RFID and Application Security

Lynn A. DeNoia and Anne L. Olsen

Department of Computer Science and Quantitative Methods
Winthrop University, Rock Hill, SC 29733, USA
Email: denoial@winthrop.edu and olsena@winthrop.edu

The question of how well radio-frequency identification (RFID) technology can maintain security in business applications continues to plague both information system developers and end-consumers. Today's RFID standards do not necessarily cover all of the desired security capabilities. In this paper we suggest characterizing potential applications of RFID in terms of a set of primitive functions (presence, access, transaction, matching, and proximity), each of which may require support from security mechanisms to ensure privacy, availability, integrity, and non-repudiation appropriately. A five-step process for assessing how well current technology meets application needs is defined and examples of its use provided.

ACM Classification: H.m (Information Systems): Miscellaneous

Keywords and Phrases: RFID, application, security, privacy, availability, integrity, non-repudiation

1. INTRODUCTION

As interest grows in using radio-frequency identification (RFID) technology to enhance various business applications and processes, concerns over the security implications become more important. RFID is a wireless technology that uses a tag and a tag reader to communicate with a backend database. Many applications use low-cost, read-only tags that transmit a serial number. Other applications use tags that contain descriptive data that gives much more detail than a single number. The ability to transmit larger amounts of information and the ability to transmit without being in the line of sight give RFID technology a major advantage over barcodes and some predict that RFID technology will one day replace bar codes (McGinty, 2004; Weis *et al*, 2003). Because radio waves transmit information, RFID applications are exposed to a variety of threats such as eavesdropping, spoofing, injection attacks, denial of service, and unreliable communication (Juels 2006; Hassan and Chatterjee, 2006). Complete planning for business applications of RFID must include identification of threats, provision of countermeasures, assessment of risk, and risk mitigation.

When considering application of new technologies such as RFID, cutting through the hyperbole and excitement to examine basic characteristics and requirements of both the application and the technology can reduce the associated risks of implementation. This paper presents an overview of the basics for reducing the risks of using RFID. We cover: what is meant by security, how applications use RFID, the security requirements for each RFID use, the available mechanisms for RFID security, limitations of current standards, and a plan for evaluating proposed RFID applications against security requirements and RFID capabilities. The focus is narrow, concentrating on the communication between RFID tags and readers, with sample references to an abundance of news and literature.

Manuscript received: 31 May 2008
Communicating Editor: Rei Safavi-Naini

2. SECURITY ELEMENTS

The basic requirements for security have long been considered to consist of maintaining privacy (or confidentiality), availability, and integrity. Recently non-repudiation has become equally important. While it is quite unlikely that any system can be made 100% secure, identifying the threats and assessing the risks are vital steps toward improving security. The specific threats associated with use of RFID technology in various applications have been widely discussed in the literature (Rieback *et al*, 2006c; Garfinkel *et al*, 2005). It is often stated that security is all about privacy, availability, integrity, and non-repudiation or "P.A.I.N."

Privacy means that data are not disclosed to unauthorized readers. Threats include potential for individual identification and tracking, corporate espionage, personal data exposure, etc. (Lee and Kim, 2006; Langheinrich, 2006).

Availability means that all system components necessary to capture and process tag data are available and do their jobs properly/appropriately. Threats include lost or missing data, actions or transactions refused or allowed inappropriately, inability to correlate data from multiple tagged items, etc. (Floerkemeier, 2006; Nash *et al*, 2005).

Integrity means that data are accurate, consistent, and not subject to unauthorized modification. Threats include inaccurate identification, bad counts, improper actions, inappropriate payments or billing, etc. (Rieback *et al*, 2006a; Rieback *et al*, 2006b; Lehtonen *et al*, 2006).

Non-repudiation means that if a tag was read, that tag, and only that tag, must have been present (that is, its presence cannot later be denied by either the tag holder or the reader). Threats include lost or missing verification and improper validation due to tag forgery, cloning, replay attacks, etc. (Ruland and Lohmann, 2007).

The sample references demonstrate that the specific threats associated with RFID technology have been and are being addressed as they are recognized. However, proposed solutions have been primarily discussed independently or for isolated applications. We believe a more holistic approach to RFID security is needed to enhance understanding of the risks and improve analysis of solution suitability to a broader range of applications.

3. RFID USES

In considering the use of RFID to support various business activities and applications, we identify the basic functions that depend specifically on RFID technology. These highlight the additional security concerns that must be addressed because RFID depends on active broadcast of data that might be subject to interception, interference, interruption, or corruption as no prior identification method could have been. Applications of RFID all employ some combination of the following "primitive" function (presence) and three derivative functions (action, correlation, history) that use tag data as described below.

A particular tag identifies itself to a specific reader at a particular location and time. This is the fundamental, primitive operation underlying all uses of RFID and is known as *presence*. The very concept of presence raises immediate concerns over security, encompassing all four areas of requirements: privacy, availability, integrity, and non-repudiation. Some applications will take advantage of presence simply by recording pertinent data from a read event. Others will find additional processing or use of the data to be more important.

Data read from a particular tag is used to trigger a direct *action*. Actions are generally one of the following:

- Access, where the particular tagged item or tag holder is permitted entry to or exit from a controlled facility (e.g., authorized tag unlocks door for building entry – requires integrity, availability, and in some cases, non-repudiation); and

- Transaction, where the particular tag allows/validates a specific monetary exchange (e.g., highway toll payment – requires integrity, availability, and in some cases, privacy).

Data read from two or more tags are correlated to validate/authorize, trigger, or deny some activity. *Correlation* can be further divided into:

- Matching, where two tags are checked to see if the combination is appropriate or permitted (e.g., medication intended for a specific patient arrives in the correct room for administration to that particular patient – requires integrity, availability, and in some cases, privacy); and
- Proximity, where a particular tag brought into combination with an existing set of other tags is checked for appropriateness (e.g., one more barrel of hazardous material is placed in a storage facility – requires availability and integrity). The new tag's data might then be recorded to update the context/environment for subsequent checks. Clearly, matching can be a degenerate case of proximity checking.

The function *history* saves a set of data recordings for a particular tag (or set of tags) over some period of time. The set of data is maintained for subsequent use (e.g., tracking of products through a supply chain).

4. SECURITY REQUIREMENTS

To address security completely, the key elements of an RFID application system that must be considered are: tags, readers, middleware (coordination and management of multiple readers), application software, database, and the end users. This paper focuses on tags and readers as critical RFID components rather than trying to tackle the larger, more general subjects of security for computer databases, software, hardware, networks, and users.

Identifying the security requirements of an application is the first step. Table 1 shows which security requirements are related to each RFID function given above with the exception of history. History is omitted because security would be provided primarily by the database environment and thus is beyond the scope of this paper. Note that the table is based on current expectations about how RFID might be used, and could need to be revised as other types of applications are developed. "Yes" entries in the table indicate that the security requirement (column) applies to applications identified in our survey of the literature and trade press using that RFID function (row), while "*" entries indicate that the requirement depends upon the specific application use of the corresponding function (as suggested by our survey of the literature). The table demonstrates that all applications need availability and integrity, while some may not be concerned with privacy or non-repudiation. Examples below provide additional explanation.

RFID FUNCTION	SECURITY REQUIREMENTS			
	PRIVACY	AVAILABILITY	INTEGRITY	NON-REPUD'N
Presence	*	Yes	Yes	*
Access	Yes	Yes	Yes	Yes
Transaction	Yes	Yes	Yes	Yes
Matching	*	Yes	Yes	*
Proximity	*	Yes	Yes	*

Table 1: Security Requirements by RFID Application Function

A wide range of asset management applications can be built capitalizing on the RFID presence function. All applications need availability to be sure tags get read and integrity to ensure accurate information. Tracking an inventory of tagged consumer products through a warehouse might not need non-repudiation (except for goods of particularly high value), but companies concerned about competitors tracking the flow of goods would want privacy. If the stored goods were hazardous materials instead, privacy might be less important because their presence must often be advertised visibly, or more important to protect details (specific materials or quantities) from potential thieves and saboteurs. Non-repudiation might be required for a presence history to ensure a chain of custodial accountability. Presence is also useful when a tag is applied to one half of a medical coupler and a reader to the other half, such as coupling the feed from an oxygen tank to a patient face mask, to ensure that the wrong type of gas cannot be mistakenly connected (Bacheldor, 2006). It is not likely that privacy would be needed for coupling devices, but non-repudiation might be desired to create an audit trail (history). Tracking tagged surgical items before and after an operation would generally not need either privacy or non-repudiation if the goal was to ensure nothing got left inside a patient. However, privacy for tracking the location of expensive, specialty medical equipment might be desired to thwart potential theft (Xiao *et al*, 2006). As an enhanced version of inventory management, supply chain management requirements for privacy depend on the specific application but non-repudiation is likely required at the boundaries between enterprises along the chain, to validate shipping and receiving (Ilic *et al*, 2007; Gao *et al*, 2004; Swedberg, 2006).

A different way to use RFID presence is in targeted marketing applications. For example, a store door reader, sensing the presence of any approaching tag, could trigger broadcast or display of general advertising messages. If the tag belonged to a store-specific brand or other item, the message could be targeted. In Prada's New York Epicenter store, for example, customers can present a Prada customer card (containing an RFID chip) to signal their arrival to a preferred sales associate (RFID Journal, 2002). Gedenim has placed kiosks in their Paris stores to provide tailored information and services to loyalty card holders (Swedberg, 2007). Prada has also attached tags to clothes in order to help sell the items to customers. When a customer takes an item into the fitting room, the tag triggers a fashion show specific to that item (McGinty, 2004).

Next we consider applications that would use the RFID access function. An RFID car key could trigger locking the vehicle after the driver door opens and the tagged car key moves beyond a one-foot external range, or trigger unlocking the vehicle as an action response to the key's external appearance within one foot of the door lock reader. Privacy would definitely be required, both to protect exchanges from replay attacks and to authenticate the key with the lock (Vamosi, 2006). A similar application would be buildings or spaces with keyless door locks, but in this case, non-repudiation might also be needed depending on how the history of individual accesses might be used (Collins, 2006b). A reverse application might be a retail store with door readers that sound an alarm if a tagged retail item passes by or a home reader that sounds an alarm when a child wearing tagged clothing crosses a home boundary limit (Duvall, 2006).

Applications that use the RFID transaction function generally focus on using a tagged item to trigger a monetary exchange. The most common examples to date include highway toll payments and gasoline purchases. Such applications require both privacy and non-repudiation to protect the financial transaction (Brofman, 2006; Eckfeldt, 2005; O'Connor, 2007; McGinty, 2004).

The health care industry is one example of creative use of the RFID matching function. For example, a hospital pharmacy can package medications for a particular patient in a tagged container that will be checked for matching a patient ID tag before medicine is administered (Wu *et al*, 2005; Wessel, 2006). In a closed hospital setting, privacy might not be needed for this application while non-repudiation could be used for audit purposes. If every patient (or bed) had a reader and all hospital personnel had tagged identification, a complete history of all attending visits (e.g., doctors, nurses, aides) could be created for each patient (Xiao *et al*, 2004). Again, non-repudiation could be required for this type of tracking, while privacy would be needed only for the recorded history in the database.

Real-time monitoring for safety is one way to use the RFID proximity function. For example, consider the safe storage of hazardous materials, as ruled by industry or governmental regulations. With each container tagged to indicate the type and quantity of contents, its introduction and placement in a specific storage location can be combined with information about other items already stored in that area to ensure adding the new container conforms to all safety rules (Cordis, 2006). If not, an alarm could be sounded so that the container is not left in that location. Appropriate removal of a container would be verified by a subsequent read operation. In this case, privacy would seem useful to protect materials from potential thieves or saboteurs. The need for non-repudiation more likely depends on the types of materials being stored.

5. SECURITY PROVISIONS

Once the security requirements of an application are identified, the method of providing that security needs to be determined. In this section we examine the capabilities of RFID technology. The literature discusses many kinds of mechanisms that could be used by RFID tags and readers to fulfill security requirements (Karygiannis *et al*, 2007; Rieback *et al*, 2006c; Gao *et al*, 2004). For the P.A.I.N. security categories discussed above, we suggest some RFID mechanisms to use in protecting against typical threats. References are meant to be examples and not a comprehensive bibliography.

The fundamental threat to privacy is that tag data will be captured and used by an unauthorized reader, leading to various inappropriate or unwanted activities such as: identification, location, tracking, matching, disclosure of related data, etc. (Garfinkel *et al*, 2005). Such activities may constitute corporate espionage, remote surveillance of individuals, or capture of personal information (Neuman and Weinstein, 2006). To protect against unauthorized reading, we recommend considering:

- minimizing the distance between tags and authorized readers to reduce the likelihood that unauthorized readers can overhear the transmissions exchanged (Garfinkel *et al*, 2005) or to help distinguish unauthorized from authorized readers (Queisser *et al*, 2006)
- shielding, such as a Faraday cage applied directly around tags (Kirk, undated) or to a limited environment in which readers can exchange data with tags (Karygiannis *et al*, 2007)
- protected commands to turn a tag on and off or to kill it forever once it leaves the vicinity of an authorized reader (Ohkubo, Suzuki, and Kinoshita, 2005), or physical on/off controls (Collins, 2006a)
- destruction of the tag once it has served its primary purpose so that it cannot be abused later (Karjoth and Moskowitz, 2005)
- cover coding for communication between tags and reader to interfere with an unauthorized reader's ability to extract information from exchanges (Karygiannis *et al*, 2007)
- encryption of data stored on the tag or communicated between tag and reader to prevent use of any unauthorized data capture (Kaps *et al*, 2007)
- introduction of noise into the reading environment to reduce the likelihood that an unauthorized reader can distinguish the exchanges for a particular tag being read (Juels *et al*, 2003)

- use of authentication mechanisms (from simple passwords to sophisticated multi-factor techniques) to identify authorized readers (Engberg *et al*, 2004; Lehtonen *et al*, 2006)

Availability means that all necessary components of the system can perform their functions properly at the time and place required. Lack of availability means that tags are not read/recognized or tag data are not captured when they should be. Availability can be compromised by component or system failures, readers not fast enough to keep up with the speed or volume of passing tags, or denial of service attacks. Tags that cannot be read due to orientation or intervening opaque materials are beyond the scope of this paper. Recommendations to mitigate availability threats have generally been focused on specific issues rather than offering broad-based approaches. Types of proposals include using:

- reliable design techniques with redundant components to minimize the probability of outages or overload
- 'fast' readers or techniques (Floerkemeier, 2006; Magellan Technology, 2006) and physical controls (Karygiannis *et al*, 2007) to minimize the chance of tags getting past a reader without being properly identified
- intrusion detection systems (IDS) to prevent attacks such as those causing battery exhaustion (for an example, see Nash *et al*, 2005)

Integrity encompasses keeping data content accurate, complete, and consistent, as it is captured from tags or exchanged between tags and readers. This means nothing is missed or lost, no counterfeits are accepted, all changes are made accurately and only by authorized entities, and no malware is introduced. Protection for integrity generally entails providing redundant information for error detection, rejecting counterfeits and detecting/rejecting replay attacks, authenticating before changes are made, and logging of change activity for auditing purposes. We recommend investigating the following mechanisms and further discussion of issues:

- checksums, hashing (Lee, Asano, and Kim, 2006; Burmester, van Lee, and de Medeiros, 2006), and digital signatures for error/change detection
- protection from cloning (Juels, 2005; Dimitriou, 2005)
- tag and/or reader authentication (Kathikeyan and Nesterenko, 2005; Cui *et al*, 2007)
- potential for malware infection through data captured from tag reads (Rieback *et al*, 2006a; Rieback *et al*, 2006b)

A typical barrier in many privacy and integrity protection approaches is the limited power and data storage capacity that are characteristic particularly of today's inexpensive passive tags. A growing amount of research (e.g., Weis, 2005; Ruland and Lohmann, 2007) is focused on providing security within such limitations.

For the purposes of this paper, non-repudiation threats include claims that a particular tag was or was not present at a particular place and time and claims that a particular reader did or did not read a specific tag's data. As in more general security scenarios, digital signatures are recommended to counter non-repudiation threats. The challenge with RFID is once again to work within the limited computational and storage capabilities, especially for passive tags (Ruland and Lohmann, 2007).

6. SCOPE AND ROLE OF STANDARDS

Standards for RFID technology have come primarily from two directions, EPCglobal and ISO 18000.

EPCglobal (www.epcglobalinc.org) is a nonprofit, membership organization dedicated to developing industry standards for the electronic product code replacement/augmentation to traditional bar codes and to promoting the use of RFID throughout the retail supply chain. It is the successor to the Auto-ID Center started originally at MIT and published its first specifications from that earlier work. The current scope of coverage includes (EPCglobal, 2005):

- Class 0: tags operating at 900 MHz (UHF)
- Class 1, Generation 1: tags operating at 13.56 MHz (HF), with range up to 1 metre; and tags using the 860-960 MHz (UHF) band that is more suitable for item management
- Class 1, Generation 2: tags provide a kill command, optional password protection, optional user memory, cover coding, lock command (temporary or permanent) for write or read/write protection of a memory area

EPCglobal's Class 1, Generation 2 air interface protocol was approved in June 2006 as ISO 18000-6c and published as an amendment, thus officially becoming an international standard.

The formally accepted standards for RFID have been developed through the International Organization for Standardization's (ISO) joint technical committee with the International Electrotechnical Commission (IEC), JTC 1 (Information Technology). Subcommittee SC31 (automatic identification and data capture techniques) is responsible for the standards family 18000 (radio frequency identification for item management), which currently includes:

- 18000-1, reference architecture and definition of parameters to be standardized
- 18000-2, parameters for air interface communications below 135 kHz (range < 0.01 m, with frequency approved worldwide for industrial, scientific, and medical, ISM, applications)
- 18000-3, parameters for air interface communications at 13.56 MHz (frequency approved worldwide for ISM applications)
- 18000-4, parameters for air interface communications at 2.45 GHz (approved ISM frequency but may conflict with microwave ovens)
- 18000-6, parameters for air interface communications at 860 MHz to 960 MHz (approved ISM frequency range is only 902-928 MHz; conflicts with cordless and cellular telephones in some countries)
- 18000-7, parameters for active air interface communications at 433 MHz

Thus the standards of interest for use in applications suggested by this paper are limited in practice to 18000-3 and 18000-6. Other ISO standards such as 11784/11785 for animal tracking, 14443 for contactless smart cards, and 15693 for vicinity smart cards are outside the scope of this paper.

Table 2 shows what the two standards of interest provide as mechanisms to handle each of the security requirements described above. We find numerous important mechanisms that are not specified by today's standards, with the most notable deficiencies being encryption, intrusion detection, anti-cloning, anti-malware, and digital signature capabilities. In addition, standard authentication offers only password protection, which may or may not be sufficient in various application scenarios. Such limitations need to be considered carefully in each application context before RFID is deemed suitable for adoption.

A comprehensive and detailed comparison of the full scope of these standards has been published by the Global RFID Interoperability Forum for Standards (GRIFS) in order "to improve collaboration in RFID standardization and thereby to improve the global consistency of RFID standards" (Chartier and van den Akker, 2008).

	EPCglobal Class 1 Gen 2	ISO 18000-3
	(ISO 18000-6c)	(Karygiannis *et al*, 2007)
PRIVACY		
Distance minimization or checking	Read range up to ~10 m	Read range < 2 m
Shielding tags or environs	<not included>	<not included>
On/off commands	Lock command for temporary or permanent write-protect or read/write-protect of a memory area	Memory blocks can be permanently locked; Mode 2 also provides memory write protection
Kill command	included	<not included>
Tag destruction	<application issue>	<application issue>
Cover coding	included	<not included>
Encryption	<not included>	<not included>
Noise	<not included>	<not included>
Authentication	Optional 32-bit kill password and 32-bit access password, individually lockable	Password protection for read commands and for write commands
AVAILABILITY		
Reliable design	<implementation issue>	<implementation issue>
Fast readers (Magellan Technology, 2006)	Complex anti-collision mechanism	Simple anti-collision mechanism; theoretical read ~1200 tags/sec and 800/sec in real applications
Intrusion detection	<not included>	<not included>
INTEGRITY		
Checksums, hashing, digital signatures	CRC-16 error detection (except query is CRC-5) only	CRC-16 error detection; Mode 2 uses 16-bit for commands, 32-bit in replies (Magellan Technology, 2006)
Anti-cloning protection	<not included>	<not included>
Authentication	Optional 32-bit kill password and 32-bit access password, individually lockable	Mode 2 has password protection for read commands and for write commands
Anti-malware protection	<not included>	<not included>
NON-REPUDIATION		
Digital signatures	<not included>	<not included>

Table 2: Security Mechanisms Included in Standards Specifications

7. TECHNOLOGY READINESS TO MEET APPLICATION NEEDS

Given the broad interest in RFID, we propose a simple process for determining whether the technology is ready to handle the requirements of a particular application:

a) Decompose the application into a sequence of RFID functions as those described above (presence, access, matching, transaction, proximity)

b) Determine the security requirements that pertain to each use of each RFID function
c) Evaluate standards and products to select from the available mechanisms those which best meet the application requirements
d) Using the P.A.I.N. threat definitions above, assess the risks associated with all requirements that are not fully met (i.e., estimate the probabilities of occurrence and the impact or scope of

APPLICATION	SECURITY MECHANISMS			
	PRIVACY	AVAILABILITY	INTEGRITY	NON-REPUDIATION
Inventory, low value (presence)	Cover coding, noisy environs, encryption, reader authentication	Reliable design, fast readers, IDS	Checksums, anti-cloning, anti-malware	Not needed
Inventory, high value (presence)	Encryption, tag & reader authentication	Reliable design, fast readers, IDS	Hashing, anti-cloning, anti-malware	Digital signature
Medical couplers (presence)	Limited distance, cover coding	Reliable components	Checksums, anti-cloning	Not needed
Targeted marketing (presence)	Cover coding, noisy environs, shielding	Reliable design	Checksums, anti-cloning	Not needed
Keyless entry, car (access)	Encryption, authentication	Reliable components	Checksums, anti-cloning	Not needed
Keyless entry, low-security building (access)	Cover coding and shielding	Reliable design, fast readers, IDS	Checksums, anti-cloning, anti-malware	Not needed
Keyless entry, high-security building (access)	Encryption and authentication	Reliable design, fast readers, IDS	Checksums, anti-cloning, anti-malware	Digital signature
Boundary alarm, child (access)	Encryption, authentication	Reliable design, IDS	Checksums	Not needed
Retail door alarm (access)	Shielding	Reliable design, fast readers, IDS	Checksums, anti-cloning, anti-malware	Not needed
Financial (transaction)	Encryption, authentication	Reliable design, fast readers, IDS	Checksums, anti-cloning, anti-malware	Digital signature
Hospital pharmacy (matching)	Cover coding, limited distance	Reliable design	Checksums, anti-cloning, anti-malware	Digital signature
Hospital patient attending (matching)	Cover coding, limited distance (if needed at all)	Reliable design, IDS	Checksums, anti-cloning, anti-malware	Digital signature
Hazardous-materials storage (proximity)	Encryption, authentication	Reliable design, fast readers, IDS	Checksums, anti-cloning, anti-malware	Digital signature (if needed)

Table 3: Suggested Security Mechanisms for Sample RFID Applications

damage for each, then determine severity by multiplying the two factors together)

e) Balance the estimated risk and added costs against projected benefits and decide whether or not to implement using the available technology

Table 3 provides a sample overview of results from steps a and b for various applications when considering only the primary RFID function necessary for each. Using a detailed tabulation for a particular application would provide the evaluation criteria in step c to select suitable products. It's important to recognize that steps c–e are all snapshots in time, based specifically on product capabilities, implementer expectations, and general market/consumer readiness.

Using the low-value inventory application as an example, Table 3 recommends cover coding, noisy environs, encryption, and reader authentication as the mechanisms to address privacy in step c. Table 2 shows that the ISO 18000-6c standard includes cover coding and an optional 32-bit access password but not noise or encryption mechanisms, while ISO 18000-3 includes only password protection for read/write commands. Cover coding protects information and commands from reader to tag (e.g., passwords and commands) while noisy environs would protect the weaker signals from tag to reader (for the passive tags likely to be used in this application). If the primary threat is expected to be from unauthorized readers outside the facility (where reader-to-tag distances are greater than for authorized readers), it is more likely that reader transmissions would be overheard than tag transmissions. This makes cover coding important and favors products that conform to 18000-6c for privacy.

Each application requirement would be assessed similarly as part of step c. Using Table 3 for requirements and Table 2 for mechanisms, we find 18000-3 preferable for availability (faster reads) and little difference between the standards for integrity (both supporting only checksums), with non-repudiation not being required for low-value inventory. Standard/product selection would thus depend on the relative importance of cover coding for privacy and fast reads for availability.

Step d of the process is often difficult because it requires assumptions, any of which might have its validity called into question. We recommend addressing this issue by creating three levels of risk assessment: optimistic case, most likely case, and pessimistic case for each identified threat. Table 4 presents a sample for the loss of privacy in our low-value inventory situation where a competitor uses stolen data to anticipate an out-of-stock condition on a popular item. Note that assumptions must be presented with the risk calculations to support credibility. Complexity increases if multiple threats need to be combined into larger impact models or unanticipated, generic threats need to be included.

CASE	PROBABILITY OF OCCURRENCE	IMPACT OR SCOPE OF DAMAGE	SEVERITY
Optimistic	2%	$2,000	$40
Most Likely	5%	$8,000	$400
Pessimistic	10%	$32,000	$3,200

ASSUMPTIONS:

- Competitor runs promotion on low-stock item that takes time to re-order
  Optimistic: lost sales of 100 items @ $20
  Most Likely: lost sales of 400 items @ $20
  Pessimistic: lost sales of 1600 items @ $20

Table 4: Sample Risk Assessment Summary for Loss of Privacy to a Competitor

In step e, costs from particular standard and product selections in step c and risks from the analysis of step d are balanced against the benefits of using RFID technology. If pilferage is high and use of RFID can reduce losses more than any other approach and more than it increases risk, then proceeding to use RFID in our low-value inventory example would be worthwhile.

Keep in mind that the five-step process proposed here was developed from a very narrow focus on communication between RFID tags and readers without considering the many issues related to security of the other elements of any application system (host/server, database, network, users, etc.). RFID capabilities for security are only part of a much larger approach to making an application secure and RFID mechanisms can be only one piece of a complete solution (McLean, 2003).

8. CONCLUSIONS

In this paper we presented an overview of some of the security requirements for applications using RFID technology. We suggest a five step process to evaluate the security requirements of the RFID application and give some examples to show how the process might be used. Consideration of how the RFID technology itself can provide the desired level of security is one important step in the process of choosing the mechanism that will ultimately be used to make an application secure. Although some standards have been established, the ever-expanding use of RFID technology indicates there is an increasing need to improve standards and take all the steps necessary to provide security.

9. REFERENCES

BACHELDOR, B. (2006): Medical-tube couplings get RFID technology. RFID Journal. http://www.rfidjournal.com/article/articleprint/2423/-1/1/. Accessed 21-Jun-2006.

BROFMAN, F. (2006): Loyalty programs redesign among RFID lines, some examples from industries. IDS Packaging (24-Apr-2006). http://www.idspackaging.com/packaging/us/loyalty_programs/267/paper_information.html. Accessed 21-Jun-2006.

BURMESTER, M., VAN LEE, T. and DE MEDEIROS, B. (2006): Provably secure ubiquitous systems: Universally composable RFID authentication protocols. Florida State University. http://www.cs.fsu.edu/research/reports/TR-060112.pdf. Accessed 9-Jun-2007.

CHARTIER, P. and VAN DEN AKKER, G. (2008): D1.3 RFID standardization state of the art report, Version 1, GRIFS, November.

COLLINS, J. (2006a): E-passport tag comes with switch. *RFID Journal* (23 May 2006). http://www.rfidjournal.com/article/articleprint/2361/-1/1/. Accessed 25-May-2006.

COLLINS, J. (2006b): NFC-enabled phones to unlock hotel rooms. *RFID Journal* (23-Jun-2006). http://www.rfidjournal.com/article/articleprint/2451/-1/1. Accessed 23-Jun-2006.

CORDIS (2006): Taking sensor network technology to a smarter level. *IST Results*. http://www.cordis.lu/ist/results. Accessed 27-Jun-2006.

CUI, Y., KOBARA, K., MATSUURA, K. and IMAI, H. (2007): Lightweight asymmetric privacy-preserving authentication protocols secure against active attack. *Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07)*. IEEE Computer Society.

DIMITRIOU, T. (2005): A lightweight RFID protocol to protect against traceability and cloning attacks. *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURE-COMM'05)*. IEEE Computer Society.

DUVALL, M. (2006): Lauren Scott California: At the seams of RFID. *Baseline Magazine* (6-Apr-2006). http://www.baselinemag.com/article2/0,1397,1948608,00.asp. Accessed 15-May-2006.

ECKFELDT, B. (2005): What does RFID do for the consumer? *Communications of the ACM* 48 (9): 77–79.

ENGBERG, S., HARNING, M. and JENSEN, C. (2004): Zero-knowledge device authentication: Privacy & security enhanced RFID preserving business value and consumer convenience. *Second Annual Conference on Privacy, Security and Trust (PST2004)*. http://www.obiagent.net/Papers/PST2004_RFID_ed.pdf. Accessed 8-Jun-2007.

EPCGLOBAL (2005): EPC™ radio-frequency identity protocols Class-1 generation-2 UHF RFID protocol for communications at 860 MHz – 960 MHz Version 1.09. EPCglobal Inc., ©2004, 31 January 2005.

FLOERKEMEIER, C. (2006): Transmission control scheme for fast RFID object identification. *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)*. http://csdl2.computer.org/dl/proceedings/percomw/2006/2520/00/25200457.pdf. Accessed 11-Jun-2007.

GAO, X., XIANG, Z., WANG, H., SHEN, J., HUANG, J. and SONG, S. (2004): An approach to security and privacy of RFID system for supply chain. *Proceedings of the IEEE International Conference on E-Commerce Technology for*

Dynamic E-Business (CEC-East'04): 164-168. http://csdl2.computer.org/dl/proceedings/cec-east/2004/2206/00/22060164.pdf. Accessed 15-May-2006.

GARFINKEL, S., JUELS, A. and PAPPU, R. (2005): RFID privacy: an overview of problems and proposed solutions. *IEEE Security and Privacy* 3 (3): 34–43.

HASSAN, T. and CHATTERJEE, S. (2006): A taxonomy for RFID. *Proceedings of the 39th Hawaii International Conference on System Sciences (2006)*. IEEE, 10.

ILIC, A., MICHAHELLES, F. and FLEISCH, E. (2007): Dual ownership: Access management for shared item information in RFID-enabled supply chains. *Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07)*. http://csdl2.computer.org/dl/proceedings/percomw/2007/2788/00/27880337.pdf. Accessed 11-Jun-2007.

JUELS, A. (2006): RFID security and privacy: a research survey. *IEEE Journal on Selected Areas in Communications* 24 (2): 381–394.

JUELS, A. (2005): Strengthening EPC tags against cloning. *Proceedings of the 4th ACM Workshop on Wireless Security (WiSE'05)*: 67–75. ACM Press.

JUELS, A., RIVEST, R. and SZYDLO, M. (2003): The blocker tag: Selective blocking of RFID tags for consumer privacy. *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS'03)*: 103–111.

KAPS, J.-P., GAUBATZ, G. and SUNAR, B. (2007): Cryptography on a speck of dust. *Computer* 40 (2): 38–44.

KARJOTH, G. and MOSKOWITZ, P. (2005): Disabling RFID tags with visible confirmation: Clipped tags are silenced. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES'05)*: 27–30. ACM.

KARYGIANNIS, T., EYDT, B., BARBER, G., BUNN, L. and PHILIPS, T. (2007): Guidelines for securing radio frequency (RFID) identification systems, Special Publication 800–98, National Institute of Standards and Technology, April.

KATHIKEYAN, S. and NESTERENKO, M. (2005): RFID security without extensive cryptography. *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'05)*: 63–67. ACM Press.

KIRK, D. (undated): NEW RFID blocking wallet. http://www.rpi-polymath.com/ducttape/RFIDWallet.php. Accessed 15-May-2006.

LANGHEINRICH, M. (2006): RFID and privacy. Distributed Systems Group, ETH, Zurich. http://www.vs.inf.ethz.ch/publ/papers/langhein2006rfidprivacy.pdf. Accessed 8-Jun-2007.

LEE, H. and KIM, J. (2006): Privacy threats and issues in mobile RFID. *Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)*: 510-514. IEEE Computer Society. http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/&toc=comp/proceedings/ares/2006/2567/00/2567toc.xml&DOI=10.1109/ARES.2006.96. Accessed 8-Jun-2007.

LEE, S., ASANO, T. and KIM, K. (2006): RFID mutual authentication scheme based on synchronized secret information. *2006 Symposium on Cryptography and Information Security*. Institute of Electronics, Information and Communication Engineers. http://caislab.icu.ac.kr/Paper/paper_files/2006/SCIS_Lee.pdf. Accessed 8-Jun-2007.

LEHTONEN, M., STAAKE, T., MICHAHELLES, F. and FLEISCH, E. (2006): From identification to authentication – A review of RFID product authentication techniques. Workshop on RFID Security (RFIDSec06), Graz, Austria, 12-14 July 2006. http://events.iaik.tugraz.at/RFIDSec06/Program/papers/010%20-%20Product%20Authentication%20Techniques.pdf. Accessed 8-Jun-2007.

MAGELLAN TECHNOLOGY (2006): White paper: A comparison of RFID frequencies and protocols. Magellan Technology (31 Mar 2006). http://www.rfidjournal.com/whitepapers/download/113. Accessed 21-Jun-2006.

McGINTY, M. (2004): RFID: Is This game of tag fair play? *Communications of the ACM* 47(1):15–18.

McLEAN, P. (2003): A secure pervasive environment, from the Australasian Information Security Workshop 2003 (AISW2003), *Conferences in Research and Practice in Information Technology* 21, Australian Computer Society Inc.

NASH, D., MARTIN, T., HA, D. and HSIAO, M. (2005): Towards an intrusion detection system for battery exhaustion attacks on mobile computing devices. *Proceedings of the Third Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'05)*. http://csdl2.computer.org/comp/proceedings/percomw/2005/2300/00/23000141.pdf. Accessed 11-Jun-2007.

NEUMAN, P. and WEINSTEIN, L. (2006): Risks of RFID. *Communications of the ACM* 49 (5): 136.

O'CONNOR, M. (2007): Sunway Lagoon Issues RFID Wristbands for admission, Purchases. RFID Journal (10-Jul-2007). http://www.rfidjournal.com/article/articleprint/3469/-1/1/. Accessed 10-Jul-2007.

OHKUBO, M., SUZUKI, K. and KINOSHITA, S. (2005): RFID privacy issues and technical challenges. *Communications of the ACM* 48 (9): 69–71.

QUEISSER, M., DAUTERMANN, F., GUERRERO, P., CILIA, M. and BUCHMANN, A. (2006): Cataloging RFID privacy and security. Technische Universitat Darmstadt. http://www.dvs1.informatik.tu-darmstadt.de/publications/pdf/Queisser_2006_RFIDPnS.pdf. Accessed 8-Jun-2007.

RFID JOURNAL (2002): Learning from Prada. *RFID Journal* (24 Jun 2002). http://www.rfidjournal.com/article/articleview/272. Accessed 9-Jul-2007.

RIEBACK, M., CRISPO, B. and TANENBAUM, A. (2006a): Is your cat infected with a computer virus? *Proceedings of the Fourth Annual International Conference on Pervasive Computing and Communications (PERCOM'06)*: 169–179. http://csdl2.computer.org/dl/proceedings/percom/2006/2518/00/25180169.pdf. Accessed 17-May-2007.

RIEBACK, M., CRISPO, B. and TANENBAUM, A. (2006b): RFID Malware: Truth vs. myth. *IEEE Security and Privacy* July: 70-72. http://csdl2.computer.org/dl/mags/sp/2006/04/j4070.pdf. Accessed 11-Jun-2007.

RIEBACK, M., CRISPO, B. and TANENBAUM, A. (2006c): The evolution of RFID security. *IEEE Pervasive Computing* Jan-Mar: 62-69. http://csdl2.computer.org/dl/mags/pc/2006/01/b1062.pdf. Accessed 17-May-2006.

RULAND, C. and LOHMANN, T. (2007): Digital signatures based on elliptic curves in RFIDs. *International Journal of Computer Science and Network Security (IJCSNS)* 7 (1): 275–281.

SWEDBERG, C. (2006): ExploTrack launches e-Pedigree platform for explosives. *RFID Journal*: 16-Jun-2006. http://www.rfidjournal.com/article/articleprint/2400/-1/1/. Accessed 16-Jun-2006.

SWEDBERG, C. (2007): French Jean Boutique adopts RFID to boost loyalty. *RFID Journal*. http://www.rfidjournal.com/article/articleprint/3472/-1/1/. Accessed 13-Jul-2007.

VAMOSI, R. (2006). Gone in 60 seconds—the high-tech version. *CNET Reviews* (5-May-2006). http://reviews.cnet.com/4520-3513_7-6516433-1.html. Accessed 15-May-2006.

WEIS, S.A. (2005): Security parallels between people and pervasive devices. *Proceedings of the 3rd Int'l Conf. on Pervasive Computing and Communication Workshops (PerCom 2005 Workshops)*. IEEE.

WEIS, S.A., SARMA, S.E., RIVEST, R.L. and ENGELS, D.W. (2003): Security and privacy aspects of low-cost radio frequency identification systems. *Security in Pervasive Computing*: LNCS 2802: 201–212.

WESSEL, R. (2006): German hospital expects RFID to eradicate drug errors. *RFID Journal* (9-Jun-2006). http://www.rfidjournal.com/article/articleprint/2415/-1/1/. Accessed 21-Jun-2006.

WU, F., KUO, F. and LIU, L. (2005): The application of RFID on drug safety of inpatient nursing healthcare. *Proceedings of the seventh international conference on electronic commerce (ICEC'05)*. ACM Press. http://delivery.acm.org/10.1145/1090000/1089571/p85-wu.pdf?key1=1089571&key2=6992043811&coll=ACM&dl=ACM&CFID=27283171&CFTOKEN=81196464. Accessed 8-Jun-2006.

XIAO, Y., SHEN, X., SUN, B. and CAI, L. (2004): Security and privacy in RFID and applications in telemedicine. *IEEE Communications* 44 (4): 64–72.

BIOGRAPHICAL NOTES

Lynn A. DeNoia

Lynn A. DeNoia is a professor of computer science at Winthrop University in Rock Hill, South Carolina, USA. She received her PhD in Computer Science from Brown University and has varied professional experience as a chief information officer, consultant, network and network management architect. Her research interests include effective management of information and technology resources, IT valuation techniques, network architecture, and RFID applications. Academic and professional publications cover a range of topics from networking to IT management to curriculum and pedagogy, including chapters on wide area and metropolitan area networks in The Internet Encyclopedia *and* The Handbook of Information Security.

Anne L. Olsen

Anne L. Olsen is an associate professor of Computer Science at Winthrop University in Rock Hill, South Carolina, USA. She holds the PhD in Information Technology from the University of North Carolina at Charlotte. She has developed and taught courses in a number of areas including software engineering and data management. Her research areas include evolutionary algorithms, software engineering, and RFID applications. Publications include articles in the International Journal of Production Economics, Computers & Industrial Engineering, *and in* Lecture Notes in Computer Science.