Radio Frequency Identification: The Current and Future Solutions for Privacy and Security

Author: Vivek Jain
Faculty Mentor: Susan Brown Eve, Department of Applied Gerontology, College of Public Affairs and Community Service & Honors College
Department: Department of Electronics Engineering Technology, College of Engineering & Honors College

Bio:

Vivek Jain graduated as a Distinguished Honors Scholar from UNT in December 2006 with a major in Electronics Engineering Technology and a minor in Mathematics. His research interests include encryption algorithms, neuroscience, and radio frequency identification, the latter of which is the subject of his undergraduate thesis. He has presented papers/posters at the Great Plains Honors Council Conferences of 2003 and 2005, the National Honors Council Conference of 2004, and University Scholars Day in 2005 and 2006. He was awarded the Outstanding Undergraduate International Student award in 2005 and the Outstanding Engineering Technology Student award in 2007, and is a member of the Phi Kappa Phi, Tau Alpha Pi, and Golden Key Honor Society. He is currently working as an Applications Engineer at CodeSource, LLC, a startup firm in the optics and RFID industry in Denton, TX.

Abstract:

There has been a lot of interest expressed by the public and media at large about the security and privacy issues involved in the adoption of a rapidly growing, relatively new identification technology: Radio Frequency Identification (RFID). Although most interest has been generated by the unique advantages this technology brings with it, substantial and mostly valid concerns have been raised at various public policy and academic fora. RFID, just like any other wireless technology, is open to 'rogue' interceptions. However, distinct challenges arise in this new technology because of the inherent ease and low cost of the methods that can be used to access and manipulate data stored in the RFID media. Like any new technology, however, there is a mismatch between the nonprofessional's perception and technical realities concerning both the advantages and concerns of RFID. This paper, therefore, explores the plethora of standards, protocols, 'attack models,' and security algorithms and collates them for use as a compendium for RFID students and practitioners alike.

Introduction

Radio Frequency Identification (RFID) is a contact less technology for automated or manual identification of objects (and/or living beings). We explain in a later section the basics of RFID communication, and why it has been hailed as the next major revolution in identification technology. We will first discuss the identification systems that are in common use today.

An Overview of Identification Technologies in Widespread Use Today

Optical codes. The most common, seen everywhere from the product-specific UPCs (Unique Product Codes) to the U.S. Postal Service automatic markings on envelopes, barcodes have penetrated wide and deep in the retail and logistics industry. Their major attractiveness lies in their cheap cost (< 10 cents per barcode) and ease of handling (can be printed or affixed on almost any product). Refer to Figures 1 and 2. The major drawback of barcodes, like any other optical-based identification technology, is the necessity for a barcode to be placed in the line-of-sight of the reader (Juels 2006). This need makes automation prohibitively difficult to attain (as in automatic checkout of goods from a store, or the check-in of inventory at storage points), because human intervention becomes necessary. The other major drawback to optical barcodes is their inability to uniquely identify objects (Juels 2006; Kim et al. 2006; Garfinkel et al. 2005).

Biometric identification. Although more specialized, and hardly found in the retail industry, biometric identification has been widely used for some time now for basic access authorizations by companies or in identity-establishing documents (passports, driver's licenses, etc.) by the government. Such biometric procedures could consist of fingerprints, eye scans, or facial-recognition algorithms.

Although unique in identity determination, biometric identification is still a costly proposition, and requires explicit human intervention to affect its operation. Moreover, most

consumers may not like to give out fingerprints for checking out their weekly groceries. Their use, therefore, remains specialized (Finkenzeller 2005, Ch. 1).

*Magnetic strip*s. Widely used in an array of plastic cards (ID cards, credit cards, driver's licenses), magnetic strip-enabled cards have been a low-cost solution to simple data-encoding and retrieval systems. This simplicity is their big advantage, whereas the major disadvantage is of physical contact (the swipe) between the card and the reader.

RFID Basics

An RFID device consists of two components: the tag (or the data-holding circuit), and the reader (the querying circuit). From this basic setup, a multitude of combinations can arise to result in very specialized RFID implementations, and consequently, a host of governing protocols. Therefore, the specific use a particular implementation of RFID is going to demand determines the type of tag used, which in turn, defines the characteristics of the reader.

An RFID 'tag' (or 'transponder') is a simple circuit that 'responds' (by oscillating at a specific query frequency) to a 'read' signal by the reader. When the query is completed, and the tag response recorded, the reader is free to perform a host of other uses with this acquired data from the tag. The fascination with RFID, indeed, lies with the post-retrieval use of the data (i.e., database-linking post reading to store/retrieve rich history about the unique ID just accessed). Refer to Figure 3.

Current State of Affairs

RFID Advantages

Juels (2005; Juels and Weis 2006) lays down the two distinct advantages of RFID:

1. *Unique identification*: Unlike barcodes that do not hold globally unique identifiers (they are more class-specific: for example, all milk containers from a certain

company may have the same barcode readings), RFID tags can store globally unique identifiers. These identifiers can then "act as pointers to database entries containing rich transaction histories for individual items" (2006, p. 2).

2. *Automation*: Barcodes and almost all other non-RFID methods of identification today require either physical or at least a line-of-sight contact with readers. In contrast, RFID tags can be read without precise positioning as long as they are in their nominal 'read ranges.' Refer to Figure 4.

These obvious advantages, combined with a long-term use of tags for inventorying and/or tracking consumer behavior, have been very attractive to big retailers like Wal-Mart. The Department of Defense (DoD) has also recognized the efficiency potential of tracking defense shipments (over $5,000) using RFID pallet and crate tags. In the United States, these two organizations have exponentially expanded the RFID market. Many more corporations are expected to follow soon, and consequently the once-prohibitive costs of RFID tags (as compared to other technologies like barcodes) are expected to fall.

Technology vs. Financial Reality

RFID tags have to compete against the existing solutions to identification. Barcodes cost less than 10 cents each to produce, while RFID tags are currently over 25 cents a piece. Many protocols govern the tags in production today and each of them has been designed keeping financial reality in mind: "the tags that will be most inexpensive and most prevalent, such as basic EPC tags, lack the computing power to perform even basic cryptographic operations"

Although the technology exists to secure tags comprehensively, the appetite for increased costs does not. This paper, therefore, will look only into proposed solutions that seek to work within the pricing and cost structure dictated by the financial reality of keeping the per-tag

production costs under the "magic" price of 10 cents. Garfinkel et al. (2005) point out , however, that "[i]f industry fails to address [privacy/security concerns]" (p. 34), the likelihood of a public or legislative restrictions backlash will increase.

RFID Classification/Protocols

Tag classification, therefore, is sufficient to describe the type of RFID implementation being used in any given setting. Primarily, tags are divided by the criterion of whether or not they are self-powered. If there is an on-board battery (costlier tags), transponders can send their own signal and are then considered active transponders. However, if they are like the vast majority of tags being used, they will not have an on-board power supply. They are then known as passive transponders. There are also various semi-active and semi-passive tags, but for this study, we will concentrate on the most widely used tags, the *passive tags*.

Current Applications

Garfinkel et al. (2005) report that between "20 and 50 million Americans carry an RFID chip in their pocket every day," with most of it being in forms of smart cards to enter buildings or automobile keys with immobilizer chips. Broadly, RFID is today being used in the following:

1. *Automobile Immobilizers*: Usually low frequency (125 kHz to 134.2 kHz), these passive RFID tags authenticate and thereby enable a vehicle operation. Although only costing a few dollars, they have been credited for up to a 50% reduction in vehicle thefts.
2. *Animal Tracking*: At a cost of $15/animal, RFID tracking has enabled lost pets, farm animals, and feral animals to be tracked and inventoried. Even high-end tracking using GPS tags ($4,000/tag) has been achieved by researchers tracking deep-sea marine life.

3. *Payment Systems*: TI's Speedpass system introduced in Exxon Mobil's gas stations a decade ago are common place, and the European Union considered placing RFID tags into its currency in 2005 (Garfinkel et al. 2005).
4. *Automatic toll collection*: New York's *EZPass* operates on a 921.75 MHz semi-passive tag with a life of five to seven years.
5. *Inventory Management*: Adopted in a large way by retailers like Wal-Mart, RFIDs are a great option to use for tracking and inventorying of supplies and therefore increase efficiency, which in turn, exponentially decreases costs.

Technology Potential

With a technology as rapidly developing as RFID is today, it may be anyone's guess as to what the future holds, but certain developments seem to stand out in terms of their starkness of intent and technological achievability. The role of legislative regulation and citizen action will also be a significant determining factor in the future application and adoption of this technology.

Technology Developments

RFID technology is going through a rapid expansion phase with a dual objective: increasing tag-data capacity, and reducing tag cost. However, with the recent privacy outcry (Phillips et al. 2005; Garfinkel et al. 2005) and policy steps, industry is beginning to realize the third objective: privacy and security. We will see that these are two separate subjects, though, but with a common goal of data integrity and secrecy.

With increased proliferation of tags, and the awarding of the ONS (Object Naming Service) contract to Verisign by EPC, there are valid concerns regarding the privacy of the end-users of such technology: individual users. Many questions arise, which we attempt to examine next.

Juels (2006) notes the following few very-achievable possibilities in the near future:

1. *Smart appliances*: RFID tags in garments, food packages, and home appliances could "talk" to each other by communicating among themselves. Although "Blue Tooth" was supposed to achieve similar objectives a decade ago, the simplicity of RFID communications gives it much more appeal.
2. *Shopping*: Consumers could check out whole carts at a time by just rolling through any of the RFID-enabled terminals. A bit more disconcerting is the idea that RFID-enabled payment devices could "perhaps even charge the consumer's [credit cards]."
3. *Medication compliance*: RFID-enabled medicine cabinets could verify (and warn otherwise) if medications are being taken in a timely manner. Hospitals are set to benefit using RFID due to ease of medical instruments inventorying.

Technological Constraints

The performance of an RFID chip embedded on a tag is dependent on many conditions. Also, the FCC power regulations, at the minimum, guarantee that the read-ranges of the devices will not be exceeded significantly. The following environmental constraints are applicable to radio-frequency powered circuits:

1. *Faraday cage effect*: If a tag is wrapped in or surrounded by a metal, it becomes invisible to any incoming radio frequency signals. This is due to the dissipation of radio frequency by the surrounding metal. This same effect is also achieved when fluid (electrolytes) surround the tag. The human body, being mostly water, would in fact block many potential RFID "attacks" (Juels 2006).

2. *Longer than 'expected' range*: Sometimes RFID tags could have excessively long ranges, causing readers to in fact detect more tags than are in the actual 'reading area.'
3. *Tag failure*: Excessive radiation can actually destroy the tag due to electromagnetic burn effect. This is sometimes the principle used to disable a tag for good. Note that this is different from the "KILL" command (Juels 2006), in which there is a unique PIN provided to the tag by a reader authorized to disable the tag.

Security and Privacy

Threats to data integrity and secrecy form different categories of concerns: security and privacy.

According to Juels (2006), a security threat would constitute either physically or electronically destroying or cloning a data-containing RFID tag. This is the threat most likely in cases of corporate espionage (competitors scanning and retrieving classified company product history), combat situations (the enemy trying to locate DoD tags in order to track military movements), and rogue suppliers (vendors stealing genuine shipments and replacing them with shipments labeled with copied/cloned data tags).

Threats to the privacy of tag information are more numerous and much more noticeable because they affect the end-users (or the consumers) of the RFID-tagged products. Ironically, the basic problem arises due to the fundamental advantage of an RFID tag: its uniqueness. Although this uniqueness becomes very desirable from an inventory/logistics point of view (Juels and Weis 2006), this same uniqueness can also result in the unique tracking of individuals carrying such unique tags. Although the tags themselves carry only small amounts of data (up to 256 bits at most), the vulnerability arises when the readers are able to associate an individual with a

unique ID, and then track that person's movements, buying preferences, and in effect, rob him or her of the fundamental right to privacy.

Kim et al. (2006) lay out a Platform for Private Preferences (P3P) that will hard-code the privacy settings desired in different situations into the tags as and when they are produced. In the following sections, we explore the threats to privacy/security and proposed low-cost solutions in the current literature. Our objective is to draft a comprehensive solution compendium for such issues.

Security Threats

EPC (Electronic Product Code) is the protocol most in demand due to its adoption by both Wal-Mart and the DoD. Because security threats pertain more to the corporate side of the RFID equation, threats to EPC are considered to contain all major threats out there.

Garfinkel et al. (2005) identify the following four major threats posed due to current low-cost protocols:

1. *Corporate Espionage Threat*: Competitors can easily and remotely gather supply chain data, taking advantage of the unique numbering of each tag. What is not considered in the literature is the fact that such threats would be counterbalanced to a point where they could almost cancel each other out, because if anyone can implement RFID, anyone can get enough readers to perform espionage.
2. *Competitive Marketing Threat*: Customer preferences can be stolen by competitors and used in competitive market scenarios.
3. *Infrastructure Threat*: Radio-frequency jamming could cause significant losses due to delays/destruction in supply-chain infrastructure.

4. *Trust Perimeter Threat*: Large volumes of electronic data offer newer opportunities for clandestine attack.

Privacy Threats

Garfinkel et al. (2005), recognizing that most personal privacy threats arise from the uniqueness of RFID tags, list the following major categories of such threats:

1. *Action Threat*: An individual's behavior (or intent) is inferred by the monitoring of the actions of a group of tags associated with that person.
2. *Association Threat*: All EPC-encoded RFID tags are registered in a central ONS database. If and when a consumer buys an EPC-labeled product, that person's identity can be easily associated with the EPC and stored in a database in a clandestine and involuntary manner.
3. *Location Threat*: Placing covert readers at strategic locations can monitor and reveal the location of individuals carrying unique tags.
4. *Preference Threat*: The goods being carried by individuals can be monitored or tracked using powerful enough readers, which could compromise the safety of customers after they leave the shop.
5. *Constellation Threat*: The RFID tags contained in a shopping bag create a radio frequency 'constellation' around a person, which can easily allow clandestine monitoring and tracking of the individual.
6. *Transaction Threat*: Persons moving from one constellation to another can reveal important and critical information about their relationships.
7. *Breadcrumb Threat*: As the name suggests, the RFID tags gathered by an individual over a period of time would still retain their association with the individual despite

being discarded. This could, in turn, be used for malicious purposes by someone posing as the individual by carrying such permanent "IDs" during crimes or other acts.

Cloning Threats

The assumption of any encryption is that its public/private keys are long enough to endure a sustained "brute force" attack to decode the data. However, RFID tags have one major constraint: their data capacity is very low to keep prices accordingly low. Therefore, an encryption state of as low as 40 bits was considered to be pretty safe by TI (which is less than 20% of the current bits used in online encryption). RSA Labs were able to show (Juels 2006) how easy it was to crack TI's Speedpass devices, which control most of today's automobile immobilizer systems.

Cloning involves an attacker who records the response of a tag, and then infers its ID. Once the ID is received, the system then poses as an authentic tag, mimicking its behavior when queried by a reader.

Proposed Solutions

There have been several solutions proposed, some stronger, some cheaper. We attempted to compile all the ones that do not compromise cost efficiency (otherwise, they are not likely to be adopted). The first solution to the problem of tag-reader relationship is the basic anti-collision feature of today's RFID Tags (Avoine and Oechslin 2005; Floerkemeier and Wille 2005; Hernandez et al. 2001; Myung and Lee 2005; Yan et al. 2005).

There are two major frameworks in this area:

1. *ALOHA (Areal Locations of Hazardous Atmospheres)*: Multiple tags being queried at the same time by a reader 'broadcasting' their responses back to the reader at timed

intervals. A transmission node that has a packet to transmit selects at random one of the time slots, and thus is able to maximize its read efficiency.

2. *Tree-based Protocols*: They split a group of tags into two subgroups until the reader receives signals of tags without collisions. In the binary tree protocol, tags are required "to have functionalities of managing a counter and a random number generator" (Myung and Lee 2005, p. 375).

Garfinkel et al. (2005) and Juels et al. (2006) suggest multiple options, and compiled the studies of various authors in the past five years (Avoine and Oechslin 2005; Floerkemeier and Wille 2005; Golle et al. 2004; Juels 2004, 2005; Juels et al. 2005; Juels et al. 2003; Kim et al. 2006; Hancke and Kuhn 2006; Heydt-Benjamin et al. in progress; Tsudik 2006; Xiao 2006), and we feel, rightly omit costlier propositions. The RFID privacy/security puzzle rests on finding solutions to two problems:

1. Uniqueness of the tag data (encrypted or not)
2. Data integrity (to stave off 'cloning' attacks)

The suggestions of Garfinkel et al. (2005) and Juels et al. (2006) try to address these two basic criteria:

1. *"Killing" and "Sleeping"*: EPC tags address consumer privacy by adding a KILL command (provided it is supported by a PIN), which will permanently disable the tag after its primary use (that is at the point-of-sale or receiving terminal). Although this approach is simple and easy to implement, it "eliminates all of the post-purchase benefits of RFID for the consumer" (Juels 2006, p.386). Garfinkel et al. (2005), in fact, question the wisdom of doing such a thing in the commercial world, where the sole purpose of RFID is to keep track of inventory and logistics until the very end of

the supply chain. Killing is not a solution in that scenario. As an alternative to 'killing,' Juels et al.(2006) offer 'sleeping' tags. However, that would involve a different PIN for putting to sleep and 'waking' up individual tags by customers, which is rightly rejected as an unsound solution.

2. *Renaming Approach*: The sticking point with most solutions is that, even though the encrypted ID being emitted by a tag has no specific meaning, it is still unique. This, in itself, is a threat. Juels et al. (2006), therefore suggest re-labeling, both physical and electronic, minimalist cryptography, which would involve only a small collection of pseudonyms (considerably slowing read time), and re-encryption as proposed, using a public-private key cryptosystem. There, the authorization to 'write' tags would only be granted to "authorities" like central bankers and/or law enforcement officials. It is vaguely based on the RSA encryption algorithm (FAQ on RFID), and actually demonstrates a way cryptography can be effectively used on tags that are inherently incapable of hardware-supported security capacity.
3. *The Proxying Approach*: Actually having a *private RFID reader* on the person of the RFID-carrying individual could theoretically be programmed to set interaction policies of the RFID tags within its read range, to not allow any incoming radiations to reach the tags unless specifically deactivated or programmed to deactivate when certain conditions were met.
4. *Distance Measurement*: A few sophisticated attacks are "relay attacks," that is, a proxy attack reader scans a potentially 'correct' tag from a distance; transmits it to a proxy tag at a farther distance; which in turn reflects this signal to a reader at a significant distance away from the original tag. This causes the reader to mistake a

'reflector' tag for the original one, in turn acting as an ephemeral 'clone.' To prevent this, Hancke et al. (2006) devised a distance-bound verification algorithm that achieves distance-bounding through time-delay recording. Therefore, the reader is able to query a tag and calculate the delay in its signal, therefore concluding its distance from itself. One can imagine this as a series of reflecting mirrors, each of which represents a tag. A light source representing a reader will have a sensor that calculates the time a light beam took to be reflected back into itself. This time difference could be set to a critical value, above which the reader would not accept the response of the tag, because it will be deemed to be too far.

5. *Blocking*: This involves placing a special tag alongside a 'constellation' of RFID tags. This tag, called the blocker tag, would mark its neighboring tags PRIVATE or PUBLIC by jamming incoming radio signals. Blocker tags could be present in shopping bags so that the contents carried away by shoppers would be safe from prying eyes or corporate espionage. However, blocking, just like other aspects of RFID, is affected by the environmental conditions it is subjected to; a blocker tag may fail to protect a few or all of its surrounding tags if it happens to be shielded itself.

The 'perfectly secure' system is a still years away. This paper attempts to explore the solutions in the literature, while bringing to light the myriad of protocols and regulations that govern the implementation of RFID. The fundamental issue of RFID tag ID transmittal is still sticky, although there have been many attempts to address them.

In Conclusion: Perspective from the Users

The number one concern of the industry is the ROI – Return on Investment of the RFID. Due to this goal, and to the still deep penetration of alternative technologies in the market, the barcodes and the optical systems, RFID has faced immense pressure to keep on reducing the complexity, and hence, as the hope goes, the price. The industry also has ignored security and privacy concerns. The magic figure of 10cents per tag is still years away, and the minimum number of logic 'gates' to implement even the most basic security are not predicted to be installed in any mass-used tag in the near future. Poirier and McCollum (2006) point out that a retailer loses an average of 4% of sales due to out-of-stock items. If RFID is to bring value, its deployment then has to obviously cost less than that figure.

Because not only personal privacy concerns but also corporate security concerns are increasingly gaining ground, it will not be surprising to see an adjustment of the total cost of tags to include the potential losses caused by the lack of privacy/security enhancements in the future generations of RFID tags.

Public policy also has to reflect these concerns in a more regulatory fashion. Taking cue from the FCC, policy formulated at the highest levels will have to be mandated to bring about an overall acceptance of this potentially malicious technology. For instance, California passed the Identity Information Protection Act in 2005 dictating certain terms and requirements governing the use of RFID to track goods and customers (Garfinkel et al. 2005), placing a "moratorium on embedding RFID in drivers' licenses and outlawing surreptitious interception of RFID signals" (Phillips et al. 2005, p.86).

Future research in this field necessitates the involvement of specialists and experts from many different fields of study like engineering, mathematics, business, and public policy.

Although the technology continues to grow at its own pace, its implementation has to be sustainable, giving due cognizance to the concerns of the ultimate beneficiaries: the end-users.

Bibliography

Allied Bus. Intelligence. “RFID White Paper,” 2002.

Avoine, G., and Oechslin, P. “A Scalable and Provable Secure Hash-Based RFID Protocol.” Pervasive Computing and Communications Workshops, Proceedings of the 3rd International Conference on, IEEE Computing Society, 2005.

Dimitriou, T. “A Secure and Efficient RFID Protocol that Could Make Big Brother (partially) Obsolete.” Pervasive Computing and Communications Workshops, Proceedings of the Fourth Annual IEEE International Conference, IEEE Computing Society, 2006.

Finkenzeller, K. *RFID: A Handbook.* 2nd Ed. Translated by R. Waddington. Munich: Wiley & Sons, 2005.

Floerkemeier, C., and Wille, M. “Comparison of Transmission Schemes for Framed ALOHA Based RFID Protocols.” Applications and the Internet Workshops, Proceedings of the International Symposium, IEEE Computing Society, 2005.

Garfinkel, S. L., Juels, A., and Pappu, R. “RFID Privacy: An Overview of Problems and Proposed Solutions.” *IEEE Security & Privacy* (May/Jun 2005): 34–43.

Golle, P., Jakobsson, M., Juels, A., and Syverson, P. “Universal Re-encryption for Mixnets.” Proceedings of the RSA Conference – Cryptographer's Track (CT-RSA), Lecture Notes in Computer Science, vol. 2964, pp. 163–178, 2004.

Hancke, G. P., and Kuhn, M. G. “An RFID Distance Bounding Protocol.” Security and Privacy for Emerging Areas in Communications Networks, Proceedings of the First International Conference, IEEE Computing Society, 2006.

Hernandez, P., Sandoval, J. D., Puente, F., and Perez, F. “Mathematical Model for a Multi-read Anticollision Protocol." Communications, Computers and Signal Processing, 2001. PACRIM. 2001 IEEE Pacific Rim Conference, vol. 2, pp. 647–650, August 2001.

Heydt-Benjamin, T. S., Bailey, D. V., Fu, K., Juels, A., and Hare, T. O. “Vulnerabilities in First-Generation RFID-enabled Credit Cards.” [DRAFT], RFID Consortium for Security and Privacy. 2006

Juels, A. “RFID Security and Privacy: A Research Survey.” *IEEE Journal on Selected Areas in Communications* 24, no. 2 (Feb 2006): 381–394.

Juels, A. “Strengthening EPC Tags Against Cloning.” Wireless Security, Proceedings of the 4th ACM Workshop, International Conference on Mobile Computing and Networking, pp. 67–76, 2005.

Juels, A. “Yoking-Proofs for RFID Tags." Pervasive Computing and Communications Workshops, Proceedings of the 2nd IEEE Annual Conference, pp. 138–143, Mar 2004.

Juels, A. and Weis, S. "Defining Strong Privacy for RFID." [IN SUBMISSION], International Association for Cryptologic Research, 2006.

Juels, A., Molnar, D., and Wagner, D. "Security and Privacy Issues in E-Passports." Security and Privacy for Emerging Areas in Communications Networks, 1st International Conference, SecureComm, pp. 74–88, Sept 2005.

Juels, A., Rivest, R. L., and Szydlo, M. "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy." Computer and Communications Security, ACM, Oct 2003.

Kim, I., Lee, B., and Kim, H. "Privacy Protection Based on User-defined Preferences in RFID System." International Conference on Advanced Communication Technology, pp. 858–862, Feb 2006.

Kim, I., Lee, B., and Kim, H. "Privacy-Friendly Mobile RFID Reader Protocol Design Based on Trusted Agent and PKI." Consumer Electronics, IEEE Tenth International Symposium, ISCE '06, pp. 1–6, Jun 2006.

Myung, J. and Lee, W. "Adaptive Binary Splitting: A RFID Tag Collision Arbitration Protocol for Tag Identification." Broadband Networks, 2005, 2nd International Conference, vol. 1, pp. 347–355, Oct 2005.

Phillips, T., Karygiannis, T., and Kuhn, R. "Security Standards for the RFID Market." *IEEE Security & Privacy* (Nov/Dec 2005): 85–86.

Poirier, C., and McCollum, D. *RFID: Strategic Implementation and ROI.* 1st Ed. Florida: J. Ross Publishing, 2006.

RSA Labs. "FAQ on RFID and RFID Privacy.". Accessed on December 2006, at http://www.rsasecurity.com/rsalabs/node.asp?id=2120.

RSA Labs. "Technical Characteristics of RFID." Accessed on December 2006, at http://www.rsasecurity.com/rsalabs/node.asp?id=2121.

Tsudik, G. "YA-TRAP: Yet Another Trivial RFID Authentication Protocol." Pervasive Computing and Communications Workshops, Proceedings of the Fourth Annual IEEE International Conference, IEEE Computing Society, 2006.

Weis, S. A. "RFID Privacy Workshop: Concerns, Consensus and Questions." *IEEE Security & Privacy*, Mar/Apr 2004: 48–50.

Xiao, Y., She, X., Sun, B., and Cai, L. "Security and Privacy in RFID Applications and Telemedicine." *IEEE Communications Magazine* (Apr 2006): 64–72.

Yan, H., Jianyun, H., Qiang, L., and Hao, M. "Design of Low-power Baseband-processor for RFID Tag." Applications and the Internet Workshops, Proceedings of the International Symposium, IEEE Computing Society, 2005.

Figure 1. A Sample Linear Barcode
(http://gfx.download-by.net/screen/16/16073-barcode-activex-linear-barcodes-by-wolf-software.jpg, Retrieved: Dec 2006)

Figure 2. A Sample 2D Data Matrix
(http://www.barcodetools.com/images/barcode/barcodetypes/2d/datamatrix.gif,
Retrieved: Dec 2006)

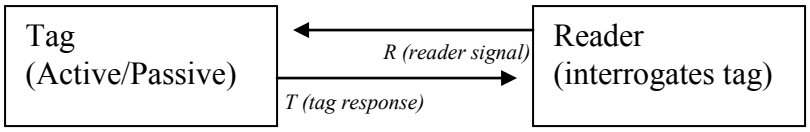

Figure 3. Basic RFID Communication

RFID Technology/ Protocol	FCC-defined frequency range (MHz)	General Use	Technical Features			Privacy	Security
			Band	Range (m)	Data Capacity		
EPC Class 0/0+	868-915	Supply Chain	Ultra High Frequency (UHF)	3	64 or 96 bit with Read/Write (R/W) block	None	* Parity Bit * CRC error detection
EPC Class 1/Gen 1	868-915	Supply Chain	UHF	3	64 or 96 bit with R/W block	None	* 5 Parity Bits * CRC error detection
EPC Class 1/Gen 2	868-915	Supply Chain	UHF	3	256 bit with R/W Block	* KILL operation using 8-bit key * Marked reader-to-tag communic-ations using one-time pad cipher * Tags addressed by 16-bit random numbers	* CRC error detection
ISO/IEC 18000-2	125 kHz	Item Management	Low Frequency (LF)	<0.01	< 1 kB R/W	None	* CRC error detection * Factory set 64 bit ID * LOCK ID

ISO/IEC 18000-3	13.56	Item Management	High Frequency (HF)	<2	R/W	* 48-bit password protection while READ-ing * QUIET mode	* CRC error detection * No WRITE protection in Mode1 * 48-bit WRITE password in Mode2
ISO/IEC 11784-85	125 kHz	Animal Tracking	LF	<0.01	64-bit ID	* 16-bit random numbers* QUIET mode	* Re-tagging counter * CRC error detection
ISO/IEC 10536/14443	13.56	Contact-less Smart Cards	HF	<2	R/W	* Masked reader-to-tag * Random number * QUIET mode	* CRC error detection
ISO/IEC 15693	13.56	Vicinity Smart Card	HF	1.5	<1kB R/W	None	* Protect-ion on WRITE command * Error checking on air interface

Figure 4. Types of Passive Tags – A General Overview

The major types of RFID tags and their protocols are listed above. (Allied Bus. Intelligence 2002; Garfinkel et al. 2005; Phillips et al. 2005; Xiao et al. 2006; Finkenzeller 2005)