Security that is Meant to be Skin Deep

Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices

Stuart Schechter
Microsoft Research
StuS@microsoft.com

Abstract

Implantable medical devices, such as implantable cardiac defibrillators and pacemakers, now use wireless communication protocols vulnerable to attacks that can physically harm patients. Security measures that impede emergency access by physicians could be equally devastating. We propose that access keys be written into patients' skin using ultraviolet-ink micropigmentation (invisible tattoos).

1 The IMD Key Storage Problem

Life-critical implantable medical devices (IMDs) are becoming increasingly commonplace. The most familiar, the pacemaker, is implanted into a million patients each year [11] and generates $1.98 billion for market leader Medtronic alone [10, p22]. Implantable cardiac defibrillators (ICDs) grew in popularity starting in 1990 [8]. Recently, researchers have raised concerns about IMDs use of wireless protocols; the of lack authentication and integrity mechanisms put patients at risk from attack by anyone with a transmitter [5, 6, 7].

Cryptographic authentication and integrity-protection would require an access key available to authorized physicians but not attackers. In emergencies, patients may require the care of physicians not previously authorized to access the device. Emergency physicians cannot rely on patients to be conscious to provide access keys.

RFID tags, such as the VeriChip [13], cannot be used to store access keys as they provide no defense against malicious key requests. Access keys could be stored on medical bracelets, as are used to disclose conditions such as diabetes in emergencies [7]. Denning *et al.* proposed a medical bracelet that would prevent access to IMDs when worn and that would be removed in an emergency [3, 4]. Regardless of whether bracelets provide or prevent access, patients may lose or forget these bracelets and the mere presence of a bracelet reveals a patient's condition to potential attackers.

2 Encoding keys as UV-Ink Tattoos

We propose that a user-selected human-readable key be encoded directly onto patients using ultraviolet-ink micropigmentation, adjacent to the point of implantation. To increase reliability the encoding could be augmented to include an error correcting code and/or be replicated in full on the base of the patient's leftmost foot—at the arch. All devices used to communicate with the IMD would be equipped with a small, reliable, and inexpensive ultraviolet light emitting diode (UV LED) and an input mechanism for key entry (a keypad or touch-screen). A single key would be sufficient for multiple devices and could be re-used when devices are replaced.

The key encodings could take the form of user chosen character strings (optimizing for user choice), random character strings (optimizing for minimal size), or strings of hieroglyphic-like images chosen from a subset deemed acceptable to the user. The first option gives the greatest control to reluctant patients, whereas latter two options guarantee a minimum level of key entropy and can easily be augmented with error correcting codes. Each patient would be allowed to request new random encodings until finding one he or she deemed acceptable.

3 Safety, security, and reliability

The biggest safety concern with UV micropigmentation the UV ink formulations used in tattoo's today have not yet been sufficiently refined to minimize skin irritations and proven free of long-term health risks [12].

Unlike bracelets, UV micropigmentation does not advertise the presence of the IMD to potential attackers. When not covered by clothing, the UV ink can be hidden by UV-blocking sunscreen. Anyone close enough to read a patient's tattoo is already close enough to harm the patient using other forensically untraceable mechanisms.

Also unlike bracelets, patients cannot forget their tattoo. Placing micropigmented encodings adjacent to scars makes them easy to find. Error correcting codes and a redundant copy on the foot protect against readability failures resulting from changes in the skin. Using a human-readable encoding ensures that patients' can detect if bodily changes render their tattoos unreadable.

A human readable encoding is a business necessity for device makers, even if these encodings can often be scanned and read automatically. Verifying that devices can read encodings on a sufficiently diverse sample of human flesh is impractical. If a machine-readable encoding cannot be read, and there is no alternative, the device manufacturer will inevitably face a loss-of-life lawsuit. If a human-readable encoding degrades to the point where it can no longer be read by a doctor, the manufacturer of the reader is unlikely to be deemed responsible.

4 Patient-acceptability

One attractive feature of UV micropigmentation is that it requires no day-to-day effort or notice from the patient, except (perhaps) more attention to the use of sunscreen.

Pain and the risk of infection might be among patients' immediate concerns. In most cases, patients will already be undergoing local or general anaesthesia to receive the implantation. Patients may also be receiving painkillers that would minimize any residual pain following micropigmentation. The risk of serious infection due to a surgically-performed skin-deep tattoo should be significantly lower than that from the more intrusive implantation of a device.

Like pain, the perceived permanence of a invisible writing should be small in comparison to the impact of the implantation: a visible scar.

Patients may have cultural concerns that arise from perceptions of tattoos as signals of low socioeconomic status, affiliation (e.g. motorcycle gangs), or youthful short-sightedness. Patients may recall the use of tattoos to identify prisoners during the holocaust or to identify citizens in depictions of dystopian futures.

The invisibility of UV micropigmentation under normal lighting reduces the likelihood that it will be a signal detectable by others. If others do use it as a social signal, its association with body-art tattoos can be reduced by maximizing the difference in appearance, and terminology, between these tattoos and medical micropigmentation. Establishing medical micropigmentation as a social norm for IMD patients should also help; the first set of patients to receive them may be informed that medical tattoos have been in use for over half a decade to disclose patient conditions [1, 2, 9].

The use of UV ink may be of less consolation to those patients who associate tattoos with their use as involuntary identifiers. In the holocaust, identification tattoos reminded prisoners no longer controlled their own bodies. Giving the patient a choice of whether or not to use micropigmentation, the type of encoding to use, and some control over the process that generates the encoding should help to address these concerns.

To make an informed choice, patients will need to know the benefits and risks of both UV micropigmentation and the alternatives. For example, patients should be provided with statistics on the risk of infection from micropigmentation and the risk that a tattoo could be rendered unreadable when needed. Patients should also be aware of the fraction of patients issued medical bracelets who arrive at emergency departments without them.

References

[1] Saleh A. Aldasouqi, Ahmad Sheikh, and Pamela Klosterman. Tattoos as medical alerts. In *Proceedings of the American Association of Clinical Endocrinologists 18th Annual Meeting & Clinical Congress: Exploring New Frontiers in Endocrinology*, Houston, TX, May 13–17, 2009.

[2] Kimberly Berryman. Tattoos as medical warning: Some diabetics opt for warning tattoos; Docs still stand behind bracelets. *ABC News*, December 20, 2007.

[3] Tamara Denning, Alan Borning, Batya Friedman, Brian T. Gill, Tadayoshi Kohno, and William H. Maisel. Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In *Proceedings of the 28th ACM Conference on Human Factors in Computing Systems (CHI 2010)*, Atlanta, GA, April 13, 2010.

[4] Tamara Denning, Kevin Fu, and Tadayoshi 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.

[5] Kevin Fu. Inside risks, reducing the risks of implantable medical devices: A prescription to improve security and privacy of pervasive health care. *Communications of the ACM*, 52(6):25–27, June 2009.

[6] Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing, Special Issue on Implantable Electronics*, January 2008.

[7] Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proceedings of the 29th Annual IEEE Symposium on Security and Privacy*, 2008.

[8] William H. Maisel, Megan Moynahan, Bram D. Zuckerman, Thomas P. Gross, Oscar H. Tovar, Donna-Bea Tillman, and Daniel B. Schultz. Pacemaker and ICD generator malfunctions. *Journal of the American Medical Association (JAMA)*, 295(16):1901–1906, 2006.

[9] Mary Brophy Marcus. Tattoos being used for medical alerts. *USA Today*, May 14, 2009.

[10] Medtronic Corporation. 2009 Annual Report. `http://www.medtronic.com/temp/2009/annual-report/medtronic-2009-annual-report.pdf`.

[11] Janet Moore. Making pacemakers MRI-friendly. *Star Tribune*, March 7 2010.

[12] TattooHealth.org Staff. Ultraviolet tattoos. `http://www.tattoohealth.org/content/uv.asp`, Archived 2010/3/16.

[13] VeriMed Patient Identification. Keeping you and your patients connected. `http://www.verimedinfo.com/for_physicians.asp`, Archived 2010/3/16.