A Taxonomy of Vulnerabilities in Implantable Medical Devices

Jeremy A. Hansen
Department of Computer Science
Norwich University
Northfield, VT 05663 USA
jhansen3@norwich.edu

Nicole M. Hansen
Department of Veterinary Clinical Sciences
Louisiana State University
Baton Rouge, LA 70803 USA
nhanse1@lsu.edu

ABSTRACT

Once the domain of science fiction, devices connecting biological systems with computers have become reality. Security vulnerabilities that might be exploited in such systems by malicious parties or by inadvertent manipulation are also now a reality. Where previous research has described certain categories of attacks against and countermeasures for implantable medical devices (IMDs), we construct a loose vulnerability taxonomy useful for the design of countermeasures that reinforce the security of these devices and evaluate avenues of attack that are novel to devices implanted in the body. Using this taxonomy, we discuss several well-known and novel countermeasures and discuss the specific categories of attacks that each can foil.

Categories and Subject Descriptors

J.3 [**Life and Medical Sciences**]: Medical information systems

General Terms

Design, Security

Keywords

Implantable medical device, intra-body network, taxonomy, vulnerability

1. INTRODUCTION

Implantable medical devices (IMDs) have come a long way from the first pacemakers and prostheses, so that doctors now have the ability to remotely or autonomously monitor patients and deliver treatments without requiring an office visit. With the ability to communicate over a distance comes the possibility that unauthorized parties can intercept such communications or compromise the device remotely. Though such devices do not yet exist, the difficulty of securing such devices is increasing by virtue of the devices' abilities to communicate *with one another* and potentially establish complex feedback loops, since a previously innocuous attack against one IMD might affect a different IMD.

We define an implantable medical device as a device permanently or semi-permanently implanted into a patient which treats some underlying medical condition, enhances the function or appearance of some part of the body, or provides a previously unrealized ability. This definition remains broad and includes the second two properties because we feel that elective implants (that may or may not specifically treat any underlying condition) such as LED tattoos [7] with dynamic displays will become increasingly available. In fact, we will use implantable dynamic tattoos (IDTs) as a running example. Though these tattoo devices are still theoretical, they are easy to understand: their operation is as simple as a computer monitor and they are visible outside the body. We refer to a collection of IMDs in a single patient as an intra-body network (IBN) [3], and will use that term when referring to systems consisting of multiple IMDs.

It is important to guarantee security in these systems – automated mishaps as occurred with radiotherapy machine software that was responsible for overexposing patients to high levels of radiation [25] are avoidable when possible faults and system interactions are better understood. We seek to help understand how to protect IMDs from both accidental mishaps[1] and malicious effects by evaluating methods that can be used to predict probable future attack avenues. By considering related classifications used in medical, engineering, and computer security systems, we break down vulnerabilities in a way such that commonalities and differences can be easily spotted.

1.1 Organization of This Paper

In this introduction, we illustrated the need for an evaluation of security vulnerabilities specific to implantable medical devices. We continue in Section 2 by reviewing previous work in classifications and taxonomies relevant to the security of IMDs. In Section 3, we describe some possible categories, and then apply them to a handful of known vulnerabilities. Using the categories enumerated in Section 3, we discuss existing and novel countermeasures for known and unknown vulnerabilities in Section 4. We conclude with

[1]Note that IMD vulnerabilities do not require a malicious attacker to exploit and can be quite simple. It has been shown that children playing on plastic slides build up a sufficient static electricity charge to interfere with the programming of their cochlear implants [31]. Some of the countermeasures described herein may defend against nonmalicious adverse events.

SPIMACS'10, October 8, 2010, Chicago, Illinois USA.

a brief review and a discussion of possible future research directions in Section 5.

2. PREVIOUS APPROACHES

The fields of biomedical engineering, medicine, and information security have developed classifications related to security or IMDs appropriate to each field. Since no current classification scheme encompasses the unique properties of security in IMDs, the approaches of these fields are too restrictive to be directly usable in the development of IMD security models. In this section we describe each field's contribution to our categorization of IMD vulnerabilities and in the subsequent section combine these perspectives to generate a "big picture" view of vulnerabilities and countermeasures in IMDs.

2.1 Biomedical Engineering

In places like the United Kingdom, manufacturers of IMDs are held to certain standards when testing and implementing their devices. According to the UK's National Research Ethics Service [28], the following are considered to be "Serious Adverse Events" in medical device research:

- Results in death
- Is life-threatening
- Requires hospitalisation or prolongation of existing hospitalisation
- Results in persistent or significant disability or incapacity
- Produces a congenital anomaly or birth defect
- Is otherwise considered medically significant by the investigator

We use this definition of adverse events as a starting point to describe the medical effects of an exploited IMD vulnerability and describe adverse events in far more detail in Section 3.4: "Result/Pathogenesis". Table 1 shows various IMDs with some specific adverse events that might result from vulnerabilities in each. For example, an IDT programmed to display blood glucose levels might be compromised to display inaccurate data or unauthorized text and consequently result in an inappropriate insulin injection.

2.2 Medicine

The field of medicine classifies diseases and health issues with an extensive coding system. The International Statistical Classification of Diseases and Related Health Problems (ICD-10) [39] reserves four categories (each with ten subcategories) for complications related to implanted medical devices, a sampling of which follows:

- **T82**: Complications of cardiac and vascular prosthetic devices, implants and grafts
- **T83**: Complications of genitourinary prosthetic devices, implants and grafts
- **T84**: Complications of internal orthopædic prosthetic devices, implants and grafts
- **T85**: Complications of other internal prosthetic devices, implants and grafts
  - **T85.1**: Mechanical complication of implanted electronic stimulator of nervous system
  - **T85.3**: Mechanical complication of other ocular prosthetic devices, implants and grafts

This classification divides up the complications based on the type of IMD that is involved, which is consistent with medicine's method for classifying the etiology of diseases by their symptoms. Clearly some expansion of this classification is necessary to account for IMDs that are not cardiovascular, genitourinary, orthopædic, or ocular in nature, and do not involve electronic stimulation, like our example of the IDT. The combination of this medical classification with the adverse events of Section 2.1 provides two categories to start our classification: IMD activity and adverse effects.

2.3 Information Security

Relevant classifications in the field of information security [1, 2, 5, 6, 20, 21, 22, 26, 37] are divided into those that describe threats to systems and those that evaluate the vulnerabilities. While the taxonomies tend to describe the same risks, the perspectives differ. We embrace this separation of threats and vulnerabilities and include categories for both the threat mechanism and the effects of a compromise. Unfortunately, our work's focus on IMDs does not have nearly the same amount of information relating to actual risks to IMDs as found in the 40-year history of security in computer systems and networks. The information security taxonomies are intentionally more general than ours and describe specific features of the operating system, software, or networking components. We use the taxonomies as a reference, but adopt categories relevant to the security of IMDs and ignore those categories and approaches that do not apply.

3. VULNERABILITY CLASSIFICATION

Since there have been few security vulnerabilities reported in IMDs as previously noted, many of the vulnerabilities and category combinations we propose here are hypothetical. We have attempted to predict as many types of vulnerabilities as possible by taking a defense-centric perspective, but we acknowledge that this approach likely falls short of being exhaustive. We also acknowledge that the types of threats that future IMD users might face might vary dramatically, from corporate privacy threats to hostile governments, so we intentionally aim to encompass all of these possibilities. Nevertheless, while we focus on the sorts of threats that are largely well-known, like those affecting modern computer systems, the classifications of vulnerabilities described in Section 2 can be used as a reference to evaluate other likely categories and sensible divisions of the space of all IMD vulnerabilities.

The overall scheme that we adopt also relies heavily on the field of medicine's study of diseases according to their *etiology* (or cause) and *pathogenesis* (or mechanism/effects).

3.1 Scope

Where Halperin et al. [18] focused upon the tensions between the security, safety, and utility design goals of wireless IMDs, we focus more specifically upon the security vulnerabilities in the IMDs themselves. We do not try to enumerate attacker motivations or the equipment required for an attack and do not restrict our analysis only to wirelessly-communicating devices. Conflicts with safety, utility, or

Table 1: Potential Adverse Events in Various Implantable Medical Devices

Device	Adverse Events
Pacemaker, implanted cardiac defibrillator [27], ventricular assist device [15]	Heart failure, tachycardia, bradycardia, arrhythmia
Cochlear implant	Deafness, phantom sounds, distraction/confusion
Prosthetic limb control system [38]	Injury, damage to prosthetic limb, inadvertent movement
Spinal cord stimulator [29]	Loss of pain relief, inappropriate stimulation
Sacral anterior root stimulator [8]	Infection from inability to void, inappropriate stimulation
Retinal prosthesis [10], implanted contact lens, intraocular lens	Blindness, phantom images, distraction/confusion
Implanted infusion pump	Inappropriate dosage/timing
Brain-machine interface, other neuroprosthesis [32, 34]	Loss of consciousness, neural effects [14]
Responsive neurostimulator, other deep brain stimulator [35]	Inappropriate stimulation, failure to stimulate
Implanted monitor or sensor	Incorrect readings
Implanted RFID tag [17]	Loss of privacy, data leakage
Implanted dynamic LED tattoo	Inappropriate display

patient acceptability are mentioned where appropriate, but this paper does not address these as primary concerns of the classification scheme. We are also not interested in those threats that directly and physically affect the body and result in trauma regardless of the presence of an IMD. For example, high levels of radiation exposure can interfere with a microprocessor in an implanted device, but the radiation is likely to damage the surrounding tissue much more. We are also not interested in side effects related to the surgical procedures necessary to implant the devices such as infection, immune response to foreign material, or scarring, though these issues are of concern in the design of an acceptable and effective IMD.

We propose five ad hoc categories, divided into two groups consistent with disease taxonomies as mentioned above: *cause* or etiology (which encompasses proximity, activity, and patient state) and *result* or pathogenesis (encompassing the affected component and the permanence of the effect). In order to evaluate a new vulnerability, we choose the most appropriate item(s) per category and choose values for subcategories as appropriate. Refer to Table 2 for several examples of vulnerabilities broken down according to this classification.

3.2 Authentication

Since a vulnerability is often defined by the level of access an unauthorized user might attain, it is helpful to first discuss what it means to be an authorized party. One difficulty with guaranteeing the security of an implantable medical device is that the list of authorized parties may change depending on the patient's circumstances, as discussed at length in [18].

When the IMD is operating normally in a non-emergency situation, authentication can be handled the same as any other computer system: by requiring proof that the authenticating party is legitimately representing itself. This authentication is typically guaranteed by requiring the authenticating party to provide one or more of three factors: something known (like a password), something possessed (like a physical key), or something unique about the party (like a fingerprint).

In special circumstances or in an emergency, it is important for emergency medical professionals to know about and have access to the IMD and its facilities[2]. For example, an ILT might be configured to provide diagnostic information or an audible cue to emergency personnel if it detects a weak pulse, low blood glucose, or if the patient is unconscious. In these circumstances, the IMD may discard typical authentication requirements and allow access to unauthenticated or weakly-authenticated users. When this happens, an unauthenticated user can be an *authorized* user, and for the sake of the discussion of our classification, will be treated as equal to a fully authenticated (and authorized) user in non-emergency situations. For the purposes of our discussion here, we will only refer to parties as authorized or unauthorized and largely ignore how they became authorized (or did not).

3.3 Cause/Etiology

The cause of a compromised vulnerability (one might also call this the threat vector or the etiological agent) can be divided into three categories: proximity, IMD activity, and patient state.

3.3.1 Proximity

Proximity refers to the distance from the patient or IMD at which a vulnerability is exploitable. In the closest case, an attacker would need to physically touch the patient, though we do not consider measures an attacker might take to make such contact innocuously[3]. We might define general categories like the following:

- Contact: touch
- Short: up to 1 meter
- Medium: 1 meter-50 meters

[2]It should be noted that patients themselves should probably have partial control of their implants, but controls may be put in place to prevent accidental or intentional misuse of their IMD. The amount of access a patient is allowed is an interesting ethical question beyond the scope of this paper. For example, should users have the rights to see the source code to the devices which may be keeping them alive?

[3]Like any system, long-term physical access to an incapacitated or compliant patient will allow for virtually all IMDs to be compromised.

Table 2: A Breakdown of Several Vulnerabilities According to our Classification

Threat	Proximity	Activity	Patient State	Component(s) Affected	Permanence
Headphones with magnetic interference [24]	Contact	N/A	N/A	Target IMD (Actuating), Patient (Heart)	Temporary
Plastic slide [31]	Contact	N/A	N/A	Target IMD (Actuating), Patient (Hearing)	Temporary
Wireless traffic sniffing	Medium	Communicating	N/A	Target IMD (Communicating)	Temporary
Wireless pacemaker exploit []halperin:pacemakerexploit	Short	Communicating	N/A	Target IMD (Actuating), Patient (Heart)	Temporary
Contrived ILT exploit (see §3.5)	Network	Communicating	Glucose level	External device	Temporary
Contrived prosthetic eye exploit (see §3.5)	Line of sight	Actuating	Visual pattern	Target IMD (Actuating)	Permanent

- Long: 50 meters+
- Line of sight
- Network

Note that line of sight and network overlap with other proximity descriptors, but we include them here to distinguish between vulnerabilities that require only visual contact (those affecting the optics of a camera) or those that connect to the IMD over a network but are otherwise "proximity agnostic". When the distance is known more concretely, it is better still to be more specific and describe the proximity in terms of the ranges of the devices involved, such as "Bluetooth signal range" or "approximately 10 meters".

3.3.2 Activity

Devices in an IBN (indeed, nearly any networked device) can engage in one or more of four general activities [23]: sensing (collecting information from the body or environment), actuating (producing some effect, typically therapeutic), information processing (performing some computation using collected or communicated information), and communicating (with other devices in the IBN, external devices, or the patient). These activities are used to categorize both the vulnerable mechanism (as in this section) and the type of IMD behavior affected by an attack, as in Section 3.4.1.

3.3.3 Patient State

The state of the patient also plays a role in IMD vulnerabilities. This state can be leveraged in countermeasures that are sensitive to the patient's body and environment, as described in Section 4.6. Data from environmental, worn, or implantable sensors can provide this sort of data to IMDs that do not contain such functionality on their own. We also discuss two contrived attacks in section 3.5 that rely on the patient's state to produce their effect.

While states like body position, glucose level, location, magnetic field presence, pulse rate, and body temperature have been proposed elsewhere and may have real-life implementations, several of the patient states used as examples here require additional explanation, and may not reflect actual sensors or devices currently available. A sensor that monitors consciousness would detect when the patient is sleeping, under anæsthesia, or has lost consciousness due to trauma. An ILT might display a warning in the presence of a particular drug, such as a prescribed medication, illegal substance, or environmental toxin that could interfere with the patient's treatment. A muscle tension sensor could be used by conscious patients to activate a programming mode of their IMD by a sequence of voluntary flexes of certain muscles. For patients with a neural interface, the "link status" could be used as a deciding factor in granting access to programming mode, or to certain other IMD behaviors.

3.4 Result/Pathogenesis

Adverse effects, as introduced in Sections 2.1 and 2.2, are further broken down into two categories: component affected and permanence.

3.4.1 Component Affected

The category of component affected can be initially classified as one of the following: IMD, patient, or device outside of patient IBN. When an IMD is determined to be affected, we must then determine whether the targeted IMD is directly affected or if a second IMD bears the effects. We make this distinction because it seems possible that a second IMD or external device that trusts the targeted IMD (such as if the targeted IMD was used as a biometric token in an external authentication scheme, as used in our contrived example later) could be compromised as a result of a "bounce" attack via the targeted IMD in the same vein as an FTP bounce attack [19]. We further divide effects on IMDs into their corresponding four components: processing, actuating, communicating, and sensing.

3.4.2 Permanence

The effects of an IMD failure can be categorized as temporary (the effects wear off after a time or after the threat is removed) or permanent. The magnetic interference generated by common headphones discussed in [24] is a good example, since the adverse effect on the defibrillator only lasted as long as the headphones were in close proximity and disappeared (with one exception) when they were removed. A permanent effect might be the result of an irreparable firmware update ("bricking") or, in the worst case, the death of the patient.

3.5 Application of the Classification

In addition to four real-world examples listed in Table 3, we offer here two contrived examples of threats that demon-

Table 3: Vulnerability categories and subcategories of component affected

IMD	Target IMD	Processing Actuating Communicating Sensing
	Other IMD	Processing Actuating Communicating Sensing
Patient	Nervous	Brain Neural circuits Spinal cord
	Circulatory Gastrointestinal Genitourinary Immune Musculoskeletal Reproductive Sensory Skin/cosmetic	...
External device	Different classification	...

strate attacks which rely on the patient's state, affect outside devices, or are permanent, none of which have appeared as genuine concerns with current IMDs.

Consider an ILT that not only acts as a glucose level display on the patient, but also provides authentication to the patient's personal computer as a representation of something unique about the patient. A malicious user could exploit an unpatched vulnerability to install a logic bomb triggered by a low glucose level (for some reason) to hijack the authentication exchange and attempt to compromise the computer.

The second example would rely on a prosthetic eye having faulty programming which respond to a particular sequence of flashing lights (say, a similar sequence that might trigger epileptic seizures) by permanently disabling the eye's microcontroller. We accept that these two examples are quite unlikely, but we feel that the security of complex future interactions of IMDs warrant the wild speculation.

4. COUNTERMEASURES

Previous works [18, 14] describe many possible countermeasures to prevent vulnerabilities in IMDs, several of which follow. We also introduce several of our own novel countermeasures. Countermeasures may exist which make an otherwise vulnerable device invulnerable to a category (or several categories) of threats. We note that when IMDs (and their countermeasures) fail, they should fail open, since it is almost always better to give possibly-inappropriate access if the alternative is death or disability, as described in Section 3.2.

Security countermeasures are often divided into three primary groups: protective, corrective, and detective countermeasures. Protective countermeasures such as network firewalls aim to prevent a threat from exploiting a vulnerability, and would therefore be relevant in the scope of this paper to the "cause" categories of proximity, exploited activity, and patient state. Corrective countermeasures like data backup and recovery mitigate or lessen effects of a successful compromise, and are relevant to the "cause" categories of component affected and permanence. Detective countermeasures like intrusion detection systems cover all of our categories, in that they provide an audit trail of an exposure to a particular threat or the results of a successful compromise. As we discuss each example we give below, we explain to which of these three primary groups the countermeasure belongs.

4.1 Auditing

Auditing can be an effective detective countermeasure that is relevant to all five categories of the taxonomy. Not only can auditing provide a record of authorized and unauthorized access, it can document in detail patient state data, which could prove useful in troubleshooting badly-behaving (or compromised) IMDs. As in nonmedical computer systems, auditing might also eventually be required for regulatory compliance.

4.2 Notification

This detective control allows for direct communication with the patient, bystanders, or emergency personnel in the form of audible or visual cues, vibration, mild electric discharge, or through external devices like a personal computer/base station, portable display (say, in a watch or smart phone), or IDT. The only attack which could not be affected by this countermeasure is one which requires the patient to be unconscious (for patient notifications) and/or alone (for bystander and emergency personnel notifications). A vibrating notification would not be useful in these cases.

4.3 Trusted External Devices

Hardware access tokens [4] and communications cloakers [13] are two known instances of this protective countermeasure, which offload power-intensive computation and some of the protection mechanisms to a device outside the patient's body. A specific instance of a trusted external device called Cloaker provides security when worn and fails open when removed, which is tested for by detecting the patient's pulse. A similar external device could use inductive coupling to detect removal if worn close enough to the IMD. These external devices protect against attacks against the communication facilities of the IMD in all circumstances except when the malicious party can physically touch the patient.

4.4 Cryptographic Protections

Cryptographic methods protect communications channels and device logs, and also show promise in preventing unauthorized parties from initiating communications with the goal of draining the IMD's battery [9]. They may also provide a detective control through the use of cryptographic hashes and digital signatures on components that should not change. As cryptographic key management and rotation is difficult, cryptographic keys for use with IMDs and IBNs have been proposed to be located on bracelets, traditional tattoos and "invisible" tattoos only visible under ultraviolet light [33], and might be derived from physiologic or biometric values sensed by the IMD.

4.5 Trusted Internal Devices: The IMD Hub

We conceive of a protective countermeasure in an implantable "IMD Hub" which would act as a central authentication gatekeeper and network switch for all IMDs in the IBN and bring the IBN towards a more traditional network

model. This hub might support the other IMDs by providing a centralized power source and network connection bridged to the outside world, or by acting as a mobile but "always on" base station. The centralized power source would allow for increased lifespan in the face of power-draining attacks, a single location to apply inductive charging, to place a glucose energy harvester [11], or to attach semi-replaceable implanted batteries[4]. The fact that this IMD hub provides a single point of failure is a concern, and more research would be required to develop a redundant and robust hub (such as connecting together two hubs that would fail over to one another) that doesn't *decrease* the security and safety of the IBN.

4.6 Context awareness

As discussed at some length in Section 3.3.3, by making the IMD aware of a particular state in the patient or environment and restricting behavior based on that state, a powerful protective mechanism becomes available to any IMD that can include the necessary sensors [30, 16]. At a basic level, an IMD can be configured to only accept programming if a required state is present. A programmer for a cochlear implant might use a "control tone" or audible trigger to initiate programming mode if that simplified the configuration of the IMD. Note that in closed-loop systems, an IMD's assessment of the patient's environment and the actions it takes as a result may introduce safety and liability concerns if the "wrong" decision is made and the patient experiences an adverse effect.

4.7 Shielding

Shielding is a simple protective countermeasure to secure the communications of an IMD against passive or active radio frequency attack or electromagnetic interference. This countermeasure works by attenuating the signal and preventing (or significantly hampering) the communications of the IMD with devices outside of the IBN. One example is shielded clothing (like an undershirt or jacket) or shielded bandages, both of which are lightweight, easily removed in an emergency situation, and probably acceptable to most users. Shielding would defend against all wireless communication attacks that do not require physical contact with the patient.

4.8 Subcutaneous button

We propose implanting an unobtrusive but accessible subcutaneous button or switch on the patient which allows for programming for a period of time after it is pressed. This countermeasure would be analogous to the magnetic "reed switch" used in many pacemakers, but not susceptible to magnetic or radio frequency interference, as it would be tethered to an IMD by a wire. This switch might, however, be vulnerable to inadvertent activation, so proper design and placement would be important to avoid exposing the IMD to unauthorized reprogramming, though we make no claims about the medical feasibility of such a button. This protective countermeasure would protect all communications from the IMD to the outside world from any attack not requiring direct physical contact with the patient.

[4]That is, theoretical batteries which are implanted just under the skin and can be easily surgically removed and replaced.

5. CONCLUSIONS AND FUTURE DIRECTIONS

We described a classification which can be used to classify security vulnerabilities in IMDs which in turn can help to better select appropriate countermeasures to protect the IMDs. We also introduced novel countermeasures including specific context sensitivities, shielding, IMD hubs, and tethered analog switches. A legitimate criticism of a work like this might be to point out that the vulnerabilities described herein bear no resemblance to current IMD technologies. While current IMDs may not behave in the complex ways that we have considered, we have chosen to extrapolate their capabilities so that we can predict the *sort* of countermeasures that will be required for future IMDs. As more threats to and vulnerabilities in IMDs are discovered, this classification scheme can be refined and improved to more accurately reflect the landscape of IMD applications. Further research into this topic might also encourage IMD manufacturers to document and implement countermeasures appropriate to each category of vulnerability present in their devices. The manufacturers might also publish disclaimers describing controls that may be required to protect against low-probability or out-of-scope events that the device itself does not handle. The IMD-manufacturing industry might also agree upon a standard for IMD security mechanisms analogous to those developed by bodies like the UL [36].

We are interested in more fully developing the countermeasures we have only briefly mentioned, in particular determining the feasibility of routing IBN traffic through redundant implanted routers, how effective clothing-based shielding can be, and what other sorts of context sensitivity one might install in an IMD. Another future direction we would like to explore is the construction of a web site that tracks IMD vulnerabilities and offers resources and advice to patients, doctors, and device engineers.

6. ACKNOWLEDGEMENTS

Thank you to the anonymous reviewers for their valuable insights into the earlier draft of this paper.

7. REFERENCES

[1] T. Aslam. *A Taxonomy of Security Faults in the UNIX Operating System*. PhD thesis, Purdue University, August 1995.

[2] T. Aslam, I. Krsul, and E. H. Spafford. Use of a taxonomy of security faults. In *Proc. 19th NIST-NCSC National Information Systems Security Conference*, pages 551–560, 1996.

[3] S. Baskiyar. A real-time fault tolerant intra-body network. *IEEE Conference on Local Computer Networks*, 0:0235, 2002.

[4] S. Bergamasco, M. Bon, and P. Inchingolo. Medical data protection with a new generation of hardware authentication tokens. In *Mediterranean Conference on Medical and Biological Engineering and Computing (MEDICON)*, pages 82–85, Pula, Croatia, 2001.

[5] M. Bishop. A taxonomy of UNIX system and network vulnerabilities. Technical Report CSE-95-10, Department of Computer Science, University of California at Davis, 1995.

[6] M. Bishop and D. Bailey. A critical analysis of vulnerability taxonomies. Technical Report

CSE-96-11, Department of Computer Science, University of California at Davis, September 1996.

[7] K. Bourzac. Implantable silicon-silk electronics. *Technology Review*, November 2009.

[8] G. S. Brindley, C. E. Polkey, and D. Rushton. Sacral anterior root stimulators for bladder control in paraplegia. *Paraplegia*, 6(20):365–381, 1982.

[9] H.-J. Chae, D. J. Yeager, J. R. Smith, and K. Fu. Maximalist cryptography and computation on the WISP UHF RFID tag. In *Proceedings of the Conference on RFID Security*, July 2007.

[10] A. Y. Chow, V. Y. Chow, K. H. Packo, J. S. Pollack, G. A. Peyman, and R. Schuchard. The artificial silicon retina microchip for the treatment of vision loss from retinitis pigmentosa. *Archives of Ophthalmology*, 122(4):460–469, 2004.

[11] P. Cinquin, C. Gondran, F. Giroud, S. Mazabrard, A. Pellissier, F. Boucher, J.-P. Alcaraz, K. Gorgy, F. Lenouvel, S. Mathé, P. Porcu, and S. Cosnier. A glucose biofuel cell implanted in rats. *PLoS ONE*, 5(5):e10476, 05 2010.

[12] T. Denning, A. Borning, B. Friedman, B. Gill, T. Kohno, and W. H. Maisel. Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In *Conference on Human Factors in Computing Systems*, 2010.

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

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

[15] B. Glenville and D. Ross. Ventricular assist devices. *British Medical Journal*, 292:361–362, February 1986.

[16] S. K. S. Gupta, T. Mukherjee, and K. Venkatasubramanian. Criticality aware access control model for pervasive applications. In *PERCOM '06: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, pages 251–257, Washington, DC, USA, 2006. IEEE Computer Society.

[17] J. Halamka, A. Juels, A. Stubblefield, and J. Westhues. The security implications of VeriChip cloning. *Journal of the American Medical Informatics Association*, 13(6):601–607, 2006.

[18] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing, Special Issue on Implantable Electronics*, January 2008.

[19] Hobbit. The ftp bounce attack, July 1995. `http://nmap.org/hobbit.ftpbounce.txt`.

[20] D. Hollingworth. Towards threat, attack, and vulnerability taxonomies. In *IFIP WG 10.4 Workshop of Measuring Assurance in Cyberspace*, June 2003.

[21] I. V. Krsul. *Software vulnerability analysis*. PhD thesis, Purdue University, West Lafayette, IN, USA, 1998.

[22] C. E. Landwehr, A. R. Bull, J. P. McDermott, and W. S. Choi. A taxonomy of computer program security flaws, with examples. Technical report, Naval Research Laboratory, November 1993.

[23] J.-C. Laprie. From dependability to resilience. In *38th IEEE/IFIP International Conference On Dependable Systems and Networks (DSN 2008 - Fast Abstracts)*, pages G8–G9, June 2008.

[24] S. Lee, K. Fu, T. Kohno, B. Ransford, and W. H. Maisel. Clinically significant magnetic interference of implanted cardiac devices by portable headphones. *Heart Rhythm*, October 2009.

[25] N. G. Leveson and C. S. Turner. An investigation of the Therac-25 accidents. *Computer*, 26(7):18–41, 1993.

[26] D. L. Lough. *A taxonomy of computer attacks with applications to wireless networks*. PhD thesis, Virginia Polytechnic Institute and State University, 2001. Chairman-Davis,IV, Nathaniel J.

[27] M. Mirowski, M. M. Mower, W. S. Staewen, B. Tabatznik, and A. I. Mendeloff. Standby Automatic Defibrillator: An Approach to Prevention of Sudden Coronary Death. *Arch Intern Med*, 126(1):158–161, 1970.

[28] NHS National Research Ethics Service. Approval for medical devices research, 2008. `http://www.nres.npsa.nhs.uk/EasySiteWeb/GatewayLink.aspx?alId=11473`.

[29] R. B. North, D. H. Kidd, M. Zahurak, C. S. Jones, and D. M. Long. Spinal cord stimulation for chronic, intractable pain: Experience over two decades. *Neurosurgery*, 32(3):384–395, 1993.

[30] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun. Proximity-based access control for implantable medical devices. In *CCS '09: Proceedings of the 16th ACM conference on Computer and communications security*, pages 410–419, New York, NY, USA, 2009. ACM.

[31] J. Robert E Morley and E. J. Richter. Final report on measurements of static electricity generated from plastic playground slides, March 2006. `http://www.access-board.gov/research/play-slides/report.htm`.

[32] G. Santhanam, S. I. Ryu, B. M. Yu, A. Afshar, and K. V. Shenoy. A high-performance brain-computer interface. *Nature*, 442(7099):195–198, 2006.

[33] S. Schechter. Security that is meant to be skin deep: Using ultraviolet micropigmentation to store emergency-access keys for implantable medical devices. Technical Report MSR-TR-2010-33, Microsoft Research, April 2010.

[34] D. Song, R. H. M. Chan, V. Z. Marmarelis, R. E. Hampson, S. A. Deadwyler, and T. W. Berger. 2009 special issue: Nonlinear modeling of neural population dynamics for hippocampal prostheses. *Neural Netw.*, 22(9):1340–1351, 2009.

[35] F. T. Sun, M. J. Morrell, and R. E. Wharen. Responsive cortical stimulation for the treatment of epilepsy. *Neurotherapeutics*, 5:68–74, January 2008.

[36] Underwriters Laboratories. UL Standards for Safety, 2010. `http://www.ul.com/global/eng/pages/corporate/standards/`.

[37] C. Vanden Berghe, J. Riordan, and F. Piessens. A vulnerability taxonomy methodology applied to web

services. In *Proceedings of the 10th Nordic Workshop on Secure IT Systems*, 2005.

[38] M. Velliste, S. Perel, M. C. Spalding, A. S. Whitford, and A. B. Schwartz. Cortical control of a prosthetic arm for self-feeding. *Nature*, 453(7198):1098–1101, May 2008.

[39] World Health Organization. ICD-10 : international statistical classification of diseases and related health problems, 2007. `http://apps.who.int/classifications/apps/icd/icd10online/`.