Privacy Implications of RFID Tags

by Paul Stamatiou

CS4001, Georgia Institute of Technology
November 8th, 2007

Radio Frequency Identification (RFID) is a maturing wireless technology with widespread uses, many of which individuals interact with on a daily basis, whether they are aware of it or not. RFID tags can make businesses more efficient through rapid inventory management, provide consumers with a faster method of checking out at their local convenience store, ensure that people are properly administered the medicine they need, and more (Bhuptani, 2005, p. 5). While RFID tags do not yet have bulletproof security measures and can expose personally-identifiable information, there remains a strong incentive to continue using and developing RFID technology (Want, 2006, p. 4, 59). Due to the vast range of RFID applications, the scope of this paper will be limited to consumer and individual applications as opposed to corporate uses of RFID technology.

To adequately understand the privacy issues that arise from the use of RFID tags, one must first grasp the technical aspects of RFID systems in general. A typical RFID system is comprised of three components: a tag, an interrogator, and a controller (Hunt, 2006, p. 5). The tag is a tiny module containing a chip and antenna. The interrogator, also referred to as a reader, provides a means to power the often-passive RFID tag's semiconductor chip and enable communication with the tag, usually for data retrieval (Glover, 2006, p. 36). The last part of an RFID system is the controller, which serves as the regulatory entity for the system. The controller processes the data taken from the RFID tag via the interrogator by interfacing with a host computer (Bhuptani, 2005, p. 43). This data may then be used to update a database, authenticate a person, or complete virtually any task. Of the three parts of an RFID system, it is the RFID tag that must be adapted for various applications and is available in many formats.

RFID tags are designed and developed with their application in mind. Implantable tags are manufactured in sterile glass casings, paper tags are printed for use on packages, sew-on tags

are affixed to clothing, and so on (Bhuptani, 2005, p. 41). Furthermore, there are two main types of tags: passive and active. Passive tags only need a semiconductor chip and antenna. They receive power from the interrogator's radio frequency signals through a process known as induction (Want, 2006, p. 7). As a result, these tags only receive power when read by an interrogator. There are several positive and negative implications to not having an on-board power source. First, passive RFID tags are smaller than their active counterparts, and considerably cheaper to produce. Unfortunately, the absence of a battery also results in a shorter transmission range, a smaller memory capacity, and the need for stronger interrogators to power them (Hunt, 2006, p. 7).

Several examples of passive RFID tags found within clothing labels. Only one motions the consumer to remove the label after purchase. Image courtesy of http://spychips.com.

Active tags on the other hand utilize a battery or other on-board power source to sustain the chip and transfer data over the integrated antenna. These tags are capable of maintaining

larger memory stores and interacting with less powerful interrogators. Their power may also be used to run additional circuitry, such as a temperature or other environmental sensors, to identify expired goods (Glover, 2006, p. 58). A drawback of active tags is that they are more complex, larger and more expensive than passive tags. There is also a class of pseudo-active tags that contain a battery, which is not put towards communicating with an interrogator and is reserved for powering sensors and processors. The power source of RFID tags affects not only the size and cost of the tag, but also the read range.

Passive tags generally operate within low and high frequency ranges, with a read range of just a few feet. Active tags take advantage of their battery to boost the read range to around 10 to 30 feet, while on a high frequency (Hunt, 2006, p. 17). However, these are optimal use cases and ranges may be affected by several factors including frequency, antenna gain, and interrogator power. For example, a group of hackers at a 2005 Defcon convention were able to read a passive RFID tag from almost 70 feet away using a high-powered interrogator (Sieberg, 2006, p. 1). RFID tags may also operate on higher frequencies like UHF and Microwave for greater read ranges. However, these higher bands are more sensitive to differences in RFID tag orientation making it difficult to accurately read the tag on the first try without the use of complex modulation (Hunt, 2006, p. 15). As such, they are more expensive and generally limited to static, controllable situations like warehouse pallets (Glover, 2006, p. 60).

RFID tags come in many shapes and sizes, with varying positives, negatives and disparate capabilities. When narrowed down to typical consumer applications – key chains meant to replace credit cards, modern car keys, passports, et cetera – passive tags are the clear winner. Cost is a major factor when choosing to embed RFID tags into millions of products, so it should be no surprise that passive tags have become the de facto standard. At roughly 10 cents apiece,

passive tags are far from an ideal price of 5 cents and a far cry from the less than one-cent price of competing bar codes (Garfinkel, 2005, p. 86). Furthermore, most RFID tags have a unique ID making it possible to identify a particular tag; this has stronger connotations when taking into account a global database of consumers as explained later (Want, 2006, p. 30). Unfortunately, these low-cost passive RFID tags do not benefit from encryption, which inevitably leads to a privacy dilemma in certain consumer RFID applications (Garfinkel, 2005, p. 331).

Low-cost RFID tags have penetrated the marketplace due to their sheer benefits over traditional barcodes, which hold several limitations. RFID tags fortify the primary draw of bar codes – the ability for ordinary items to be machine-readable at a trivial cost. Where as bar codes store an infinitesimal amount of data, ranging from 8 numeric characters to 2000 ASCII characters, RFID tags may hold up to 128 kilobytes (Hunt, 2006, p. 21). However, it is the wireless capabilities of RFID tags that make their uses obvious over bar codes. Many tags may be read at once and tags need not be within line-of-sight. Their technical implementation also ensures tags are difficult to replicate (Hunt, 2006, p. 22). Even though RFID tags compete with bar codes, tags are far from being limited to similar uses. The wireless ability of RFID tags has opened the door to previously impossible applications.

If RFID system implementation and tag costs were ideal, which is foreseeable with a firm push from major corporations like Wal-Mart, consumers would have dozens of tags in their household and personal belongings (Garfinkel, 2005, p. 529). Imagine that Jill is a 23-year-old recent graduate and successful programmer at a large web company in California. She has always embraced technology and enjoys spending her new disposable income. On a typical Saturday morning, Jill sets the alarm and locks her house all by waving her RFID tag-implanted hand next to a reader in the wall. Upon walking out the door, her house text-messages her mobile

phone to let her know that it scanned her RFID tagged credit card and recommends she not spend over $200. Jill proceeds to leave her house by first unlocking and turning on her car with a keyless entry card that authenticates her with the vehicle. Jill then drives to the local mall where she pays for parking without stopping to swipe any card. Later on, she walks into her favorite store and an RFID reader in the store detects she is wearing a pair of boots purchased from the store. The store is able to find Jill's previous purchases with the unique ID of the RFID tag in her boots and discovers she is a frequent customer, urging a sales person to greet her warmly. Jill then picks up the scarf she wants and walks right out the door. The store is able to read the price of the scarf from its RFID tag and subsequently charge Jill's RFID tagged credit card. All of this is possible with RFID technology. It is only a matter of time. While that may sound like utopia to Jill, it presents great vulnerabilities waiting to be exploited.

Tags used for item-level tagging, such as on individual products like Jill's scarf, would most likely be cheap, passive EPC RFID tags. For example, it would not make sense to put a more complex one-dollar active tag on a tube of toothpaste and so on. EPC RFID tags abide by a standard set forth by EPCglobal and have become commonplace (Thornton, 2006, p. 39). Unfortunately, this means that EPC RFID tags identify themselves to readers but do not authenticate themselves. For a tag to be able to authenticate itself, it must hold private data created through some encryption or keyed hash algorithm to prove its identity. Generating such private data would require a more complex tag capable of carrying out the computation. Cost is a driving factor when implementing RFID tags on a large scale, so EPC tags are of the low-cost, passive type. The RFID reader must also maintain a copy of that private data key for each tag, which introduces the issue of distributing such keys from tag manufacturers to readers that are used by third parties (Garfinkel, 2005, p. 140).

Not all tags used are low-cost EPCglobal tags. Where necessary, the cost for more complex RFID tags capable of encryption and advanced authentication techniques would easily be justifiable – an example being an RFID tagged credit card. While it is clear that RFID tags utilized for contactless payment solutions must be secure, they are still open to exploitation through the man-in-the-middle attacks that plague all wireless communication systems (Thornton, 2006, p. 138). American Express and Chase RFID tagged credit cards claim to use encryption, but a cheap RFID reader easily obtained private credit card information in plain text (Schwartz, 2006, p. 1). However, the real risk comes from widely used simple, unencrypted tags placed in individual products.

The canonical doomsday scenario for RFID tags does not deal with cracking encrypted RFID tags used for payment so much as creating a global consumer database from tags in consumer purchases. RFID tags were intended, like most technology, to offer the end user a cheaper, more efficient, and convenient product in the long run. But with RFID tags, how much convenience is too much? Perhaps when it can be used to track people with any degree of accuracy. This is where item-level tagging should be used with caution. Item-level tagging is the term for the embedding RFID tags in individual products as opposed to pallets of bulk products in a warehouse. Item-level tagging is not yet prevalent but at the current pace it is expected between 2010 and 2020 (Bhuptani, 2005, p. 182).

How much information can a single tag attached to a pair of jeans store? A lot. While the tag itself does not have much room in its own memory to hold data, it is the unique ID of the tag that presents the real privacy risk. Back to the doomsday scenario again, in the future there might be millions of RFID readers installed throughout the nation to support the predominant item-level tagging in use (Garfinkel, 2005, p. 263). Combine that with the ability for RFID tags to be

read without a person's knowledge, including hidden tags woven into their clothing, and the privacy issues are apparent (Ohkubo, 2005, p. 68).

MIT Professor Jerry Saltzer once stated that privacy is a database correlation issue. Suppose several separate entities have their own databases of information from someone. Entity A might have their name and address, Entity B their name, SSN and list of recent purchases, Entity C their name, date of birth, mother's maiden name and so on. All it takes is a malicious person with access to these databases (that may just mean access to the Internet in some cases) to cross-reference a shared term such as that person's name and they will have a great deal of information about that person. This might sound Orwellian, but it is a real concern that should be heeded. Katherine Albrecht expands on this database issue in regards to an RFID-tagged society where the unique ID of a tag in a product could be used as the key to cross-reference multiple databases (Garfinkel, 2005, p. 266). Such databases could store information about manufacturing and shipping information for a product, product identification data, point of sale records including information about the buyer, and even information tracked after the point of sale. Ordinary, uninformed consumers may not know about the RFID tags in their purchased goods, much less how to disable them after leaving the store. There are, however, technical, social, and legal solutions to this privacy problem.

Even if an item-level tag is in place, there is no need for it to remain active after a sale. It only makes the consumer vulnerable to being picked up by one of the ubiquitous RFID readers. Consumers can easily protect themselves by finding and removing the tags. Yet, this is not always easy as modern RFID tags can be smaller than a grain of salt (Murray, 2006, p. 72). Another simple way to subdue tags is to apply the Faraday cage approach and shield the tags with metal mesh or foil that is impenetrable by radio signals (Juels, 2003, p. 105). As this

method is not flawless, it is not reasonable to shield every purchased product at all times. Another tactic for securing privacy is to implement a kill command to quickly and permanently disable tags after purchase or at any time requested by the consumer (Bhuptani, 2005, p.165). This kill command is part of EPCglobal's standard yet its drawback is that once the RFID tag is disabled, consumers will not be able to take advantage of other conveniences some tags boast. For example, a refrigerator might be able to tell its owner that a carton of eggs has expired, but not after the tag has been killed (Juels, 2003, p. 104). Also, it would be possible for someone to develop the hardware necessary to kill many tags in stores (Thornton, 2006, p. 99). IBM created a solution of its own called the Clipped Tag (Wagner, 2006, p. 1). The Clipped Tag allows consumers to tear off the antenna portion of the tag, limiting its range to only an inch. However, the Clipped Tag is suited more for clothing items than other products. Deploying RSA Security's blocker tag is yet another method of controlling RFID tags. When a blocker tag is used in range of other RFID tags, it induces a privacy zone where an RFID reader will become overwhelmed by the blocker tag's broadcast of serial numbers, preventing the tag reading (Glover, 2006, p. 207). The blocker tag can be considered a wireless form of the Faraday cage approach. Continuing with the trend, blocker tags have their own drawbacks as well. They can be used maliciously to hide products at checkout or induce denial of service attacks on RFID readers. Currently, there is no perfect solution to managing RFID tags after the point of sale so as to thwart potentially malevolent tag scans.

Taking a step back, why is item-level tagging necessary? It is not necessary, it is just a future, idealistic convenience. By not having low-cost, unencrypted RFID tags in every item, consumers would not be exposed to as many privacy risks. Unfortunately, the market cannot easily be swayed from its current route towards the efficiency that RFID tags bring. RFID

systems are great for corporations and once tags can be produced inexpensively, there is no doubt that they will be embedded into more and more items. Stores would be able to checkout customers faster with a single RFID reader capable of simultaneously reading multiple tags, instead of maintaining many bar code scanners and employees (Hunt, 2006, p. 107).

Before RFID proliferation reaches the tipping point, consumers should know their RFID rights and corporations should follow them. Privacy expert Simson Garfinkel proposed the RFID Bill of Rights to serve this purpose. They include the rights to: know whether products contain RFID tags, have tags removed or disabled once tagged items have been purchased, use RFID-enabled services without tags, access the data stored on an RFID tag and know when, where, and why tags are being read (Garfinkel, 2002, p. 35). Similar to how a pack of M&M's states they were manufactured in a plant that processes peanuts, future items containing RFID tags should make it easy for the ordinary consumer to know whether the item is tagged. This is vital as RFID tags will indubitably become a part of everyone's life in the near future.

The privacy implications of RFID tags are not explicitly black or white. Tags have numerous benefits that should not be simply written off due to potential privacy risks. Technology is inherently vulnerable. Given proper resources, anything can be exploited, circumvented, or disabled. Even encrypted RFID tags can be exploited or cloned through a bevy of radio frequency manipulation techniques (Thornton, 2006, p. 59, 98). Many examples in this paper pointed out flaws in current RFID technology. The reality is that there are not skilled RFID hackers everywhere in the world, waiting for people to leave their houses so they can scan their RFID tagged credit cards. The Internet is filled with brilliant hackers and malicious viruses, but millions of people still go online daily. Similar to Internet users, RFID tag users must know how to stay safe, and this will only happen once a proper RFID Bill of Rights is adopted. Otherwise,

consumers would not be able to enjoy the perks associated with RFID applications. A great example of RFID use comes from the San Francisco Exploratorium Museum. Visitors may opt to carry an RFID tag with them, scanning in at each exhibit so that they may later access extra content from those exhibits, in addition to view a log of their museum visits on a protected web site (Hsi, 2005, p. 62). The Exploratorium exemplifies how RFID tags can add great value to a consumer's experience when implemented safely and properly. What other kinds of incredibly useful applications of RFID tags could emerge? The answer to that question will emerge once consumers are aware of the capabilities of RFID tags, and corporations make an effort to protect the privacy of those consumers. There will always be hackers, but that is no reason to hinder progress in RFID technology that may make tags even more secure and bring about interesting applications.

Bibliography

Bhuptani, M. & S. Moradpour. (2005). *RFID Field Guide: Deploying Radio Frequency Identification Systems.* Upper Saddle River, New Jersey: Prentice Hall.

Garfinkel, S. (2002, October). An RFID Bill of Rights. *Technology Review*, 35.

Garfinkel, S. (2005). *RFID: Applications, Security, and Privacy*. Westford, Massachusetts: Addison Wesley.

Glover, B. & H. Bhatt. (2006). *RFID Essentials.* Sebastopol, California: O'Reilly Media, Inc.

Guardian. (2006, November 17). *Cracked it!* Retrieved October 15, 2007, from http://www.guardian.co.uk/idcards/story/0,,1950226,00.html

Hsi, S. & H. Fait. (2005). RFID Enhances Visitors' Museum Experience at the Exploratorium. *Communications of the ACM, Vol. 48 Issue 9, 60-65.*

Hunt, V. Daniel. (2006). *RFID - A Guide to Radio Frequency Identification*. Indianapolis, Indiana: Wiley.

Juels, A., Rivest, R., and Szydlo, M. *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy.* In Proceedings of the 10th ACM Conference on Computer and Communications Security (Washington, D.C., Oct. 27-30). ACM Press, New York, 2003, 103-111.

Murray, Charles J. (2006). RFID Tags: Driving Towards 5 Cents. *EDN, Vol. 51 Issue 12, 69-74.*

Ohkubo, M. (2005). RFID Privacy Issues and Technical Challenges. *Communications of the ACM*, Vol. 48 Issue 9, 66-71.

Schwartz, J. (2006, October 23). *Researchers See Privacy Pitfalls in No-Swipe Credit Cards.* The New York Times. Retrieved November 1, 2007, from http://nytimes.com/2006/10/23/business/23card.html

Sieberg, D. (2006, October 23). *Is RFID tracking you?* CNN. Retrieved November 3, 2007, from http://cnn.com/2006/TECH/07/10/rfid/index.html

Thornton, F. & B. Haines, et al. (2006). *RFID Security.* Rockland, MA: Syngress Publishing, Inc.

Wagner, M. (2006, May 15). A Simple Fix For RFID Privacy. *InformationWeek.* Retrieved October 15, 2007, from http://informationweek.com/blog/main/archives/2006/05/a_simple_fix_fo.html

Want, R. (2006, January). RFID Explained: A Primer on Radio Frequency Identification Technologies. *Synthesis Lectures on Mobile and Pervasive Computing, Vol. 1, Issue 1, 1-94.*