Borui Wang
ESL118 Section 005
Mr. Terry B Nuckolls
IRP Final Draft
April 19th, 2010

Implantable RFID Technology: Not yet Ready for Its Mission

Imagine a single device that can store and link to information about one's identity, physiological characteristics, health status, nationality, and security clearances, or can start a car, unlock the front door, let an emergency room physician know a patient is a diabetic even if the patient is unconscious. A device like this was developed just several years ago. It is a very tiny chip called the implantable radio frequency identification (RFID) tag that can be implanted inside one's body. Once implanted, the chip and the information it contains are always with the implantee, and the chip carrier would never lose his important information again.

In 2004, the U.S. Food and Drug Administration, the organization that regulates medical devices in the United States, approved one kind of implantable RFID tag called VeriChip which is at present the only approved implantable chip for use in humans ("FDA approves," 2004). VeriChip is a simple device consisting of an antenna encapsulated in a glass sleeve and does not include any battery. It uses any RFID scanner's magnetic field as the power source and transmits data through its radio signal. Each VeriChip's signal is embedded with a unique identifying number that connects to a database, which includes information linked with the number (Foster & Jaeger, 2007, p.26). By 2005, there were fifty million house pets implanted with RFID tags to

help them return to their owners when they're lost (Juels, 2005, p.2), and about 2000 people already have VeriChips implanted in their bodies (Foster & Jaeger, 2007, p.27). Although the many potential use in healthcare, emergency, financial, and security applications, various undesirable sides of implantable RFID technology were found in recent years. RFID tags should not be implanted into the human body because RFID tags erode the personal right of privacy, because the RFID signal and data system is technically unreliable and insecure, and because RFID implants can induce serious health problems.

People who carry implanted RFID tags face serious privacy threats and may not be able to control the use of their personal information. Without the knowledge of what the RFID information system is actually gathering via the implants, implantees are not aware of the unauthorized readings from the RFID tags, which erode their privacy. Since RFID tags respond to scanner interrogation without alerting their owners, personal information, including medical records, financial reports , Social Security Numbers or even lifestyle preferences of the tag owner can be collected, refined, and exploited all under the excuse of customer relationship management (CRM) (Michael and Michael , 2004 p.4). The personal information gathered via RFID tags can be systematically categorized to determine commercial valuable variables. Michael and Michael point out that it is not difficult to derive telemarketing lists and census information aggregated to an individual level from the RFID database and convert these data to represent market interests. Michael and Michael conclude that disclosing or abusing sensitive

private data obtained from the database through implanted RFID tags would have devastating impact on civil liberties (p.4).

Other than by analyzing personal information with data gathered from RFID signals, breaches of personal information can also happen on a more comprehensive level by the tracking of individuals with RFID implants. Research by Masters and Michael (2006) suggests that implanted RFID tags can be continuously visited by any amount of readers they passes by at all times, and this gives the possible result of gaining the ability to build connections between the information from the chip implant with the physically location of an individual, and to track and investigate a individual's pattern of habits and behaviors (p.35). They are concerned that the violations to personal privacy become more intolerable as information gathered for one purpose is used to track and record completely separate information gathered for another purpose, such as utilizing the same data originally collected from the payments received from implanted drivers as they drive through sensor-based road toll stations to detect possible illegal driving speeding for the automatic issue of fines (p.36). Master and Michael further point out that such way of data gathering, where an implanted person must have their personal information disclosed to data gathering devices in order to get access to a particular service, negates the fundamental view of privacy and ‘‘an individual having the right to control the use of his information in all circumstances’’ (cited in Master and Michael, 2006, p.36).

Implanting RFID chips in people not only raise the concern of the possible invasions of privacy by corporations, but also raise the fear of potentially empowering the government to turn

the advanced technology into a way of watching and tracking people in the future. Albrecht (2005), who describe RFID tags as spy chips, suggests the potential that the power of RFID technology could be controlled by global corporations and government bureaucracies and "strip away the last shreds of privacy we have left," and its power of tracking, recording, and revealing could ultimately enslave people (P.12). According to Albrecht, the government could follow the signal from the RFID tags to track suspicious person who are wearing or carrying RFID chips in public areas, and he argues that if the government has the ability to track chip implanted people are regarded suspicious, it can track everyone else with RFID tags implanted as well (p.35). In fact, The U.S. Department of Homeland Security (DHS) is actively searching for improved RFID technology that can read feedback signals from up to 25 feet away, precisely locate pedestrians on street corners, and even catch the identity of people moving by in cars at 55 miles per hour ("Homeland Security2006). The government may further use the RFID system as a new surveillance system and look over its people in a much more silent and precise ways. In fact, the nature of RFID chips implanted beneath the skin gives individuals no ability to know when their implants are transferring data and when they are not, which impairs people's ability to control the information flows from the device and in what way the data is used.

Another major reason for not using RFID chips inside humans is that the technical weaknesses of RFID signal and database systems make commercial use of implantable RFID insecure and unreliable. A study by Halamka, Juels, Stubblefield, and Westhues (2006) finds that that the commercial implantable RFID tag VeriChip is vulnerable to be cloned and attacked , and

they point out that an attacker can attack the commercial VeriChip system by secretly intercepting a VeriChip ID and reproducing or replaying its signals with a trivial and cheap process (p.604), but the consequences of attacking and copying signals for payment or validation-control systems that rely on VeriChip systems are serious (p.606). Furthermore, putting a security identification system inside human body incurs the possibility of the physical body being attacked. Halamka et al. note that no matter how the identification systems are designed, implantable RFID tags should be used only for identification but not authentication purpose since there would be higher incentives for adversaries to commit physical attacks against implantees in order to extract their implanted tags for identification purpose (p.602). Considering over-the-air attacks and the possibility of even physically "hacked," RFID tags put users' information and their own bodies in insecure situations that are not acceptable at all.

Even if RFID signals are safe and secure, they bear another technical issue of interfering and reacting with other medical devices, which could cause potential hazards. The research by Vandertogt et al. (2008) reveals that RFID tags, which are increasingly being used in hospitals to identify patients and track medical supplies, can interfere with medical equipment, such as pacemakers and ventilators (p.2884). They tested a total of 41 medical devices such as ventilators, syringe pumps, dialysis machines and pacemakers, and found passive RFID signal interfered with 26 medical devices, of which 22 cases were classified as hazardous (p.2888). Vandertogt et al suggest more strict and careful management of RFID communication systems is required in areas that include extensive amount of electronic critical life-supporting medical

devices (p.2889). The finding implies that using RFID system in places where intensive RFID-incompatible medical devices which are used could impact the device users disastrously, and even put their safety and lives at risk. This intrinsic weakness of RFID signals may greatly limit the use of RFID systems in many fields that require higher standard of signal design.

Implantable RFID system is not only unsecure and unreliable with respect to the signal transfer level, it also faces security threats in its database, the place where the personal data are ultimately stored. Like any other computer database, the information database linked by RFID tags can be attacked or disturbed. Researchers at Vrije University Amsterdam suggest that the vulnerability of RFID system can be exploited by database attack (cited in Kirk, 2006). And special intended RFID tags can be embedded with malicious code to visit a Structured Query Language (SQL) RFID database and injected codes into the database (Kirk, 2006). These technical problems cannot guarantee RFID system as a trustworthy solution for personal identification, and the service provider, as well as the clients, will face a huge loss if any part of the RFID system is attacked or their data is lost.

RFID tags should not be implanted into human body for another crucial fact that the implanted tags are not totally free of health risks and can lead to serious health hazards. When FDA approved the request of marketing VeriChips , it used the term “adverse tissue reaction” as one of the potential risks to health associated with the tag (U.S. Food and Drug Administration,2004). But the health risk is actually underestimated. In the lab experiments on mice, Elcock et al. (2001) found tumors circling around implanted microchips developed at the

occurrence rate of about one percent in the second year of experiment (p.483). They used implantable microchip consisting of a tiny cylindrical signal device encapsulated in a bio-compatible glass in the experiments (p.484) and found that “malignant schwannoma”, the most common tumor in the nerve system arising from foreign bodies, developed in a rapid growth rate, and killed the rats in several weeks (p.491). Blanchard et al. (1999) suggests that the implanted radio transponder identification device, which is composed of an identification chip encased in a smooth glass sleeve, induce sarcoma, a common cancer affecting tissues such as muscle and bones in an experiment on rats, (p.519). The identification devices used in both experiments by Elcock et al. and Blanchard et al. have the very similar structure to commercial VeriChips implanted in humans. Although the rate of the occurrence of the tumor is relatively low, the study raises the red flag of the possibility of tumor after having foreign bodies left in people.

Besides the risk of tumor raised from the direct contact between the implant body and animal tissue, another study suggested that the signal radiated from the RFID implants may cause thermal assault on animal organisms. According to Covacio (2003), implanted microchips emit radio frequency radiation to the chip recipients, which may cause many adverse biological effects, such as DNA damage and heat shock protein response and thermal effects, such as thirst, coma and possible death (p.849). He points out that recent research in RFID has led to an increasing concern with the adverse impact of non- ionizing radiation on organic matter from different radio signal frequencies, and research has discovered that multilevel risks are associated

with the implementation of radio frequency identification technology in humans (p.845). It seems that radiation from RFID implants poses further threat to the health of implantees, and using such a radiation source inside one's body as an identification device is not a convincing idea.

Some disagree that RFID tags raise serious privacy issues and argue that the privacy concerns of using RFID tags are exaggerated. Brito (2004) claims that the owner of the RFID tags have no need to worry about their RFID signals being tracked or intercepted because the technical constraints of RFID signals are not likely to make such a situation occur. He suggests that although the signals sent from the reader can reach RFID tags from several hundred meters away, the feedback signal of RFID tags can only be received within the range of twenty to thirty feet at most according to the Electronic Product Code (EPC) standard, and RFID signals cannot penetrate dense materials such as metal and liquids, which limit the read range of RFID signals even more (p.19).

Indeed, the limits to the range of the RFID readers can be exceeded and it's not hard to retrieve higher read range using higher power antennas or different RFID protocols. A study by Avoine and Oechslin shows that the limits of the reading range depend on standards and regulations, but it is not necessarily true that that the tags cannot be scanned from a greater distance (p.127). They suggest that using antennas equipped with high gaining power levels or unqualified reading devices still make a tag readable from greater distances, and using other signal source to neutralize or cancel out the targeted RFID signal can also disturb functionality of

the RFID system (p.128). Juels (2005) observed that there are several ways to significantly increase the reader-to-tag intercepting range. He suggests that with some RFID protocols, a powerful reader with much higher power can convey signals at much greater distances and boost regular distance of signal communications between tags and readers to even kilometers away (p.5). Recent development in the RFID system has also overcome the technical problem of transmitting RFID signals through liquid and metals. A dual-frequency RFID reading system that combines both low and high RFID signals can communicate with tags independent of the presence of metal, water and concrete, and such a system has been examined successfully scanning tags buried 20 meters under the ground on metal pipes (Collins, 2004). In brief, RFID signal systems can be altered and evolved to satisfy any need of tracking and locating tag carriers.

RFID implants still need much effort to become a mature personal identification device. Although initially it may seem that the human tagging system offers many benefits and convenience to human life, current RFID technology confronts multilayer issues of security, privacy and health problems and is far from being satisfactory. It is not that a new technology should not be accepted just because it is new, rather implantable RFID technologies must be fully examined to be reliable, secure and free of health risks before being put on the market.

Concerning data privacy and security, Wisconsin became the first state in the United States to ban coerced implants in humans (L. Songini, 2006); the law dictates that no one can implant RFID microchips into others without their consent, but volunteers for implants are not mentioned

in the law. Nevertheless, the law does not eliminate the situation in which a person has to voluntarily implant chips in order to get a job or meet a particular requirement of a service; thus, stronger laws should be adopted. Current RFID systems can not ensure a secure and safe way for personal identification and will face more issues or even complete corruption once being put into massive use. Therefore putting RFID tags in humans should not be conducted based on the present RFID systems, and similar ideas of tagging people using other chip devices should be carefully thought out in order to avoid the same problems as the implantable RFIDs currently have.

References

Albrecht K.,Mcintyre,L.(2005). *Spychips: How major corporations and government plan to track your every move with RFID*. New York: Thomas Nelson, Retrieved March 28th from http://books.google.com/books?hl=en&lr=&id=YDxDuMYVJdcC&oi=fnd&pg=PR9&dq=RFID+track&ots=bnNXfPGLJw&sig=NjIPu0Xs7MQRuRUWB0VI0_NVP9U#v=onepage&q=&f=false.

Avoine,G., Oechslin,P.(2005). RFID Traceability: A multilayer problem. *Springer-Verlag Berlin* 125-140.

Blanchard,K.T.,Barthel,C.,French,J.E.,Holden,H.E.,Moretz,R.,Pack,F.D.,Tennant,R.W., Stoll,R.E.(1999). Transponder-induced sarcoma in the heterozygous p53+/- mouse. *Toxicol Pathol, 27*(5) 519-527. Retrieved April 07,2010 from http://tpx.sagepub.com/cgi/content/abstract/27/5/519.

Brito J.(2004). Relax don't do it: Why RFID privacy concerns are exaggerated and legislation is premature. Federal Circuit Bar Journal, Retrieved April 6th 2010from http:// www.lawtechjournal.com/articles/2004/05_041220_brito.pdf.

Collins,J.(2004, September 1st) New Two-Frequency RFID system. *RFID Journal*, Retrieved April 16th, 2010 from http://www.rfidjournal.com/article/articleview/1105/1/1/.

Covacio,S.(2003, June). Technological problems associated with subcutaneous microchips for human identification, *Informing Science,*844-853.

Elcock,L.E.,Stuart,B.P.,Wahle,B.S.,Hoss,H.E.,Crass,K.,Millard,D.M.,Mueller,R.E.,Hastings,T.F.,Lake,S.G.(2001). Tumors in long-term rat studies associated with microchip animal identification devices. *Exp Toxic Pathol,52,* 483-491.

FDA approves computer chip for humans. (2004, October 13). *Msnbc.* Retrieved March 12th, 2010 from http://www.msnbc.msn.com/id/6237364/.

Foster,K.R., Jaeger,J. (2007), RFID inside: The murky ethics of implanted chips, *IEEE Spectrum*,24-29. Retrieved March 26th, 2010 from http://ro.uow.edu.au/infopapers/393.

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

Homeland security RFI Heightens public concern over FRID (2006, February 21). *The Spychips*, Retrieved March 12th, 2010 from http://www.spychips.com/press-releases/dhs-rfid.html

Kirk,J. (2006, March 15). RFID tags vulnerable to viruses, study says. *Computerworld*，Retrived April 12th , 2010 from http://www.computerworld.com/s/article/109560/RFID_tags_vulnerable_to_viruses_study_says?taxonomyId=17&pageNumber=1.

Juels (2005, September 28). RFID security and privacy: A Research Survey, *IEEE journal on selected areas in communications 24*(2), 1-19.

Masters,A., Michael,K.(2007). Lend me your arms: The use and implications of humancentric RFID. *Electronic Commerce Research and Applications ,6*,29-39. Retrieved March 12th from Science Direct database.

Michael,K., Michael,M.G.(2004). *The social, cultural, religious and ethical implications of automatic identification,* Paper presented at the Seventh International Conference in Electronic Commerce Research, Dallas, Texas, USA, 10-13 June, 2004, 433-450.

Morrissey, S. (2007, October 18). Are microchip tags safe? *Time*, Retrieved April ,1st 2010 from http://www.time.com/time/health/article/0,8599,1672865,00.html.

U.S. Food and Drug Administration (2004). *Evaluation of automatic class III designation VeriChip(TM) health information microtransponder system.* Washington,DC: U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES. Retrieved April 7th, 2010 from http://www.scribd.com/doc/22533693/FDA-Approval-VeriChip-RFID-Implant-Class-2-Device-12Oct04.

Vandertogt R.,Vanlieshout,E.J.,Hensbrock,R.,Beinat,E.,Binnekade,J.M.,Bakker,P.J.M. (2008, June 25). Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment, *Journal of the American Medical Association,299* (24),2884-2890.

Songini,M.L.,(2006, June 12).Wisconsin law bars forced RFID implants, *Computerworld,* Retrived March 19,2010 from http://www.computerworld.com/s/article/111542/ Wisconsin_law _bars_forced_RF ID_ implants.