# Privacy and Security Aspects of RFID Tags

**Dong-Her Shih**

Department of Information Management,

National Yunlin University of Science and Technology,

123, Section 3, University Road, Douliu, Yunlin, Taiwan

Cell Phone:(886)932-690178

Fax:(886)5-5312077

Email: shihdh@yuntech.edu.tw

**Chin-Yi Lin**

Department of Information Management,

National Yunlin University of Science and Technology,

123, Section 3, University Road, Douliu, Yunlin, Taiwan

Email: g9223744@yuntech.edu.tw

**Binshan Lin**

College of Business Administration,

Louisiana State University in Shreveport, Shreveport, LA 71115 USA

Phone: 318-797-5025

Fax: 318-797-5127

Email: blin@pilot.lsus.edu

## ABSTRACT

*RFID has recently received a lot of attention as an augmentation technology in manufacturing, SCM and retail inventory control. However, widespread deployment of RFID tags may create new threats to security and privacy of individuals and organizations. This paper gives an overview of all types of RFID privacy and security problems and its countermeasures.*

# 1 INTRODUCTION

Radio Frequency Identification is another step towards fully automatic identification systems. The technology promises faster, reliable and more accurate identification of goods marked with RFID-tags. The technology gives itself a wide range of uses. The first traditional technology to be replaced by RFID is the bar code system – RFID can do everything bar codes can and much more (Johansson, 2004). Optical barcodes suffer from several drawbacks. First, human intervention is required to scan a barcode. Objects must be physically manipulated to align barcodes with scanners. Anyone who has shopped in market has likely witnessed a cashier struggling to scan an item. Second, the readability of barcodes could be affected by dirt, moisture, abrasion, or packaging contours. Third, the ability of storing data on barcode is very low. Fourth, retailers also often affix barcodes which are unnecessary for them on top of packaging of goods. The last, the barcodes is easy to be counterfeited and so on. These issues limit the performance of optical barcode based on auto-ID systems. Today, over 5 billion bar codes are scanned daily world-wide (Weis *et al.*, 2004), (Juels and Pappu, 2003) and this is just one operation which RFID technology is predicted to take over. The actual idea of RFID has been around since 1960 (Weigart, 2000) (Royal Air Force, 1940).

RFID supporters claim to see an integration of RFID in all businesses. In the world of RFID Walmart (Anderson and Kuhn, 1997) is currently the strongest advocate promoting this new way to identify everything that can be marked with a tag. Walmart encourages its suppliers to adopt the technology by 2005, at the latest, for identification at case level (Juels, 2004). Main competitors to Walmart – e.g. Tesco and Metro group – follow close behind, and cooperate to a certain extent in evaluating and implementing RFID at trial sites. The Metro Group operates “next-generation” supermarket in Rheinberg, Germany, with RFID implemented, where benefits of the technology have been seen (Weis et al., 2004).

With RFID, new uses of identification and collection of data about movements of items will be possible; also, it is understandable that major interest is given to issues of information security and privacy. Lack of assurance regarding privacy and information security is one of the remaining obstacles for widespread usage of RFID (Juels, 2004). RFID still can be done without security assurance if individuals do not have to worry about forsaking their privacy. Many issues related to information security and privacy within RFID systems is inherited through using already known technology and methods (Aljifri and Tyrewalla, 2004). However there are many new issues, especially regarding personal privacy that need to be discussed. Along with the advances of RFID there are many consumer rights and privacy rights groups protesting against trial sites of RFID and appealing to courts for stricter regulations on the use of RFID. Also, the impact and barriers of mobile commerce (Tan et al.,

2003) (Anil et al., 2003) take into account are considered. Today RFID is in use at production and assembly sites, in car keys and in home security alarms (Koelle et al., 1976) protecting things of high value. Prices of RFID tags are still too high to compete (Koelle et al., 1976), but prices are dropping and market analysts believe that the first major roll-outs on case level (Weis et al., 2004) will take place in the near future.

## 2 RFID PRIMER

RFID systems consist of three main components: the RFID tag, the RFID reader and the back-end database. Tags typically consist of a microchip that stores data and a coupling element, such as a coiled antenna, used to communicate via radio frequency communication. The readers usually consist of a radio frequency module, a control unit, and a coupling element to interrogate the tags via radio frequency communication. Tag readers interrogate tags for their contents through an RF interface. As well as an RF interface to the tags, readers may contain internal storage, processing power, or an interface to back-end databases to provide additional function. The RFID tags obtain their power from the magnetic field generated by the reader through inductive coupling.

Tags may be either actively or passively powered. Active tags contain an on-board power source, such as a battery, while passive tags must be inductively powered via an RF signal from the reader. The distance a reader may interrogate tags from is limited by the tag's power. Consequently, active tags may be read from a greater distance than passive tags. Active tags may also record sensor readings or perform calculations in the absence of a reader. Passive tags only can operate by a reader and are inactive otherwise. Readers may use tag contents as a look-up key into database storing product information, tracking logs, or key management data. A ubiquitous low-cost RFID system would most likely require the use of passive tags.

## 3 RFID SECURITY AND PRIVACY RISKS

With the use of Internet many vulnerabilities and threats to the system security and the privacy of the users are inherited. This can be a malicious agent faking an innocent PML request over an ONS service or a disgruntled employee adding incorrect product information in the database, causing confusion and damaging the systems integrity. RFID tags may pose security and privacy risks to both organizations and individuals. This section will look closer at the privacy and security concerns arising from areas in which RFID distinguishes itself from most current usage of information technology (Lu et al., 2004) (Siau, and Shen, 2003). Unprotected tags may be vulnerable to eavesdropping, traffic analysis, spoofing or denial of service. Unauthorized readers may compromise privacy by accessing tags without adequate

access control. Even if tag contents are protected, individuals may be tracked through predictable tag responses; essentially a traffic analysis attack violating “location privacy”. Spoofing of tags may aid thieves or spies. Saboteurs could threaten the security of systems dependent on RFID technology through denial of service.

Therefore, the RFID security problem can be generalized four components. One is eavesdropping (Weis, 2003) from RFID-tagged items. When reader queries tag, tag may return information back to reader, others would have an opportunity to fetch content sent. The second is traceability (Ohkubo et al., 2003) or traffic analysis (Weis et al., 2004). By tracking tag signal, eavesdropper could trace individual behavior and distinguish personal identification. The third is spoofing (Weis et al., 2004). Cheat RFID system with a counterfeit tag make RFID system think that this counterfeit tag is a legal tag. The final is industrial sabotage (White Paper, 2004). Somebody may corrupt data in tags by using a hand held device, and erase or modify the contents. We describe these security problems as follows.

### *3.1 Eavesdropping*

Eavesdropping (White Paper, 2004) is defined as listening in on longer-range communication systems like UHF, which broadcast signals (albeit very weak) up to 100 meters. Tag readers are assumed to have a secure connection to a back-end database. Although readers may only read tags from within the short (e.g. 3 meter) tag operating range, the reader-to-tag, or forward channel is assumed to be broadcasted with a signal strong enough to monitor from long-range, perhaps 100 meters. The tag-to-reader, or backward channel is relatively much weaker, and may only be monitored by eavesdroppers within the tag’s shorter operating range. Generally, it will be assumed that eavesdroppers may only monitor the forward channel without detection (Weis, 2003) (White Paper, 2004). Eavesdropping may cause two kinds of security problems. The first is individual information leakage (Ohkubo et al., 2003) and the other is industrial espionage (Sarma et al., 2002).

#### *3.1.1 Individual Information Leakage*

In daily life, people are prone to carrying various objects around with them. Some of objects are quite personal, and provide information that the user does not want anyone to know about, for example, money, expensive products, medicine, or books. If such items are tagged, various personal details can be acquired without the owner’s permission. The private information leaks either only via the wired network or involving the communication between an RFID tag and a reader. (Aljifri and Tyrewalla, 2004) (Anil *et al.*, 2003)

### *3.1.2 Industrial Espionage*

Aggregate logistics and inventory data hold significant financial value for commercial organizations and their competitors. A store's labeled inventory may be monitored by competitors conducting surreptitious scans. Sales data may be gleaned by correlating changes over time. Individuals carrying items with unsecured tags are vulnerable to privacy violations. In retail environment, where a competitor capable of reading tags in shops or warehouses may gather business intelligence regarding the turnover rate of stocks, the shopping patterns of customers, and so forth. Somebody could derive sales, inventory data and offer his services to business adversary as a corporate spy (Weis et al., 2004) (Juels, 2004).

## *3.2 Traceability*

Another important privacy concern is the tracking of individuals by RFID tags. A tag reader at a fixed location could track RFID-labeled clothes or banknotes carried by people passing by. Correlating data from multiple tag reader locations could track movement, social interactions, and financial transactions. To stretch the point a bit, this situation is similar to forcing the user to carry a tracking device. These violate the concept of location privacy (Bereford and Stajano, 2003). Concerns over location privacy were recently raised when a major tire manufacturer began embedding RFID tags into all their products.

## *3.3 Spoofing*

In addition to threats of passive eavesdropping and tracking, an infrastructure dependent on RFID tags may be susceptible to tag spoofing (Weis et al., 2004) (Tan et al., 2003) (Anil et al., 2003). There are two kinds of security issues about spoofing. One is theft and the other is counterfeiting which are discussed as follows.

### *3.3.1 Theft*

By spoofing valid tags, a thief could fool automated checkout or security systems into thinking a product still on a shelf. Alternatively, a thief could rewrite or replace tags on expensive items with spoofed data from cheaper items. Saboteurs could disrupt supply chains by disabling or corrupting a large batch of tags.

### *3.3.2 Counterfeiting*

Counterfeiting (White Paper, 2004) is defined as being able to read or intercept data written

into a tag, which uniquely identifies or certifies a product. Once the data is known, similar read/write tags could be purchased and updated with the authentic data. Thus it is possible that malicious attacker use counterfeiting products to spoof RFID security system.

### *3.4 Industrial Sabotage*

Industrial Sabotage is defined as one, with a grievance against a company, who decides to start corrupting data in tags by using a hand held device and erasing or modifying the contents (White Paper, 2004). Physical attacks and DoS are the most popular methods.

#### *3.4.1 Physical Attacks*

One may conduct physical attacks against tags, such as specified in Weigart (2000). These attacks may include probe attacks, material removal through shaped charges or liquid etching, energy attacks, radiation imprinting, circuit disruption or clock glitching (Weis, 2003).

#### *3.4.2 Denial of Service (DoS)*

The attacker can also pose a weakest threat. She/he could flood RF channels with noise to disrupt or garble communication. The attacker might even be able to conduct a low-level directed energy attack to destroy tags. Analogously, someone could easily destroy barcodes by tearing them off or writing over them. The attacker cannot derive useful information from an RFID system, but can launch denial of service attacks against the system. (Weis et al., 2004) (Juels et al., 2003) (Tan et al., 2003).

## 4 COUNTERMEASURES

In this section, an overview of the known methods that prevent malicious attacks on RFID system is presented. Several papers have examined the protection of RFID security and user privacy. The countermeasures are divided into two major groups. One depends on cryptographic algorithms and the other is non-cryptographic scheme. In this section a brief description of different types of countermeasures are given. For each type, some proposal methods are presented.

### *4.1 Non-Cryptographic Scheme*

To minimize cost, this type of countermeasures has no cryptographic function. The non-cryptographic scheme can be classified into Tag-killing approach, selective blocker tag,

rewriteable memory and physical ID separation, which are described as follows.

### *4.1.1 Kill Tag approach*

The most straightforward approach to the protection for consumer privacy is to kill RFID tags before they are placed in the hands of consumers. The kill command may be assumed to be a slow operation that physically disables the tag, perhaps by disconnecting the antenna or short-circuiting a fuse. Tags supported by the Auto-ID Center (Auto-ID Center, 2002) have the following kill properties. Each tag has a unique 8-bit password, and upon receiving the password, the tag erases itself. This function is useful in protecting the user privacy, but a conscious decision is required to initiate the procedure.

### *4.1.2 Selective Blocker Tag*

Juels et al. (2003) propose the idea of blocker tags, which simulates all of the IDs in a desired zone of ID values, and which can selectively protect the zone from being read by malicious readers, with the blocker tag which simulates all of the IDs in the zone. This approach is available in tree-walking protocol widely used in UHF frequency, and is quite effective as regards cost since RFID tags on objects needs no additional enhancement. Since this approach is to block private information using optional blocker tags, practical requirement that the communication area of a blocker tag must cover that of RFID tags in objects should be fulfilled in the implementation of this approach.

### *4.1.3 Rewriteable Memory*

Inoue and Yasuura (2003) proposed this method. Each RFID tag has a read only memory (ROM) and a rewritable but non-volatile memory (RAM). A unique and permanent ID of the RFID tag is set in the ROM by the producer. In the RAM, a private and temporary identification code is set by the owner of tag. ROM and RAM memory are used only exclusively. In the ROM mode, unlimited object identification for any users is provided by the identification code of the RFID tag. In the RAM mode, the restriction of object identification to limited user is achieved.

### *4.1.4 Physical ID Separation*

An RFID sequence for naive assignment for globally-unique ID is divided into two fields (Inoue and Yasuura, 2003). The one is Class ID about the information on the object, such as UPC/EAN codes used in barcodes. The other one is Pure ID such as serial number or lot

numbers. When the owner of a product in a stage of the life cycle (retailer) is to pass his/her ownership to the next stage (consumer), he/she takes off the Class ID. The owner of the next stage (consumer) prepares RFID tags with several user-assigned Class IDs. Consumer could attach the tags to the products to make the concatenation of his/her ID and Pure ID.

### *4.2 Cryptographic Scheme*

Cryptographic Scheme is also classified as Hash Based Access Control, Randomized Access Control, Silent Tree Walking, Hash Chain and XOR based One-Time Pad, which are described as follow.

#### *4.2.1 Hash Based Access Control*

Each hash-enabled tag in this design will have a portion of memory reserved for a temporary metaID and will operate in either a locked or unlocked state (Weis et al., 2004). To lock a tag, a tag owner stores the hash of a random key as the tag's metaID, i.e. metaID $\leftarrow$ hash(key). This may occur either over the RF channel or a physical contact channel for added security. While locked, a tag responds to all queries with only its metaID and offers no other functions.

To unlock a tag, the owner queries the metaID from the tag, looks up the appropriate key in the back-end database and finally transmits the key to the tag. The tag hashes the key and compares it to the stored metaID. If the values match, it unlocks itself and offers its full functionality to any nearby readers. To prevent from being hijacked, unlocked tags should only be unlocked briefly to perform a function before being locked again.

#### *4.2.2 Randomized Access Control*

This approach is similar to Hash Based Access Control. Randomized access control (Weis et al., 2004) could improve traceability problem. Beside a one-way hash function, tags also have a random number generator. Each tag will operate in either a locked or unlocked state. An unlocked tag may be locked with a simple instruction from a reader; no protocol is necessary. Tags respond to reader queries by generating a random value, r, then hashing its ID concatenated with r, and sending both values to the reader. That is, tags respond to queries with the pair (r, h(ID||r)). A legitimate reader identifies one of its tags by performing a brute-force search of its known IDs, hashing each of them concatenated with r until it finds a match. Although impractical for retailers, this mode is feasible for owners of a relatively small number of tags.

### *4.2.3 Hash Chain*

Initially tag has initial information s1. In the i-th transaction with the reader, the RFID tag sends answer ai = G(si) to the reader, and renews secret si+1 = H(si) as determined from previous secret si, where H and G are hash functions. The reader sends ai to the back-end database. The back-end database maintains a list of pairs (ID; s1), where s1 is the initial secret information and is different for each tag. So the back-end database that received tag output ai from the reader calculates ai' = G(Hi(s1)) for each s1 in the list, and checks if ai ?= ai'. The back-end database find ai' = ai and return the ID, which is a pair of ai'.

The hash chain technique (Ohkubo et al., 2003) could renew the secret information contained in the tag. Thus, the private information of user could be protected, and traceability becomes impossible.

### *4.2.4 XOR based One-Time Pad*

XOR based one-time pad scheme, by RSA Lab (Juels, 2004), needs only an XOR calculation, and so is very low cost. In this scheme, the reader (actually the back-end database) and the tag share a common list of random keys, and in some interactions they confirm that the partner has the common list. If the check passes, the tag sends its ID. This scheme is very low cost. However, this scheme requires several interactions between the reader and the tag. Moreover, the common list must be overwritten completely as needed to ensure security. These points may make implementation difficult.

## 5 COMPARISON

For above-mentioned security problems, we explore the existing possible solutions and generalize the results in Table 1. If the solution 'A' could prevent the illegal attack 'B', we represent it by "◯", otherwise "X". If it is a undeterminable situation, we represent it by "△" for differentiate and left for other researchers to resolve.

| Problems / Securitv / Solutions | Individual Information | Industrial Espionage | Traceability | Theft | Counterfeiting | Physical Attacks | DoS |
|---|---|---|---|---|---|---|---|
| Kill Command Feature | ○ | ○ | ○ | ✕ | ○ | △ | △ |
| The Blocker Tag | ○ | ○ | ○ | ✕ | ○ | △ | △ |
| Rewritable Memory | ○ | ○ | ✕ | ✕ | ✕ | △ | △ |
| Physical ID | ○ | ○ | ✕ | ✕ | ✕ | △ | △ |
| Hash-Based Access Control | ○ | ○ | ✕ | ✕ | ○ | △ | △ |
| Randomized Access Control | ○ | ○ | ○ | ○ | ○ | △ | △ |
| Hash Chain | ○ | ○ | ○ | ○ | ○ | △ | △ |
| XOR Based One-Time Pad Scheme | ○ | ○ | ○ | ○ | ○ | △ | △ |

**Table 1: RFID security problems and its possible solutions**

## 6 CONCLUSION

It is possible that RFID tags revolutionize society. While bringing to fruition their convenience, we must understand their risks also. Implementing ubiquitous network connectivity in society will demand a close examination of personal privacy from both the technical and social aspects. The privacy problems raised by their indiscriminate nature are serious enough to demand a comprehensive and effective technique that can ensure user privacy while retaining their benefits (Floerkemeier, and Lampe, 2004). Some of them allow tag output to include relatively constant information. Some of them demand the data in the rewritten tag memory by to avoid tracking. Others fail to satisfy the forward security requirement. While there are several existing schemes, no one provides a complete solution. With new technology advances allowing more features to be incorporated into tags, the line between RFID devices, smart cards, and general-purpose computers will blur. Understanding RFID security today will aid in development of secure ubiquitous computing systems in the future. Recognizing inherent privacy or security threats of RFID systems will be also helpful for decision-making regarding the obligations of RFID manufacturers and the privacy rights of end users.

**Acknowledgement:** The author would like to give thanks to the National Science Council of Taiwan for grant NSC 93-2218-E-194-016 to part of this research.

## REFERENCES


H. Aljifri, and N. Tyrewalla, (2004), “Security model for Intra-Domain Mobility Management Protocol”, *Int. J. of Mobile Communications*, Vol. 2, No.2, pp. 157 – 170.

R. Anderson and M. Kuhn, (1997), “Low Cost Attacks on Tamper Resistant Devices”, In IWSP: International Workshop on Security Protocols, LNCS, volume 1361, pages 125-136.

S. Anil, L. T. Ting, L. H. Moe, G. P. G. Jonathan, (2003), “Overcoming barriers to the successful adoption of mobile commerce in Singapore”, Int. J. of Mobile Communications, Vol. 1, No.1/2, pp. 194-231.

Auto-ID Center, (2002), “860MHz-960MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical communication Interface Specification Proposed Recommendation Version 1.0.0”, Technical Report MIT-AUTOID-TR-007, November.

A. Bereford and F. Stajano, (2003), “Location Privacy in Pervasive Computing”, IEEE Pervasive Computing, Vol. 2, No. 1, pp 46-55.

K. Finkenzeller, (2003),”RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification”, Second Edition, John Wiley & Sons, Ltd.

C. Floerkemeier, and M. Lampe, (2004), ”Issues with RFID Usage in Ubiquitous Computing Applications” In: Alois Ferscha, Friedemann Mattern (Eds.): Pervasive Computing: Second International Conference, PERVASIVE 2004, LNCS, volume 3001, Springer-Verlag, pages 188-193, Linz/Vienna, Austria, April 18-23.

S. Inoue and H. Yasuura, (2003),”RFID Privacy Using User-controllable Uniqueness”, Kyushu University, November.

B. Johansson, (2004), “An Introduction to RFID – Information Security and Privacy Concerns”, TDDC03 Projects, Spring.

A. Juels and R. Pappu, (2003), “Squealing euros: Privacy protection in RFID-enabled banknotes”, In proceedings of Financial Cryptography – FC’03, LNCS, volume 2742, Springer-Verlag, pages 103-121.

A. Juels, (2004), “Minimalist Cryptography for Low-Cost RFID Tags”, In C. Blundo, ed., Security of Communication Networks (SCN), To appear.

A. Juels, R. L. Rivest and M. Szydlo, (2003), “The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy”, In V. Atluri, ed. 8th ACM Conference on Computer and Communications Security, pages 103-111. ACM Press, (CCS 2003), October.

A. R. Koelle, S. W. Depp, J. A. Landt, and R. E. Bobbett, (1976), “Short-Range Passive Telemetry by Modulated Backscatter of incident CW RF Carrier Beams”, Biotelemetry, 3:337-340.

J. Lu, C. S. Yu, C. L., Catherina Y. F. Ku, (2004), “Wireless trust: conceptual and operational definition”, Int. J. of Mobile Communications, Vol. 2, No.1, pp. 38 – 50.

M. Ohkubo, K. Suzki and S. Kinoshita, (2003),”Cryptographic Approach to ‘Privacy-Friendly’ Tags”, Nippon Telegraph and Telephone, November.

Royal Air Force, History:1940, http://www.raf.mod.uk/history/line1940.html

S. E. Sarma, S. A. Weis, and D. W. Engels, (2002), “RFID Systems and Security and Privacy Implications”, In Workshop on Cryptographic Hardware and Embedded Systems, CHES 2002, LNCS, volume 2523, Springer-Verlag, pages 454–469.

K. Siau, and Z. Shen, (2003), “Mobile communications and mobile services”, Int. J. of Mobile Communications, Vol. 1, No.1/2, pp. 3-14.

J. Tan, H. J. Wen, and T. Gyires, (2003), “M-commerce security: the impact of wireless application protocol (WAP) security services on e-business and e-health solutions”, Int. J. of Mobile Communications, Vol. 1, No.4, pp. 409 – 424.

S. H. Weigart, (2000), “Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses.” In Workshop on Cryptographic Hardware and Embedded Systems, CHES 2000, LNCS, volume 1965, Springer-Verlag, pages 302-317.

S. Weis, (2003), “Security and Privacy in Radio-Frequency Identification Devices”, Masters Thesis, MIT. May.

S. A. Weis, S. E. Sarma, R. L. Riovest, and D. W. Engels, (2004), ”Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, In D. Hutter et al. (Eds.): Security in Pervasive Computing 2003, LNCS, volume 2802, Springer-Verlag, pages 201–212.

White Paper, (2004) “A basic introduction to RFID technology and its use in the supply chain”, LARAN RFID, January.