding and reasoning about privacy e.g., [1, 2, 15, 25]. For example, some research draws ideas from social psychology to frame a view of privacy as a dynamic regulation of information boundaries [20]. A related body of work is more focused on implementations and concrete models of privacy systems e.g., [14, 16, 17, 19], including a toolkit to aid developers in creating privacy-respecting ubiquitous computing applications [14]. Privacy work in the healthcare area includes [5, 23, 24], although these references concern balancing privacy and utility for hospital employees rather than patients.

Our work differs from these others in several ways. IMDs have unique properties because of their embodied nature: they are a technology that is inseparably incorporated into the user's body, and are in most cases necessary for the user's physical well-being. Unlike cell phones or media spaces, users cannot walk away from their implanted devices, and designers of the security systems cannot assume that users will be conscious to interact with the system. There is limited prior work addressing IMD security technology, and we believe that IMDs have new and unique interactions with their users, which have not yet been thoroughly studied. To the best of our knowledge, ours is the first study that investigates the human implications of security systems for implanted devices.

Value Sensitive Design

Given a range of technical security approaches, it can sometimes be unclear which to pursue. This challenge arises because security is often in tension with other important but different values, such as autonomy, dignity, and self-image. To meet this challenge, we drew on Value Sensitive Design (VSD) [9] to investigate the values and priorities of cardiac patients in relation to IMD security. Key aspects entailed:

Value tensions. Prior work in Value Sensitive Design and related areas [18] alerted us to the need to identify and engage value tensions. As highlighted earlier, in an emergency situation, security for the IMD can be in tension with safety for the patient. We anticipated that security systems involving body modification or behavior change might also be in tension with patients' aesthetics and self-image.

Value dams and flows. Given the complexity of value tensions and a wide range of possible technical security systems that impact those tensions, the question becomes how to identify viable solutions. Value dams and flows is a VSD technique for identifying reasonable value-sensitive design options from among a large set of possible designs or technical features [18]. In this technique, options that are disliked by a threshold percentage of stakeholders are excluded from the list of viable solutions (dams); then from the remaining options, those that are liked by many stakeholders are selected as good candidates for solutions (flows). We extend the value dams and flows technique to identify a set of complementary security systems that, as a group, appeal to most of our study participants.

SECURITY SYSTEMS AND MOCKUPS

Our goal is to assess patients' views and values surrounding different technical approaches to provide an informed foundation for the design of future security systems. We selected a set of systems for the interview that span emerging technical approaches and potential patient values. The (non-orthogonal) technical approaches, as specified above, are: (a) passwords; (b) additional patient body modifications; (c) patient behavior changes; and (d) passive with respect to the patient. When picking systems to represent these approaches, we took care to choose system designs that would also probe patient values such as aesthetics, psychological distress, and unwanted historical associations. The system designs chosen for inclusion in this study were: a password engraved on a medical alert bracelet; a password tattooed as a visible 2D barcode; a password tattooed as a UV-visible 2D barcode; three versions of an external, computational wristband; a criticality-aware IMD; and a proximity bootstrapping device. These systems were organized into the 3 categories discussed below. We do not mean to imply that these systems are all favorable or complete designs; rather, presenting these system designs to patients and soliciting feedback provides a foundation for designing future security systems that satisfy technical requirements and respect patients' values.

We chose to use mockups of the systems during the interview to help participants envision the future systems [7]. While using specific objects can—and in some interviews did—cause participants to react to the particular appearance of the object rather than the general system properties, we found that the mockups helped make the systems concrete for participants. Since we were presenting 8 different systems, the mockups also functioned as memory triggers to help participants keep track of the different systems.

Passwords and Additional Patient Body Modifications

A natural approach to security for IMDs is to employ a passphrase such that access to read information from the

Figure 1. The front of the mockup representing a medical alert bracelet with a password engraved on its back.

Figure 2. The back of the mockup representing a medical alert bracelet with a password engraved on its back. Here the password is a translucent sticker.

Figure 3. The mockup representing a tattoo of a scannable password: the mockup is a translucent sticker with a black-ink stamp of a 2D barcode.

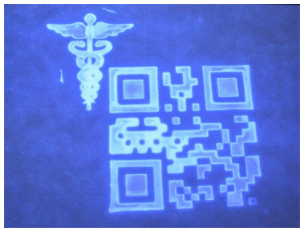

Figure 4. The mockup representing a UV-visible tattoo: the mockup is stamped with UV-visible ink (shown under a black light).

IMD or change its settings is blocked until users authenticate themselves. The following systems are password-based systems that offer different approaches for communicating a passphrase to medical staff. Additionally, two of the system concepts involve patient body modifications beyond the IMD implant.

Medical alert bracelet (Figures 1 and 2). Medical alert bracelets are accessories that are worn by some patients in order to inform emergency medical staff of their diagnoses in the case where the patient is unconscious. Since medical alert bracelets are less likely to be lost in an emergency than materials carried by patients—such as informational cards in their wallets—they are a safer way to convey the IMD passphrase to medical staff. In this security system, access to the IMD is protected by a passphrase engraved on the back of a medical alert bracelet that is worn at all times by the patient. This system reasonably satisfies the security property (preventing unauthorized access), since the passphrase can be protected from casual observation. However, the system does not fully satisfy the safety property (access in case of medical emergencies) even if the patient wears the bracelet at all times: the bracelet can still be lost or damaged in an accident, which would render the IMD inaccessible to emergency medical staff.

We included this system in the interview—despite its technical drawbacks—for several reasons: some patients may already wear medical alert bracelets, and people are generally familiar with the concept of a passphrase; the medical alert bracelet provides a contrast to the password-based tattoos (below) since it shares some of their properties but not others; and the medical alert bracelet provides a contrast to the wristband systems, which also require wearing something on the wrist (but operate by a different mechanism and require additional maintenance).

Visible tattoo (Figure 3). Tattoos have been used throughout history as artistic and cultural forms of expression. They are also an effective way to permanently carry information. In this security system, access to the IMD would be protected by a passphrase that is encoded as a 2D barcode and tattooed onto the patient's skin. There are two advantages to this system over the medical alert bracelet system: patients cannot forget or lose their passphrase, and they do not have to wear anything on their wrists. This system does not completely satisfy the safety property, since the tattoo could be damaged and rendered unscannable in an accident. Additionally, this system makes it more difficult to revoke or reissue passphrases. Using a tattoo as a security system for medical devices also touches on patient views and values such as self-image and freedom from unwanted historical associations.

The authors had some reservations about including a tattoo-based patient identifier in this study, especially considering potential associations with tattooing of prisoners in concentration camps during World War II; however, when some of the authors discussed the solution space at security conferences, they frequently heard the suggestion that a way to solve the problem of losing a carried passphrase in an accident is to tattoo the passphrase onto the patient's skin. We hypothesized that this system, while somewhat satisfactory from a technical perspective, would not be satisfactory from the patient's perspective. We included tattoos in this study in order to confirm or counter our hypothesis.

UV-visible tattoo (Figure 4). In addition to regular tattoos with black or colored inks, it is now possible to get specialty tattoos that are only visible under UV (black) lights. In this system design, access to the IMD is protected by a passphrase that is encoded as a 2D barcode and tattooed onto the patient's skin using an ink that is only visible under black lights. This system has an advantage over the visible tattoo system because it cannot be seen under normal conditions, and therefore does not affect the patient's appearance. This system was included in the interview because it provides a useful contrast to the previous system: it partially decouples a patient's tattoo from its cultural and historical associations.

Patient Behavior Change: Wristbands

In previous work, a group of computer security researchers, including some of the authors, performed a technical investigation into one potential security system for wireless IMDs. The system design consists of an external computational unit that controls access to the IMD [6]. The researchers call this system a Cloaker because its presence causes the IMD to be "invisible" to all unauthorized queries; however, we chose to call this the "wristband system" in the present study to avoid using suggestive terminology. When the wristband is present and worn by the patient, the IMD only acts on commands sent by authorized entities, implemented

Figure 5. The mockups shown to participants to represent the three different wristband systems. Bottom: regular. Middle: emergency and warning. Top: patient-specified functionality.

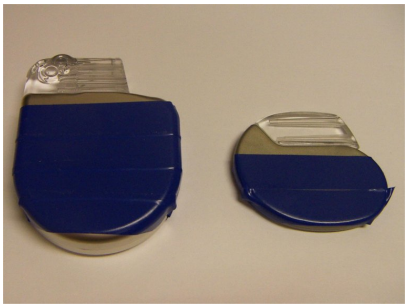

Figure 6. The mockups shown to participants to represent a future model of ICD or pacemaker that would automatically sense an emergency and respond by giving open access.

Figure 7. The mockup shown to participants to represent a proximity bootstrapping device that would be used by medical staff in an emergency.

by encrypting all communications to and from the IMD and checking them for authenticity and integrity. When the wristband is removed, the system changes its access policy to allow any programmer to access the IMD. In this way emergency medical staff can access a patient's IMD even if the wristband is lost or destroyed in an accident. This is in contrast to carrying an access passphrase on a medical alert bracelet or card, since emergency access with a traditional bracelet would not be possible if that bracelet or card were forgotten, lost, or destroyed.

The following systems are variations on the wristband concept. We included them in this study so that we could investigate human values—such as self-image, aesthetics, and convenience—implicated by a security system that has been previously proposed and published.

For the mockups of these systems, we wanted to provide a physical representation of the system concept and to avoid reactions based solely on the physical appearance of the mockup. We therefore used two sets of props for them, each of which has a slightly different appearance (see Figure 5). Our intention was that showing two different mockup models to participants would allow them to see two different hypothetical appearances for the device and encourage them to extrapolate to other physical appearances.

Regular (Figure 5). As described above, when patients wear the wristband, only pre-authorized parties—such as their cardiologists—can access the IMDs. When the wristband is removed or damaged and rendered useless, the IMD accepts communications from any programmer. This system addresses both the security and safety goals, but is only effective if the patient keeps the wristband charged and wears it on a regular basis. To distinguish this version of the system from the following versions, the mockup for this system was marked with blue tape (see Figure 5).

Emergency and warning (Figure 5). This security system, as with the previous system, restricts access when it is present and allows open access when it is absent. In contrast to the previous version, however, this system has additional features. It sounds an alarm when a patient enters an environment with a strong magnet, since strong magnets can affect the IMD's operation. The wristband also dials 911 when it detects that the patient is experiencing a cardiac emergency. The purpose of including this system in the interview was to contrast the participant's reactions to the regular wristband system with the participant's reactions to that same system when it offers additional safety benefits. To distinguish this version of the system from the other versions, the mockup for this system was marked with red and blue tape (see Figure 5).

Patient-specified functionality (Figure 5). This security system, as with the previous two, restricts access when the wristband is present and allows open access when it is absent. This system does not have the safety features of the previous (emergency and warning) system, but we invited participants to specify some additional functionality that they might find useful. In the interview we offer the examples of a watch, a pedometer, and a heart-rate monitor. This version of the wristband system is included in the interview so that we can investigate whether there is some other functionality that might entice patients to wear and maintain a security system. To distinguish this version of the system from the others, its mockup was marked with yellow and blue tape (see Figure 5).

Passive with Respect to the Patient

The security systems below share the characteristic that, unlike the above systems, they require no patient participation.

Criticality-aware IMD (Figure 6). This security system is a behavior that is built into a pacemaker or ICD, and therefore represents a system that requires no additional patient body modifications, patient behavior changes, or external equipment. The criticality-aware IMD detects indicators such as the patient's location, whether or not the patient is standing up (some pacemakers already incorporate accelerometers), and heart rhythms to determine whether or not the patient is in probable medical distress. If this data suggests that the patient is experiencing a medical emergency, the IMD changes its access policy for the duration of the emergency so that all programmers are authorized to issue commands. This behavior is intended to help ensure

the patient's safety, since then medical staff can access a patient's device in an emergency situation. This concept of a criticality-aware system is similar to Gupta et al.'s work on criticality-aware access for pervasive applications [10] and was proposed for use with IMDs in Halperin et al. [11]. This security system addresses both the security and the safety goals, assuming that it has a low incidence of false negatives (safety failures) and false positives (security failures).

Proximity bootstrapping (Figure 7). This security system consists of an external device that is used by medical staff. When placed in contact with the patient, the device negotiates a temporary key with the IMD through the patient's body—for example, via physiological keying [3] or acoustic signaling [12]—thereby gaining permission to access the IMD. As an alternative, this device could use proximity-based access, as proposed by Rasmussen et al. [22]. This security system was included because it does not involve patient participation, uses an external device carried by medical staff, and because a proximity bootstrapping device is analogous to devices currently used to communicate with IMDs via short- and medium-range wireless.

METHODS

Patients were recruited for the study at the pacemaker and ICD clinic at the Beth Israel Deaconess Medical Center in Boston after approval of the research protocol by the hospital's Institutional Review Board and the Institutional Review Board at the University of Washington. Patients with clinic appointments during the study window were asked to participate in the study. Participating patients were compensated for their expenses (parking).

We refined the interview protocol by conducting three pilot interviews with cardiac patients. A total of 17 interviews were conducted. Due to incompleteness ($N = 2$) and an irregularity in the questions ($N = 2$) we dropped 4 interviews. The data for the remaining 13 patients is reported here. Of the 13 patients, 9 had pacemakers and 4 had ICDs. The patients' average age was 67.9 (median = 69, range = 41–80). Our participant population was, on average, on their second implanted cardiac device (median = 1, range = 1–3+) and had lived with a device for 7.8 years (median = 6, range = 0–18).

The semi-structured interview protocol contained a combination of yes/no, multiple choice, and open-ended questions. The Mockup Evaluation portion of the interview presents participants with all 8 security systems in the Password and Body Modification, Patient Behavior Change (Wristband), and Patient-Passive categories. The category order was randomized across participants.

The Mockup Evaluation is divided into two parts. In the Mockup Properties portion, the interviewer explains each system and solicits positive and negative feedback about that system. In the Comparative Mockup Evaluation portion, once all systems have been presented, participants are asked to identify: (1) the systems that they liked; (2) the systems that they disliked; and (3) the system or systems that they would choose to use, if they were asked to use a security system in the future, though some people chose none for (3). The interviews were audio-recorded and later transcribed.

Evaluative (quantitative) responses from the interview were coded in the following process: (1) the primary coder developed a coding scheme for each quantitative question based on the possible answers; (2) the primary coder coded the evaluative responses for all interviews; (3) the reliability coder coded the evaluative responses for all interviews; and (4) Cohen's kappa was computed for the results. The overall value of Cohen's kappa for the quantitative responses reported in this paper is 0.754.

RESULTS

If participants (1) liked the system and did not (2) dislike the system, the combined code was "like." If they did not (1) like the system and (2) disliked the system, the combined code was "dislike." If they did not (1) like the system and did not (2) dislike the system, the combined code was "neither." If they *both* (1) liked the system and (2) disliked the system, the combined code was "neither." If either response was uncodable, the combined code was also uncodable. For this portion of the interview, responses from two participants were uncodable. Thus, $N = 11$ for these analyses. The results of these codings are shown in Table 1.

An Argument for Multiple Systems: User Satisfaction

The Least Disliked: Proximity Bootstrapping

In the absence of a consensus on a liked system, we use the technique of VSD dams and flows as the inspiration to isolate multiple systems that would achieve more complete "coverage" for the participants. We focused first on "dams," since it is particularly important at a minimum that every patient have a choice of a system that they do not actively dislike. As shown in Table 1, the proximity bootstrap mockup is not the most liked of the systems, but the fact that no participants disliked the mockup makes it a good candidate for part of a security solution for implantable cardiac devices. This security solution, however, is not optimal: only 27% (3 out of 11) of the participants liked it and would choose to use it.

The Most Liked: Emergency and Warning Wristband

Once we had a system that none of the participants in our sample disliked, we shifted our attention to "flows," seeking to select additional system mockups to create a portfolio of security systems that give a higher percentage of participants an option that they would like or choose to use. From inspection of the data (see Table 1), the most natural choice appears to be the emergency and warning wristband mockup, since it has high percentages in both categories. Another possible candidate might be the criticality-aware IMD. However, if we choose two mockups as system options, we should avoid mockups which tend to be liked, disliked, and/or selected by the same participants, since choosing both systems would be redundant. One way to measure this is to consider the correlation between the like/dislike scores for pairs of mockups and avoid selecting pairs for which scores are highly positively correlated. The like/dislike ratings for

Security Approach	Mockup System	Liked (N= 11)	Disliked (N= 11)	Would Choose (N= 11)
Password & Body Modification	Medical alert bracelet	0%	27%	0%
	Visible tattoo	9%	55%	9%
	UV-visible tattoo	18%	27%	18%
Patient Behavior Change: Wristbands	Regular	0%	36%	0%
	Emergency and warning	45%	27%	27%
	Patient-specified functionality	0%	36%	9%
Patient-Passive	Criticality-aware IMD	27%	18%	27%
	Proximity bootstrap	27%	0%	27%

Table 1. Participants' evaluations of different system mockups.

the criticality-aware IMD are positively correlated with the proximity bootstrap (using Kendalls tau-b, a non-parametric correlation coefficient, $\tau = 0.510$), so this mockup would not be a useful system to add to the solution portfolio. On the other hand, the like/dislike ratings for the proximity boostrap and the emergency and warning wristband are essentially uncorrelated ($\tau = -0.131$). Thus, these two mockups—the proximity bootstrap and the emergency and warning wristband—are a reasonable choice to put together. Between the two of them, 7 out of our 11 participants have at least one choice of a system that they liked, 6 of the 11 participants have a system that they said that they would select, all 11 can have at least one system that they do not dislike, and 8 of the 11 have a choice of two systems that they do not dislike.

Satisfying the Stragglers: UV-Visible Tattoo

Despite its poor overall ratings (see Table 1), if we were to add a third system to the solution portfolio, the best choice would be the UV-visible tattoo. The criticality-aware IMD has slightly better ratings overall, but its ratings are highly correlated with the proximity bootstrap. On the other hand, both of the participants who like the UV-visible tattoo liked neither the proximity bootstrap nor the emergency and warning wristband. The like/dislike ratings for the UV-visible tattoo have slightly negative correlations with the like/dislike ratings for both the proximity bootstrap ($\tau = -0.196$) and the emergency and warning wristband ($\tau = -0.125$), which indicates that it might be a useful addition to the solution portfolio. While the tattoos are not particularly popular overall, the UV-visible tattoo seems to pick up a segment of people who are not served by the other solution options. In fact, given a choice of these three systems, 9 out of our 11 participants have at least one system that they like. The remaining two participants did not like any of the systems, so no combination of systems would include them.

The Final Solution Portfolio

It is interesting to note that this final solution portfolio includes one mockup system from each of the three different categories of security approaches. Like/dislike scores within each category tend to be somewhat highly correlated (for example, criticality-aware IMD vs. proximity bootstrap, $\tau = 0.510$; regular and patient-specified functionality wristbands, $\tau = 1.000$; emergency and warning wristband vs. each of the other two wristband systems, $\tau = 0.545$). Thus selecting multiple systems from the same category would generally be redundant. To obtain broad coverage, it is necessary to select a diversity of types of security approaches which will appeal to different patients.

Mockup System Properties: Pros and Cons

Although the population size was too small to generate definitive statistical analyses, the interview responses do provide qualitative insight into the perspectives and concerns of patients with implanted cardiac devices. Below is a list of (non-mutually-exclusive) properties—both desirable and undesirable—that surfaced during discussions with participants about the system designs.

Security. Participants expressed liking systems because of their perceived security benefits and disliking systems because of their perceived security flaws. Moreover, sometimes the same system received both positive and negative feedback on its security properties. As an example, different participants complemented and critiqued the medical alert bracelet system based on its security properties. Some participants appreciated that access to their IMD would be protected by a password, while others objected to the fact that their passwords would be carried around with them and might be acquired by others.

Safety. Participants were very interested in how the mockup systems affected their safety in emergency situations. One of the better-liked systems, the emergency and warning wristband (45%, 5/11), was much better liked than the other wristband versions. Comparing the scores on the like/dislike scale for the emergency and warning wristband system versus the other wristband systems using a Wilcoxon signed-rank test yields a test statistic of $Z = -2.121$ and p-value of 0.034, indicating that like/dislike scores were significantly higher for the emergency and warning wristband system. The emergency and warning wristband differed from the others by offering two features that enhance the safety of the patient. The fact that this wristband version stood out from the others suggests that participants valued it for its safety features. Similarly, participants rejected some systems based on their perceived safety flaws. In almost all of these cases, the participants were worried that hospitals might not have the correct equipment, causing their IMDs to remain inaccessible in an emergency. These fears were expressed about scanning equipment for the tattoos, a black light for the UV-visible tattoo, and the proximity bootstrapping device. Further fears were expressed that medical staff might not know to look for or might not be able to locate a UV-visible

tattoo. Additionally, some participants were concerned that the criticality-aware IMD did not have a manual override.

Privacy. Some mockup systems were called out as having negative effects on privacy. In particular, participants worried that wearing something or having some other visual indicator would force them to broadcast their medical condition to others. In the words of one patient:

Subject E: *I don't like the idea of wearing the wristband...I already have a defibrillator. Why do I have to wear something on my hand...to show that I have-, that I have a defibrillator, that there's something wrong with me. No.*

Aesthetics. Participants disliked some system mockups because they found them to be unaesthetic. One participant commented that the tattoo was visually too "busy." There were also frequent comments about the appearances of the wristbands. The wristbands are meant to be worn at all times; some participants saw their unattractiveness as a major obstacle to system adherence.

Psychological welfare. Participants disliked systems that they deemed to be psychologically distressing or not respectful of their personal dignity. In particular, participants stated that wearing or seeing something that would remind them of their condition could be upsetting. One participant objected to the medical alert bracelet on these grounds:

Subject M: *It would make me feel like an invalid...That I had this thing, like the Scarlet Letter or [laughs].*

Another participant felt that the emergency and warning wristband would be very distressing if its alarm suddenly went off in reaction to a magnet.

Convenience. A prominent objection to the wristband systems was their inconvenience. This included both mental and physical inconveniences: the mental inconvenience of remembering to charge the wristband and keeping track of it; and the physical inconvenience of having something on one's wrist that could catch on objects, needs to be taken off when showering, etc.

Cultural and historical associations. Many participants had objections to the tattoo systems.

Subject M: *Well, I mean for-, because I'm Jewish it-, I'm not-, a tattoo on the arm to me means a concentration camp. So right away that's the immediate horror.*

In one case, a participant disliked the system because she associated tattoos with drunks. Clearly, it is not desirable to have a security system for a beneficial medical device to have negative associations of these types in patients' minds.

Self-image and public persona. Interestingly, one patient did not object to the visible tattoo system in principle or due to any personal associations; instead, she objected that having a tattoo would present a persona to others that would be inconsistent with the one that she wished to project.

Autonomy and notification. Some participants had strong negative reactions to the criticality-aware IMD based on the fact that it silently changes its mode in an emergency to give all programmers access. While this objection could be addressed by adding in an audio or vibrational notification, it is noteworthy that these participants felt so strongly about not being informed. Similarly, some participants appreciated the proximity bootstrapping device because—assuming that the patient is conscious—the system involves implicit consent.

Attitudes Towards Wireless IMD Security

Participants were asked a series of questions about the importance of safety, privacy, and health. Responses for each question were coded on a 5-point scale of -2 (strongly disagree) to 2 (strongly agree). Some responses were uncodable. All 13 participants agreed or strongly agreed that they were concerned with maintaining their health, with a mean score of 1.38. Most participants also agreed that they were concerned about the safety and privacy of their electronic information (mean score 1.00, 10 out of 12 agreed or strongly agreed), their personal privacy (mean 0.77, 10 out of 13 agreed or strongly agreed), and their physical safety (mean 0.82, 9 out of 11 agreed or strongly agreed).

On the other hand, a majority of participants disagreed when asked if they were concerned that someone might change the settings on their IMD without their permission (mean score -0.92, 10 out of 12 disagreed or strongly disagreed) or that medical staff would be unable to change the settings on their IMD in an emergency (mean -0.80, 7 out of 10 disagreed or strongly disagreed). Despite this apparent lack of concern about the security of their IMD, participants tended to agree that something should be done to protect the security of future IMDs (mean 0.89, 7 out of 9 agree or strongly agree). To illustrate some of these points of view, we include below quotes from two participants who lie at the opposite ends of the spectrum.

The following participant did not want random, unauthorized parties to be able to access his pacemaker. He indicated that leaving open access means that some malicious party will attempt to take advantage of that opportunity:

Subject K: *If, if anyone el-, everyone else can do it, they will do it...Or someone will do it.*

In contrast, this participant was unconcerned about the possibility of a cyber-attack targeting IMDs.

Subject D: *I'm not gonna-, I think it's ridiculous to worry about the security of it...Anybody that wants to get to me that bad, be my guest.*

DISCUSSION

Designing Security Systems for IMDs

Based on participants' reactions to our specific systems as instantiations of general system properties, if researchers and designers want their IMD security systems to be liked by—or at least acceptable to—patients, we advise them to meet the following criteria:

- **Good (perceived and actual) security properties.** Some participants objected to the medical alert bracelet system because they felt that carrying around a human-readable password was insecure.

- **Good (perceived and actual) safety properties.** Participants were very interested in whether a system was safe: for example, whether it had an override or whether medical staff might not have necessary equipment.

- **Respect patients' privacy and avoid disclosing patients' conditions.** Both the medical alert bracelet and the wristband systems were criticized for being visible indicators of patients' medical conditions, while the emergency and warning wristband was criticized because its alarm feature would require explanation if it went off in a crowd.

- **Be aesthetically pleasing (or at least aesthetically neutral).** Many participants objected to the wristbands based on their appearance.

- **Avoid causing patients sudden alarm about their health.** A participant expressed that an alarm suddenly going off might cause patients to panic.

- **Avoid needlessly reminding patients of their condition.** Depending upon the medical condition and the implanted device, patients may need to maintain some awareness of how their behavior might affect their health; nevertheless, the psychological effects of the technology should be minimized. Some participants did not want to look at medical alert bracelets or wristbands that would remind them of their conditions.

- **Avoid being physically irritating.** The medical alert bracelet and the wristbands were both criticized because they could be physically irritating to wear on the wrist.

- **Avoid requiring frequent upkeep.** The wristbands were also criticized because they require regular recharging.

- **Work with patients to offer an option that fits their self-image.** One participant in particular expressed that the visible tattoo was not palatable because it would give other people a certain impression about her—an impression that she did not want to project. Systems should be mindful of patients' sense of dignity.

- **Avoid unwanted negative associations due to historical, religious, or cultural factors.** Several participants strongly disliked one or both of the tattoo systems because of tattoos' associations with concentration camps; another participant did not like the visible tattoo system because it reminded her of drunks.

- **Provide the patient with the option to be notified of changes in system status.** Several participants disliked the criticality-aware IMD because it changed its access mode without notifying the patient.

Placing Patient Preferences in Context: Design Tensions with Single vs. Multiple Options

Although the results from the previous section suggest that patients may be served by providing a range of options, the landscape is complex and consists of more than patients' preferences. HCI research can contribute to the formation of a security ecosystem for IMDs, but patient values and preferences must be weighed against other important constraints. There are several reasons why a single-system solution might be preferable over multiple options.

Decreased usability means decreased safety. Usability and speed-of-use can translate into direct safety benefits for patients; in a medical emergency, small time delays can have serious effects. Having multiple security systems means that medical staff would require extra time to identify which system the patient is using, locate any appropriate equipment, and then respond accordingly.

Cost of FDA approval. Medical equipment must be approved by the FDA before it can be used to treat patients. Clinical trials cost time and money, which is a disincentive for manufacturers of medical equipment.

Burden of training. EMTs, nurses, cardiologists, and device technicians need to be informed about security systems and need to be trained on applicable equipment.

Expense of providing, acquiring, and maintaining equipment. Hospitals must have access to all applicable security equipment in order to be able to treat any patient who comes to that hospital.

Mental stress and complications of choice. As we observed in our interviews, different people prefer different levels of involvement in their medical decisions; some people delegate decisions to their doctors while others are very involved in the process. Having different choices for IMD security could potentially create friction between doctors and patients if a patient desires an option that a doctor believes to be unsuitable. Alternatively, if doctors offer patients a free choice of several systems, patients might experience stress while deciding and be doubtful about the wisdom of their final choice.

CONCLUSION

Prior work has focused on assessing the technical security risks with wireless implantable medical devices [12], as well as exploring technical approaches for improving their security. While these technical investigations are fundamentally important, it is also fundamentally important to understand patients' views and values surrounding these technical approaches. To do otherwise might eventually lead to solutions that are technically viable but significantly undesirable from a patient's perspective. This work seeks to address this gap via empirical investigations into patients' views and values regarding 8 mockup IMD security systems. Participant responses help identify positive and negative attributes of potential systems. Our observations suggest that no single security approach may be attractive to all patients, but rather

that different types of security approaches may appeal to different patients. Based on our results and observations, we discuss several challenges for securing wireless IMDs and provide guidelines for future designs.

Unlike most personal computing devices—cell phones, watches, computers, and so on—IMDs are unique in their embodied nature; they are a technology that is inseparably incorporated into the user's body. Our work therefore complements the existing body of literature on security and privacy for ubiquitous computing by exploring these concepts in a fundamentally different setting. Looking beyond IMDs, our findings also demonstrate how cultural and historical influences can impact the acceptability of otherwise viable technical solutions. Additionally, we provide an extension to the VSD value dams and flows technique that adjudicates value tensions by identifying multiple, complementary solutions. This study also extends the VSD literature to include investigations into embodied technologies and healthcare applications. Perhaps most importantly, this paper provides a clear example of the potential tensions between *security* and *safety* while introducing the HCI community to a new area: security for wireless implantable medical devices.

Acknowledgments

This work was supported in part by NSF Awards CNS-0905118, CNS-0905384, and an Alfred P. Sloan Research Fellowship.

REFERENCES

1. A. Adams. Multimedia Information Changes the Whole Privacy Ballgame. In *Conference on Computers, Freedom, and Privacy*. ACM, 2000.
2. V. Bellotti and A. Sellen. Design for Privacy in Ubiquitous Computing Environments. In *ECSCW*. Kluwer Academic, 1993.
3. S. Cherukuri, K. Venkatasubramanian, and S. Gupta. BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body. In *ICPP Workshops*, 2003.
4. L. F. Cranor and S. Garfinkle, editors. *Security and Usability: Designing Secure Systems That People Can Use*. O'Reilly, 2005.
5. C. A. Curran. Nurse Tracking Systems: Do the Benefits to Nurse Managers Outweigh Risks to Nurses' Privacy? Writing for the CON Position. *American Journal of Maternal Child Nursing*, 27, 2002.
6. T. Denning, K. Fu, and T. Kohno. Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security. In *HotSec*, 2008.
7. P. Ehn and M. Kyng. Cardboard computers: Mocking-it-up or hands-on the future. In Greenbaum and M. Kyng, editors, *Design at Work: Cooperative Design of Computer Systems*. 1992.
8. B. Ertl. Hooligans Attack Epilepsy Patients During Epilepsy Awareness Month. `http://www.pr.com/press-release/60959`, 2007.
9. B. Friedman, P. H. Kahn Jr., and A. Borning. Value Sensitive Design and information systems: Three case studies. In P. Zhang and D. Galletta, editors, *Human-Computer Interaction and Management Information Systems: Foundations*. 2006.
10. S. K. S. Gupta, T. Mukherjee, and K. Venkatasubramanian. Criticality Aware Access Control Model for Pervasive Applications. In *PERCOM*, 2006.
11. D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. Security and Privacy for Implantable Medical Devices. *IEEE Pervasive Computing*, 7, 2008.
12. D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In *IEEE Symposium on Security and Privacy*, 2008.
13. K. Hanna, F. Manning, P. Bouxsein, and A. Pope, editors. *Innovation and Invention in Medical Devices: Workshop Summary*. 2001. National Academy of Sciences, `http://www.nap.edu/catalog/10225.html`.
14. J. I. Hong and J. A. Landay. An Architecture for Privacy-Sensitive Ubiquitous Computing. In *Mobile Systems, Applications and Services*. ACM, 2004.
15. X. Jiang, J. I. Hong, and J. A. Landay. Approximate Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing. In *Ubicomp*, 2002.
16. X. Jiang and J. A. Landay. Modeling Privacy Control in Context-Aware Systems. *IEEE Pervasive Computing*, 1, 2002.
17. M. Langheinrich. A Privacy Awareness System for Ubiquitous Computing Environments. In *Ubicomp*. Springer-Verlag LNCS, 2002.
18. J. Miller, B. Friedman, G. Jancke, and B. Gill. The Value Sensitive Design, Development, and Appropriation of a Corporation's Groupware System. In *GROUP*, 2007.
19. G. Myles, A. Friday, and N. Davies. Preserving Privacy in Environments with Location-Based Applications. *IEEE Pervasive Computer*, 2, 2003.
20. L. Palen and P. Dourish. Unpacking "Privacy" for a Networked World. In *Conference on Human Factors in Computing Systems*. ACM, 2003.
21. K. Poulsen. Hackers Assault Epilepsy Patients via Computer. `http://www.wired.com/politics/security/news/2008/03/epilepsy`, 2008.
22. K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun. Proximity-based Access Control for Implantable Medical Devices. In *CCS*, 2009.
23. M. Tentori, J. Favela, and V. M. Gonzàlez. Quality of Privacy (QoP) for the Design of Ubiquitous Healthcare Applications. *Journal of Universal Computer Science*, 12, 2006.
24. M. Tentori, J. Favela, and M. D. Rodrìguez. Privacy-Aware Autonomous Agents for Pervasive Healthcare. *IEEE Intelligent Systems*, 21, 2006.
25. E. Yu and L. M. Cysneiros. Designing for Privacy in a Multi-agent World. In *Trust, Reputation, and Security*, 2002.