Human RFID Implants: The Good And Bad

ECE 390 - Engineering Ethics and Professionalism

Robert Billette

February 12, 2019

BACKGROUND

We live in a complex technological universe where it seems a new device is spawning every day. For every new device there exists a thousand applications, and for every application, an ethical dilemma. Engineers are constantly faced with decisions that challenge their moral compass. When faced with such a dilemma engineers must weigh their options, consider the ethics of every option, and act accordingly. In reality, it is not so black and white. Every person has a unique set of moral values and code of ethics. For this reason, in professional practice, Electrical Engineers must adhere to the clearly defined standards of the IEEE code of ethics. Ethical dilemmas can evolve in the wake of consequential, potentially world changing technologies. Here we will observe and analyze one specific engineering development that walks the line between greatness and catastrophe.

RFID is by no means a new technology. Radio Frequency Identification has been around for decades being used for tagging livestock, tracking wildlife, and identifying credit cards. It is much more prevalent than what most people expect, being used by distributors for inventory tracking, and airlines for luggage tracking.[1] The success of RFID applications leads engineers and entrepreneurs to ask, naturally, if this can be used in humans. Human RFID implants could be the most powerful application yet. From medical monitoring to wave-of-the-hand purchases, the technology holds obvious conveniences, but it's intrusive nature could leave users feeling invaded and generates much controversy.

TECHNICAL USES AND CONCERNS

The primary motivation for RFID implantation is Identification and Authentication (I&A).[3] The identification process involves translating the user's unique identity, while the authentication process involves verifying the identity. In common consumer systems, I&A is completed using a username and password, some systems use tokens; an object such as an ID badge, while others use biometrics, such as a fingerprint. In all of these circumstances, the I&A process is not immediate, nor is it automatic. One of the key benefits of RFID implants is that it does not require the user to complete a specific action, carry an object, or take any time to complete the action. The process is nearly immediate (relative to the typing of a username and password) and automatic, simply existing in the vicinity of the system being accessed will provide I&A.[3] The dominant concern surrounding the application of any I&A mechanism is safety and security. The nature of the RFID implant can lead to improved security in many domains. The embedded chip can be used as a replacement for credit cards, ID badges, and other tokens, making it

impervious to misplacement or theft. The chip is also automatic, which eliminates any need to memorize passwords, swipe a finger, and is highly reliable.[3]

However, threats to user security do exist. Consider VeriChip, the first FDA approved human implantable chip, produced by Applied Digital Solutions. The only information contained on the chip is the user ID. The memory is large enough to hold an appropriate length ID for every human in the world to have a unique ID. The chip does not store any personal data related to the chip holder, instead the personal data is stored in a centralized database, along with every other chipholder.[3] Sure, this reduces the likelihood of an individual's identity theft, but if the centralized database is hacked, or information is leaked, this would compromise every chip holders personal data. This has potential to be a major threat to the collective privacy of any consumer donning a RFID chip. Another consequence of memory and hardware constraints is the inability to create RFID chips with advanced ID encryption and authentication techniques. This leaves them potentially susceptible to ID theft through attacks, such as a relay attack. In a relay attack, a thief can scan a user's RFID tag using a fake reader, relay the data to a fake tag at any distance, then use the fake tag to authenticate the user. Relay attacks have been successfully executed and proven by researchers on an ISO-14443A-compliant RFID system.[4]

BIOCOMPATIBILITY CONCERNS

Regarding the technical concerns engineers are faced with when developing RFID implants, security is paramount, however, the biological safety of an implant to remain in a users body tissue for years is also of considerable importance. As noted by the FDA, risks to health generally associated with the use of implantable RFID systems include: adverse tissue reaction, migration of implant, electrical hazards, and MRI compatibility.[6] Depending on the size, method of insertion, and design of the chip, all or none of these risks may be mitigated. Some critics claim the chip leads to increased risk of cancer, as lab tests have demonstrated this trend in animals, however, there is no conclusive evidence of such a risk for humans.[3] Regardless, there are still biocompatibility concerns regarding RFID implants that need to be addressed, both through engineering and legal policy, to ensure the comfort and satisfaction of consumers.

ETHICAL CONSIDERATIONS FOR MITIGATING MISUSE

The above issues of safety and security are complex technical issues that require the person or group that solves them to have expertise and proficient knowledge on their details of operation and critical failure points. The people who hold these skills and knowledge are the engineers who are currently developing RFID technology. Thus, it is essential that engineers have a role in shaping discussions regarding the use of RFID implants. When it comes to the discussion of security, biocompatibility, tracking and surveillance, implementation, and even removal, engineers should posses the responsibility in deciding how every procedure is executed. Consider a large company that sells implants to consumers as a replacement for a credit card. With proper legislation and disciplinary action, the company's actions and use of data can be regulated and kept within legal (and hopefully ethical) limits. However, if the government were to implement RFID chips, the only thing regulating the government is the government. They can and will do anything they please, and will certainly get away with it. There is no regulating factor for the actions of a standalone government body that has the data and location of 300 million citizens. It is for this reason that engineers must have a critical position in defining the ethical issues surrounding this device. If the engineer can properly design a product with ethical considerations, one that has very little potential for misuse, then there leaves hardly a chance for a powerful body to abuse such a product. The engineer can enable or prevent any foreseeable outcome, and it is imperative they act ethically.

Of course, an obvious deterrent for any unethical use of an RFID implant is legal policy. Laws should and will be administered to specify privacy guidelines to be used by companies, prohibit unauthorized tracking of users, and give users the ultimate control of their privacy. As the European Group on Ethics in Science and New Technologies (EGE) states, users have “the right of informational self-determination on each individual – including the right to remain master of the data concerning him or her”.[5] In essence, lawmakers and politicians will have to act ethically and aptly to propose policies to ensure the privacy of users.

Additionally, there are economic considerations to be made when creating privacy laws on RFID. Data mining can be used for analysis of consumer habits and behavior, giving businesses the ability to create personalized products, advertisements, and services.[3] At first, this seems no different than the cookies stored on internet browser data, but remember, an internet user can disable cookies at any time. It is much less convenient to disable the RFID chip in a user’s arm, unless they want to walk around with tin foil over their implantment site. This poses the question of whether legislation will need to be created in the future for data protection.

By far, the most controversial use of RFID implants in humans is location tracking.[2] Location tracking has an air of dystopia to it. With the nearly omnipresent existence of computers, a surveillance society from George Orwell's *1984* could become a thing of reality. Science fiction aside, location tracking is a huge threat to personal privacy, and must be addressed with sincerity. With large scale tracking, we become susceptible to stalking, government control, and involuntary privacy intrusion. Again, engineers, lawmakers, and businessmen will all need to contribute to this legislation, as it affects every sector of society.

CONCLUSION

The benefits and conveniences of RFID implants are undoubtedly clear, but so are its vulnerabilities. The ethical dilemma associated with the development of RFID implants is also clear. As engineers, we have to ask ourselves what the implications of each outcome are. Luckily we have the IEEE code of ethics to help us, and ideally, our own moral autonomy should align closely with the required ethical practices of a professional engineer. The FDA approved VeriChip has been implanted in thousands of users. The Swedish company BioHax says 3,000 chips have been implanted in customers.[8] There is definite evidence that the popularity of this tech is rapidly increasing, and will continue to grow more even more popular. As evidenced in this document, the safety and welfare of the consumer is held paramount. An FDA approved chip is a prime example of this adherence to IEEE code of ethics. Additionally, after extensive research on the literature and documentation of RFID chips, it can be said that efforts have and are being made to improve the public understanding of these devices, another hallmark of the code of ethics.[7]

The smart environment we live in today is in every way intended for the betterment of our society, the improved convenience of daily labours, the monitoring of our health, and to facilitate joyous moments into our lives. Technology brings people closer, it helps form relationships, it solves problems, it saves lives, it changes the world. But with every great revolution, there is potential for destruction. As engineers, we must be cognisant of ethical issues surrounding our work, for adverse results can be disastrous. We must be cautious and foresightful, to keep the peace, and to keep technology on our good side.

REFERENCES

1. Weiss, Haley. “Why You’Re Probably Getting a Microchip Implant Someday.” *The Atlantic*, 21 Sept. 2018.
2. Labay, Vladimir, and Amber Mckee Anderson. “Ethical Considerations and Proposed Guidelines for the Use of Radio Frequency Identification: Especially Concerning Its Use for Promoting Public Safety and National Security.” *Science and Engineering Ethics*, vol. 12, no. 2, 2006, pp. 265–272., doi:10.1007/s11948-006-0026-7.
3. Rotter, P., et al. “RFID Implants: Opportunities and and Challenges for Identifying People.” *IEEE Technology and Society Magazine*, vol. 27, no. 2, 2008, pp. 24–32., doi:10.1109/mts.2008.924862.
4. P. Rotter A Framework for Assessing RFID System Security and Privacy Risks. IEEE Pervasive Computing, Vol. 7, no. 2, April-June 2008, pp. 70-77
5. European Group On Ethics In Science and New Technologies. “Ethical Aspects of ICT Implants in the Human Body.” *Jahrbuch Für Wissenschaft Und Ethik*, vol. 10, no. 1, 2005, doi:10.1515/9783110182521.501.
6. Center for Devices and Radiological Health. “Class II Special Controls Guidance Document: Implantable Radiofrequency Transponder System for Patient Identification and Health Information - Guidance for Industry and FDA Staff.” *U S Food and Drug Administration Home Page*, Center for Drug Evaluation and Research, www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm072141.htm.
7. “IEEE Code of Ethics.” *IEEE - Advancing Technology for Humanity*, www.ieee.org/about/corporate/governance/p7-8.html.
8. Graham, Jefferson. “You Will Get Chipped - Eventually.” *USA Today*, Gannett Satellite Information Network, 10 Aug. 2017, www.usatoday.com/story/tech/2017/08/09/you-get-chipped-eventually/547336001/.