https://doi.org/10.48009/2_iis_2007_336-340

RFID: A SURVEY OF ETHICAL AND PRIVACY CONCERNS

Joseph Francom, Kentucky Wesleyan College, jfrancom@kwc.edu

ABSTRACT

Radio Frequency Identification (RFID) has garnered much attention in recent years as a method of supplanting the barcode. The uniqueness that RFID has engendered, allowing an instance of a product to be tracked, has raised some important privacy concerns. RFID technology has also promised to increase the amount of aggregate data that is collected. When dealing with data, especially the tremendous amount that RFID will produce, ethical concerns about how the data is to be used are prevalent. This paper reviews the RFID technology, presents challenges that the technology creates for privacy and ethics, and suggests possible solutions to these challenges.

Keywords: RFID, Ethics, Privacy, Security

INTRODUCTION

The RFID tag is a very simple piece of electronic circuitry that can receive information, do some limited processing, and return (re-transmit) some piece of information. Many other types of electronic circuitry currently have this trait, but due to the minuscule nature of the RFID tag this technology is receiving more investigation.

RFID is not a new technology since it dates back to the second world war and was a method employed of identifying allied aircraft [6]. Currently, it is receiving much more attention since following Moore's law in that the technology has become much cheaper, and smaller.

While not the only application of an RFID tag, the RFID tag is receiving attention as being a replacement of the current bar code. A bar code, as it currently stands, has several limitations: (a) it can only be read within a limited line of site, (b) it does not offer enough distinction among instances of a certain type of object, and (c) it is difficult to change. Take, for example, the following:

> The bar code of a particular Gillette ® razor is not indicative, nor particular to that individual razor. Any other razor of that same model will have the same bar code. The bar code may only indicate the manufacturer and the model of the razor, but it cannot differentiate two separate instances of the same object.

These limitations of the bar code can be overcome to some extent by the implementation of the RFID tag [3]. The RFID tag will allow for unique tracking of each instance of a product. In the above example, an RFID tag attached to a razor would attach a unique identifier to each individual pack of razors, rather than a particular class of razors. Electronic Product Code (EPC) tags will be the successor to these bar codes [16].

Currently prices for an RFID tag range from $0.20/tag on up, depending on functionality. As Moore's law holds constant, the size and cost of these tags are decreasing and it is estimated that the cost of these tags will fall to as little as $0.05/tag within the next few years [27,19]. Prices will especially begin to fall as novel ways of tag creation are employed [24, 29].

The current utilizations of RFID are numerous. RFID is being implemented as a method of deterring counterfeiting in passports and banknotes. The FDA has recently approved the use of RFID research for the tracking of prescription drugs in order to help control counterfeiting [5, 32, 35]. It also could be used as a means of tracking drug administration to reduce the frequency of errors and track compliance [28]. Being able to track the pedigree of these drugs has been facilitated by the use of RFID [31]. RFID has been used extensively in the supply chain, in agriculture, for pet identification, and in other areas.

RFID TECHNOLOGY

In order to see why RFID tags have received so much attention, it is important to first understand how they work, and their various components. There are two types of tags: active and passive. The active tag has its own power source, and consequently has a bigger footprint than the passive tag. The on-board power source also augments the cost of the chip. The passive tag is a smaller tag that relies on power from the reader in order to transmit its message. The passive tag, because of its inexpensiveness is thought to be the most predominantly used.

One part of the tag is necessarily the antenna. The antenna is used as the method of picking up the signal from the reader, as well as sending the signal back to the reader. In the case of the passive tag, it is also the vessel in which power is obtained to operate the tag. The tag employs a method of load modulation, or backscatter modulation to communicate back with the reader [33, 34].

The tag itself, since constrained by size and thus processing ability, is limited to the amount of information that it can store. According to some authors, in the case of an EPC tag, this amount is 96 bits [9]. This minimal information is generally an identifier which is unique to each individual tag and will allow identification of each instance of an object. In order to allow unique identification of each object a typical EPC tag will consist of the following information: a header which identifies EPC version, Manager number which identifies the company or company entity, the object class which is similar to a SKU, and a serial number which will be unique for each instance of an object [13].

Each tag will have been preprogrammed with some basic functions [14], these may include:

- A kill command – disables the tag permanently.
- A sleep command – the tag no longer responds to queries, except upon receipt of a corresponding 'wake' command.
- Read – sends ID to reader
- Write – takes information from reader and stores it.

The tag is the nominal part of the RFID system. There are two other imperatives in order to make the system work: a reader and a database. The reader is the object that asks a tag for its contents, and could power the passive tag. The signal that the reader emits, creates power for the passive tag and interrogates either type of tag in order to retrieve its' contents. The signal from the reader to the tag is stronger than that from the tag back to the reader [25]. The reader must be bound to a backend data source.

Many people assume that the RFID tag itself will be the information container. This is not the case. The RFID tag can only hold a minimal identifier. The identifier, when received by an appropriate reader that is coupled to an appropriate database, allows retrieval of stored information on the database. A database is a vital piece of the RFID infrastructure.

PRIVACY CONCERNS

One of the main concerns of both the advocates of RFID as well as the opponents is that of privacy [15]. Ethical concerns associated with these privacy dilemmas are also prevalent. This paper argues that the concerns for privacy and ethics are one in the same because when privacy concerns have been addressed, ethical dilemmas are minimized. Several of the reasons for ethical/privacy concerns are discussed below.

First, since the tag uses radio based communication, line-of-sight reading is unnecessary and reading can be done from a greater distance. Due to the inherent nature of radio transmission, privacy concerns are abundant. The introduction of unauthorized, 'hidden' readers into the system may compromise security. Avoine [2] presents an adversarial model and attacks on existing known RFID protocols. A second issue to consider is location tracking. One of the functionalities, and indeed perhaps one of the advantages of the RFID system, is the ability for a tagged item to be tracked. Throughout the supply chain it is advantageous to members of the chain to see through what locality a particular order has been processed. RFID allows this. The RFID tag, as explained above, will emit a particular identifier upon query. Privacy advocates are concerned that unauthorized readers will be able to extract the ID and could use it to track unwary consumers.

The issue of invisibility has also been discussed by some authors as a point against privacy. Tags are very small and thus it can be very hard for a consumer to detect an RFID tag visually. Since RFID tags are so minuscule, how will people know what items are tagged and which are not? At the same time, how is a consumer to know when this embedded tag has been scanned? This invisibility of a tag arguably violates the Fair Information Practices act.

Peslak [22] presents four reasons given by the ACLU and CASPIAN on the ethical concerns of RFID:

(1) The tags are hidden and unknown.
(2) Tags provide an id system of every item purchased, thus allowing a universal product registration system.
(3) Aggregation of massive personal amounts of data.
(4) Allows tracking of individuals

SECURITY SOLUTIONS

For something to be secure, it must possess the following characteristics: confidential, having integrity, authentic, non-repudiable, and be available [23]. Confidentiality as defined by Avizienis and colleagues is "the prevention of the unauthorized disclosure of information" [4]. Data integrity is "concerned with preserving the meaning of information, with preserving the completeness and consistency of its representations within the system, and with its correspondence to its representations external to the system" [20]. If something is non-repudiable it means that the origin is without question. Availability is "whether a system is available for use by its intended users" [12].

Several proposals have been indicated in the literature as solutions to the privacy problem [1,7,10]. These proposals include, but are not limited to the following: the "kill tag", hash-based access control, "blocker tag", and the Faraday cage approach.

The "kill tag" [27], involves creating a command within the tag itself that upon issuance will invalidate the tag. All EPC-Gen 2 tags have this built in functionality [30,37]. The tag would be rendered inoperative at the time of sale through the use of the kill function. This method of security would meet the security requirement of confidentiality, but would violate the requirement that it be available. The tag would no longer be available for reads.

Hash based access controls as suggested by several authors [36, 10], involves creating a one-way hash function to encrypt contents from reader to tag or vice-versa. This method of security would meet the requirement of confidentiality, assure authenticity, and meet the other requirements of security as outlined by Ranasinghe [23].

The blocker tag as suggested by Juels [17] is a way of confusing the reader by broadcasting conflicting signals at the same time the reader is trying to query a normal tag. In order to perform a successful read, the blocker tag would need to be squelched. This method too would promote confidentiality, but may limit availability.

The Faraday cage approach, is perhaps the simplest, and involves putting the tag in some 'caged' environment so that it can't be read, such as a foil-lined wallet. Molnar and colleagues [21] present the use of a trusted computing initiative to secure RFID systems. Molnar suggests a new architecture for trust wherein the RFID reader contains a tamper-resistant trusted chip. The architecture also contains some policies that are enforceable to maintain privacy. Once again, confidentiality is assured, but availability would diminish.

Many of these security approaches above involve making the tag unreadable, which questionably voids the utility of the tag. The approaches above also only deal directly with the tag itself, without emphasis on the ethics of the data that is collected. Now, a discussion is given on the ethics of data collection.

ETHICAL DATA CONSIDERATIONS

Privacy as defined by Flavian and Guinaliu is "an individual's ability to control the terms by which his personal information is acquired and used" [8]. The tremendous amount of data that will be created through the use of RFID certainly casts doubt on the ability of a consumer to mandate how personal data is being used. In the business world, regulation as to what can be done with personal consumer information has always been a matter of concern. With the promise of RFID data being an exponential increase in the amount of data being collected, new data collection requirements and constraints are being investigated.

Erickson and Kelly [18] suggest that retailers have always maintained databases and information about the consumer. They suggest that within the U.S. companies have frequently been able to traffic in consumer data without the consumers consent. Comparatively, in the E.U., an opt-in policy for data collection currently exists.

The fair information practices principles given by the Federal Trade Commission suggest the following principles be utilized when dealing with consumer data: notice that data is being collected, allowing user to choose whether or not the data can be used, consumers should be able to view their collected data, and data should be secure. These principles have arguably been suggested to apply to RFID and they do address several of the points addressed presented above by Peslak.

CONCLUSIONS

In this paper, we have briefly given a synopsis of the RFID technology. We have also presented some of the hurdles relating to privacy and ethics that this technology engenders. There are many proposed solutions in the literature for personal privacy protection when dealing with RFID technology. Clearly, from the discussion above, there is still no

unified, clear-cut answer to the security problem, as well as solutions to the ethical dilemmas posed from the utilization of this technology. However, from the above the discussion the following conclusion can be given: When the barriers to privacy are overcome, ethical dilemmas tend to dissipate.

REFERENCES

1. Aigner, M., Feldhofer, M., "Secure Symmetric Authentication for RFID Tags", Telecommunications and Mobile Computing TCMC2005. March 2005.
2. Avione, G., "Radio Frequency Identification: Adversary Model and Attacks on Existing Protocols", Technical Report LASEC-REPORT-2005-001, Sept. 2005.
3. Avione, G., Oechslin, P., "RFID Traceability: A Multilayer Problem (draft version)". Available from http://lasecwww.epfs.ch/~gavione/download/rfid-multilayer-paper.pdf accessed Jan. 2005.
4. Avizienis, A., Laprie, J., Randell, B., "Fundamental Concepts of Dependability". Technical Report 01145, LAAS-CNRS, Toulouse, France, 2001.
5. Collins, J., "FDA Clears the Way for RFID Tagging", http://www.rfidjounal.com/article/articleprint/1238/-1/1/ accessed Nov. 2004.
6. Fanberg, H., "The RFID Revolution", Mark Health Services. Fall 2004. Vol. 24. No. 3. pp.43-44.
7. Feldhofer, M., "A Proposal for an Authentication Protocol in a Security Layer for RFID Smart Tags". In the 12th IEEE Mediterranean Electro technical Conference – MELECON 2004. IEEE Proceedings. May 2004. pp. 759-762,
8. Flavian, C., Guinaliu, M., "Consumer trust, perceived security, and privacy policy", Industrial Management and Data Systems, Vol. 106, No. 5, 2006. pp. 601-620.
9. Good, N., Molnar, D., Urban, J., "Radio Frequency and Privacy with Information Goods". Proceedings of the 2004 ACM workshop on Privacy in the electronic Society", 2004. pp. 41-42.
10. Henrici, D., Muller, P., "Hash-based enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers". Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops. 2004. pg. 149
11. Henrici, D., Muller, P., "Tackling Security and Privacy Issues in Radio Frequency Identification Devices". Second International Conference on Pervasive Computing, Lecture Notes in Computer Science. Springer-Verlag. April 2004. pp. 219–224
12. http://mtechit.com/concepts/availability.html accessed Jan. 2006.
13. http://www.epcglobalinc.org/about/faqs.html#6 accessed July 2005.
14. http://www.epcglobalinc.org/standards_technology/_Secure/V1.0/UHF-class1.pdf accessed July 2005.
15. http://www.spychips.com/what-is-rfid.html, accessed May 2005.
16. Juels, A. "Strengthening EPC Tags Against Cloning". ACM workshop on Wireless Security (WiSe), 2005. pp. 67-76.
17. Juels, A., Rivest, R., Szydio, M., "The Blocker Tag: Selective Blocking of RFID Tags for consumer privacy". In 10th Annual ACM CCS 2003, May 2003.
18. Kelly, E., Erickson, G., "RFID Tags: Commercial applications vs. Privacy Rights", Industrial Management and Data Systems. Vol. 105. 2005. pp. 5-6.
19. Kumagai, J., Cherry, S., "Sensors and Sensibility", IEEE Spectrum, Vol. 41, Issue 7, July 2004. pp. 18-24.
20. Mayfield, T., Roskos, J., Welke, S., Boone, J., "Integrity in Automated Information Systems", Technical Report 79-91, National Computer Security Center. Sept. 1991. Available at http://zedz.nl/rainbow/C-TR-79-91.pdf accessed Jan. 2005
21. Molnar, D., Soppera, A., Wagner, D., "Privacy for RFID Through Trusted Computing". WPES, Nov. 2005.
22. Peslak, A., "An Ethical Exploration of Privacy and Radio Frequency Identification", Journal of Business Ethics. Vol. 59, 2005. pp. 327-345.
23. Ranasinghe, D., "Low-Cost RFID Systems: Confronting Security and Privacy". Available at http://www.m-lab.ch/auto-id/SwissReWorkshop/papers/LowCostRFID-ConfrontingSecurityAndPrivacy.pdf accessed May 2005.
24. Redinger, D., Farshchi, R., Subramanian, V., "An All-Printed Passive Component Technology for Low-Cost RFID", 61st Device Research Conference. Conference Digest, 2003, pp. 187-188
25. RFID Handbook, 2nd ed. ISBN: 0-470-84402-7, April 2003, Wiley and Sons
26. Sarma, S., "Towards the five-cent tag". Technical report MIT-AUTOID-WH-006, MIT Auto ID Center, 2001. Available from http://www.autoidcenter.org. accessed March

2005.
27. Sarma, S., Weis, S., Engels, D., "Radio-Frequency Identification Systems". CHES '02, Springer-Verlag. LNCS no. 2523. 2002. pp. 454-469.
28. Schoenberger, C., "Radio RX", Forbes, Sept. 2003, vol. 172, Issue 5, pg. 126.
29. Sullivan, L., "Philips Ships Next-Generation RFID Chips", available at www.informationweeks.com/story/ShowArticle:jhtml?articleID=160401540 accessed June 2005.
30. The Gen 2 Story: Charting the Path to RFID That Just Works, Impinj Whitepaper, www.impinj.com accessed April 2005.
31. Towner, C., "Business Case: Economic Benefits of EPC in Pharmaceuticals". AUTO-ID Labs white paper. Available at http://www.autoidlabs.org/whitepapers/cap-autoid-bc001.pdf accessed April 2005.
32. US FDA Report, "Combating Counterfeit Drugs: A Report of the Food and Drug Administration", February 2004, available at http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html accessed March 2005.
33. Want, R., "Enabling Ubiquitous Computing with RFID", Computer, vol. 37, April 2004, pp. 84-86.
34. Want, R., "RFID: A Key to Automating Everything", Scientific American, Jan. 2004, pp. 58-65.
35. Wechsler, J., "Drug Safety in the Limelight", Pharmaceutical Technology, May 2003. Available at http://ptemag.com/pharmtecheurope/article/articleDetail.jsp?id=57828 accessed March 2005.
36. Weis, S., Sarma, S., Rivest, R., and Engels, D., "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems". First International Conference on Security in Pervasive Computing, 2003. Available at http://theory.lcs.mit.edu/sweis/spc-rfid.pdf accessed Feb. 2005.
37. York, C., "RFID Strategy – What Does the Gen2 RFID Standard Mean to You?". available at http://www.narm.com/Content/NavigationMenu/Distributor_Database/RFID/RFID.htm accessed January 2005.