

# Radio Frequency Identification (RFID): Privacy and Security

Hyung-Joon Kim

Dept. of Electrical and Computer Engineering  
Stevens Institute of Technology, Hoboken, New Jersey

## 1. Introduction

Despite its long history, Radio Frequency Identification (RFID) is considered as one of the most promising wireless technology in future ubiquitous computing environments. However, it's a very different form of technology than today's other wireless dominants such as cellular, satellite, and wireless computer networks. In short, RFID is a contactless, automatic, ultra-light, super-cheap, and extremely convenient method primarily for uncomplicated data capture. The physical design of RFID, therefore, is limited to the minimum capability and feasibility necessary to serve the purpose of the technology. Common wireless communication systems enable people to exchange information over the air. In other words, you're the actual sender or recipient of the information. For instance, a person talks on the cellular phone, watches the satellite TV, connects to the Internet through WiFi. Emergency services agencies (e.g. police, fire, EMS) extend their eyes and ears by public safety wireless networks in order to control the public safety. The communication is deliberately initiated and terminated by *human*. Unlike these typical wireless systems, in a RFID system, communication is automatically initiated and terminated by a RFID tag or reader, an *object*, as long as within the range of radio signals. Therefore, the communication may take place without the consent of a person having the RFID-tagged object; even worse, the person may be totally unaware of such machine-to-machine communication. The above characteristics bring about controversial privacy and security concerns. This paper overviews the RFID technology and includes the assessment of the security aspects. Based on those, the paper discusses major security issues and future directions.

## 2. Background

### 2.1 History of RFID

The first ancestor of RFID was the Identification Friend or Foe (IFF) system that was invented by United Kingdom and used by the allies during World War II to identify friendly aircrafts. In 1960s, the first Electronic Article Surveillance (EAS) systems were developed for anti-theft systems [1]. In 1973, the patent for a keyless access card, the first true ancestor of today's RFID, was granted and the US governments started investigating the technology's potential; as a result, the Department of Energy adopted RFID systems to surveil materials at nuclear weapon sites, and the Department of Agriculture used them to track cattle for the right dosage of hormones and medicines in case of illness [2]. After its slow spread for a couple of decades, in 1990s, RFID systems explosively proliferated in the supply chain. Lately, some gigantic retailers led by Wal-Mart and the Department of Defense have agreed that they plan to use RFID systems progressively more for products in

the supply chain. No doubt, the RFID explosion will continue and more applications of the technology will be integral part of our life in near future.

## 2.2 The Fundamentals of RFID

RFID is an automatic identification method using radio frequency. Even though the RFID technology is achieved over the air interface - thus, wireless communication, it is very different than other wireless technologies (e.g. cellular, satellite, WiFi, and WiMax) in terms of the functions and physical representations of the systems.

RFID exploits several different chunks of the radio spectrum. Low frequency (LF: below 135 kHz) standardized by ISO 18000-2 and high frequency (HF: 13.56 MHz) standardized by ISO 18000-3 can be used globally without a license. RFID using LF and HF requires large antennas while supporting a short range less than 3 feet. Ultra high frequency (UHF: 860 MHz to 960 MHz) cannot be used “globally” without a license since there is no single international standard. In the US, 902 to 928 MHz (central frequency of 915 MHz), standardized by AutoID Class 0/1, can be used without a license but there are restrictions on transmission power. Another UHF RFID exploits 2.45 GHz. In general, small antennas are sufficient for UHF RFID systems, which support a long range up to tens of feet. RFID supports non line-of-sight, and the tags may be equipped with non-volatile storages, possibly Electrically Erasable Programmable Read-Only Memory (EEPROM), for storing rewritable data.

The functionality and working range of RFID systems substantially vary according to implementations and applications. In general, there are two types of RFID tags:

- **Passive** – Passive tags have no onboard power source. Instead, for transmitting radio signals to readers, they utilize the energy of operational power received from readers – known as *backscattering*. Thus, as the name implies, the tags operate passively only by responding to the queries sent from the readers. With no requirement of internal battery, passive tags can be designed considerably small in size and thickness. These days, printable RFID tags as sticker labels are widely deployed in inventory systems. While passive tags have size/cost advantages, they have some limitations on operations; that is, with lack of power supply, they can convey minimal data and their operational ranges are limited to very short distances. Most of today's small and inexpensive barcode-type RFID tags, such as Electronic Product Code (EPC) tags, are passive tags.
- **Active** – Active tags are equipped with internal power source such as batteries. With help of battery power, the tags are capable to broadcast signals on their own. Active tags clearly have size/cost disadvantages over passive tags. However, with power supply generating stronger signals, they are more reliable and resistant in hostile environments where many impeding materials, like metal and water, are present. For instance, implantable RFID tags must be viable in animal or human bodies, which virtually consist of liquids. Active tags support much longer range (up to hundreds of meters). They can also contain extended data, thereby supporting more sophisticated applications.

These days, the characteristics of RFID systems are evolving: they are getting smaller (therefore, applicable to a variety of objects) and operate more on passive mode, and modern applications are developed to do more than just identification which old barcodes exist for. As a result, the data exchanged between a tag and a reader is more than just a serial number, and some may be quite sensitive data (e.g. an individual's identification, or medical and billing information). This future trend has some important implications for privacy and security.

### **2.3 Applications**

- Barcode-type RFID tags are primarily used in the supply chain management for controlling production, inventory, logistics, and customer relationship as efficiently possible.
- Anti-theft RFID tags are used as Electronic Article Surveillance (EAS), which is intended to prevent shoplifting from retail stores or pilfering from libraries.
- Contactless RFID-based keys are used for neat access control methods (e.g. for buildings, campuses, etc). RFID-equipped ignition key cards for convenience and enhanced anti-theft are adopted by automobile manufactures.
- Traditional identification cards are being replaced by electronic identification method (e.g. E-passport) using the RFID technology.
- Automatic payments, such as RFID-embedded credit cards, public transportation passes, and Electronic Toll Collection (ETC), such as E-ZPass widely used in the northeastern United States, are already popular throughout the world.
- Some medical applications are anticipated to play important roles in home care and healthcare systems, especially valuable for impaired patients.
- Implantable RFID tags are used for animal identification, vaccination, and ecology study. RFID-based animal implants can be very effective to track and control animals, especially in case of outbreaks of the recently notorious "bird flu" and "mad cow disease" [3]. Similarly, human implants can be used to reduce medical incidents and diagnostic dilemma, especially in case of emergency or unconscious patients.
- Recently, wearable RFID tags in the form of wristbands, backpacks, and clothes are being manufactured for military personnel, prisoners, and schoolchildren [3].
- RFID-enabled mobile phone, which acts like a RFID reader, has been developed by some vendors. The mobile phone is equipped to be capable of scanning RFID tags and then communicating with back-end infrastructures by nature. For example, a person can simply scan RFID tags on a poster or advertising billboard by using a RFID-readable mobile phone to make a reservation without ever dialing [4].
- In future ubiquitous environments, smart home appliances with built-in artificial intelligence can be even better with the RFID technology. The papers [3, 5] introduce some other future applications; for instance, RFID-tagged clothes can be queried by smart washing machine for adaptive selection of detergent, temperature, and wash cycle/mode, RFID-tagged medicine containers can work with a smart medicine cabinet to issue an alert, and in similar manners RFID-packed foods can communicate with a smart refrigerator. Even further, as well as on-site managements, RFID-enabled home appliances can be equipped by itself (or as part

of integrated home computing system) to place scheduled electronic orders for everyday foods or medication refills.

### **3. Security Assessment on RFID**

#### **3.1 Assets**

- RFID tags/readers and back-end infrastructures (e.g. databases)
- Frequencies/RF spectrum
- Authentication methods and cryptographic protocols
- Information carried through the systems or retrieved from back-end systems
  - Serial number and manufacture of RFID-tagged products
  - Sourcing, distributing, manufacturing, inventory, and shipping information
- Privacy and personal information such as identification, physical location, medical and billing information
- Confidential information, when used for military facilities or personnel, such as location, identification, operating characteristics
- Authorization and access privilege, when used for access control method
- RFID-tagged products or properties such as high-value items in retailers and library books

#### **3.2 Perpetrators**

- General hackers
- Terrorists scanning the innocents' RFID-enabled passports to clone the passports
- Governments, corporations, employers tracking individuals with malicious intent
- Competitors, industrial spies, and survey companies
  - Harvesting customer's preference, purchase history, and regional statistics
  - Spying competitor's supply chain management
- Insurance companies abusing individual's medical information
- Private detectives undertaking investigation into individuals
- Malicious owners of RFID-tagged objects
- Thieves, free riders, and frauds who wish to bypass the systems
- Impostors stealing someone's identity or authority
- Privacy activists and civil liberties groups against the technology
- Natural disasters damaging RFID readers/antennas or radio-absorbing materials in the surroundings of the systems

#### **3.3 Threats**

- Jamming and interference
- Sniffing and eavesdropping information in the communication links
- Malicious use of cradle-to-grave tracking systems; monitoring, tracking, and profiling of individuals or merchandise purchased by customers
- Associating identifiable data with rich information stored in the back-end systems
- Unauthorized scanning of RFID tags with malicious purposes
- Attacking back-end infrastructures

- Replay attacks by intercepting valid responses to reader's queries and relaying them for fraudulent payments or unauthorized access to buildings
- Masquerading and financial fraud
- Disclosure of customer privacy and corporation privileged information
- Spoofing, reverse-engineering, key cracking, counterfeiting or cloning of RFID tags
- Cracking authentication or cryptography protocols
- Denial of service attacks

### **3.4 Existing Safeguards**

- Physical guards and attendants on sites
- Simply restricting the transmission power, thereby limiting the operational range
- Policies and regulations
- Backup power and readers for outage or damage
- Authentication scheme and cryptographic protections of data transmission
- Kill (suicide) commands, temporary deactivation function, Faraday cage (or aluminum foil), or RF deflecting metallic sleeves [3]
- Blocker tags which work by emitting both 0 and 1 for the first bit of an identifier to disrupt the tree-walking process of readers [1, 5]
- RFID detectors, interpreter/logger for consumer's privacy [3]
- Public-key based basic access control for digital passports [3]
- Lightweight symmetric key based authentication methods [5]
- Periodical reconfiguration on rewritable tags
- Back-end authentication servers
- Passwords, random number generators, and pseudonyms (a.k.a "minimalist"), for authentication challenge [1, 4, 5]
- Proxying approach – that is, portable privacy-enforcing devices [4, 5]
- Read access control by hash-based approach (e.g. "hash-lock") [6]
- Distant measurement [5]

### **3.5 Potential Vulnerabilities**

- Physical limitations of tiny tags in term of computational and power resources for authentication and data encryption
- Cost-benefit dilemma for expensive security protections
- Difficulty defining attackers and attacks that complicates the design of a complete security scheme [3]
- Variety of types and applications
- Difficulty being aware of compromised tags, which has absolutely no history of transactions
- Unlicensed portion of radio spectrum (not governed by a single regulatory body)
- Detectible beyond line-of-sight (long-range transponders are more vulnerable to eavesdroppers)
- RFID tags are "promiscuous": they can be read by any readers
- Operating without consent and awareness of possessors
- Difficult key management

### 3.6 Additional Security Controls

- Signaling techniques, like Frequency-hopping spread spectrum (FHSS) [3], resistant to eavesdropping and jamming
- Security mechanisms without cryptography
- Ultralight cryptography for authentication and encryption
- Tight safeguards on the interface with back-end infrastructures (e.g. databases)
- Strict security policies and regulations
- International standards

## 4. Discussions of Major Security Issues

The major security issues are closely related, though not unique, to the nature of RFID technology. Most intuitively, the physical limitations that RFID systems have are the most important factors as regards its weak security. The conventional cryptography suites are far from realistic for RFID. The nature of RFID is just not friendly to any costly process. With the lack of tag-side resources, it's very challenging to develop novel cryptographic techniques for confidentiality and integrity assurance in the shared medium. The paper [1] says, in the world of RFID, "Moore's law doesn't hold forth its usual promise of inexorable increases in computing power." This is especially true because today's RFID systems rely more on passive tags in the form of EPC labels. Even though more complex applications are expected to come out in the future, the biggest winners would still be simplex passive tags in terms of cost-benefit formulas. Inexpensive passive tags, like EPC labels, cost only cents but applied to the trillions. Without strong cryptography, it's very difficult to achieve security tasks – authentication, confidentiality, and integrity.

The failure of the security tasks has important implications for privacy threat to RFID systems. An adversary has a full hand of options by intercepting the first-hand data sent from an RFID-tagged object to a reader. The intercepted data, such as a person's identity and authority, by an attack in the first degree can be directly used for unauthorized access to privileged areas (e.g. buildings or automobiles). Otherwise, the intercepted data can be used as a "key" by secondary attacks to retrieve the rich information associated with an individual from back-end data warehouses; harvesting data at the point-of-sale, by itself, could also gather "valuable" statistics for end-user marketing. In the same manner, an industrial spy would probably want to collect information about a competitor's supply chain management – from raw materials to shipped products. The leak of privacy could also cause serious social issues in various areas. For example, the medical predispositions of individuals deduced by attacks against RFID systems may be misused for discriminative treatments by insurance companies or employers.

Tracking the location of an individual who possesses an RFID-tagged object is another major privacy issue. Although most RFID tags are undetectable from a "long" distance, the technology is evolving dynamically and the ranges actually vary from one application to another. Some tags can be scanned from a long distance, say tens of meters, which may be quite satisfactory to an adversary. The short range of RFID itself cannot be a safeguard at all. There are some countermeasures for tracking threats such as a built-in "Kill" command, which deactivates itself upon a successful scan (e.g. at the point-of-sale). Often, however, the kill command is not efficient since the tag may need to be scanned later again. For

example, purchased items may need to be returned or repaired. For libraries or rental shops, tags need to stay "alive" over the lifetime of the items. Thus, "sleeping", a variant of kill command, can be a better approach in which tags can be deactivated and reactivated back and forth by a special command, "wake", issued by a RFID reader [4]. However, in practice, it's difficult to verify, without authentication, whether a "wake" command is sent from an authorized reader. Therefore, the absence of authentication makes the sleeping method still fall short of security. Besides, in many applications, on-off mode is not applicable at all. As improved versions of "sleeping" method, some hash-based read access control methods are reviewed in [6]. However, these approaches still provide the limited capability of authentication, not as strong as that for other common wireless devices. Although some proposed security schemes employ novel lightweight cryptographic mechanisms, they cannot be universally used for a variety of RFID types, some of which are just printable tags. Therefore, most existing safeguards simply try to shield a tag from being scanned by a rogue reader.

Now, another security issue is related to interoperability and availability. While RF spectrum is becoming more crowded, RFID can be deployed without a license. According to Visa Waiver Program (VWP) [5], the U.S government has mandated the adoption of "E-passport" for "visa waiver" countries as a condition of their citizen's entries to the U.S. However, the unlicensed portion of RF that UHF RFID in the U.S. exploits is used for mobile or other devices in Europe and Asia. Thus, interoperability must be considered to avoid any interference, especially in case that an RFID-enabled item is likely to travel abroad. Needless to say, RFID is not an exception to denial-of-service attacks.

The security assessment can be completed with the discussion of likelihood and impact of feasible attacks. As mentioned earlier, the lack of security protections due to the physical limitations of RFID cause native wireless security problems as well as "privacy" concerns – *association threat* and *cradle-to-grave tracking threat*. However, there have been furious debates as to the likelihood of privacy threats. In modern times, one of the prime objectives of honest enterprises is to earn customer's trust before everything else. Moreover, there are many other lawful ways available today for marketing research. While this is true from a commonsense standpoint of view, the information acquired by potential attacks could be temptingly valuable to all businesses, which are potential attackers. Hence, it is still possible for some to dare to risk business ethics. Meanwhile, the likelihood of corporate espionage against competitors may be somewhat high. It's because competitor analysis is relatively difficult and often requires veiled information. Indeed, according to [1], "although RFID poses legitimate privacy concerns, the degree and nature of the technology's threat to privacy are easily misunderstood." It's apparent that the impact of privacy threats is inconceivably huge. However, it's too early to get paranoid about privacy concerns. For example, tracking individuals after the point-of-sale is not yet practically achievable even though it's conceptually possible. Further association attacks using hijacked identifiable data are not easy, either, when fairly strong safeguards protects data warehouses.

## **5. Future Directions**

In addition to the physical limitations that RFID suffers from, the difficulty defining attackers and attacks complicates the design of a complete security scheme for RFID [3]. The term "RFID" now is a bit ambiguous without distinctions in terms of the technical

capabilities and applications of the technology. Today, there are too many types and applications from 5 cents EPC tags to 4,000 dollars GPS-equipped tags<sup>1</sup>, and they are becoming even more diverse. Without correctly specifying the nature for which security services exist, it's hardly able to design trustworthy systems. Thus, standardization bodies should take the responsibility of defining the "chaotic" RFID technology.

A peculiar vulnerability of RFID is the fact that insecure data transmission takes place even without human consent and awareness. The paper [8] points out "security and privacy in RFID tags aren't just technical issues; important policy questions arise as RFID tags join to create larger sensor networks and bring us closer to ubiquitous computing." To preserve privacy, it is necessary to establish a prudent security policy as well as a good public understanding of the RFID technology. Interestingly, Simson Garfinkel [7] proposes an "RFID Bill of Rights" as follows:

- *The right to know whether products contain RFID tags.*
- *The right to have RFID tags removed or deactivated when they purchase products.*
- *The right to use RFID-enabled services without RFID tags.*
- *The right to access an RFID tag's stored data.*
- *The right to know when, where and why the tags are being read.*

In technical fields, researchers and developers have made efforts to introduce novel security mechanisms such as signaling techniques and ultralight cryptography. As technology is drastically evolving, new security mechanisms will certainly have an effect on the improvement of security. However, RFID is likely to be put into cost-benefit dilemma since most RFID tags benefit from a great deal of size and price. Therefore, it would be more efficient to put expensive safeguards on the reader side than the tag side.

## **6. Conclusion**

The likelihood of specific attacks against RFID is arguable, but it cannot be questioned that the major loss of assets, privacy, is immeasurable. The explosive deployment of RFID is inevitable in the upcoming ubiquitous era. Meanwhile, attacks are rapidly evolving as well. It's a good sign that privacy and security concerns have been already investigated before the RFID technology seriously takes over the world or any actual threats are revealed. It's very important to keep watching the development of future RFID and prepare for security protections as well as privacy safeguards; otherwise, the failure to achieve either one will cause doomsday consequences, depending on the degree of sensitivity and privacy.

---

<sup>1</sup> Researchers have tracked dolphins and other marine animals with systems combining a GPS receiver with a radio transmitter that can be picked up by satellite (which costs approximately \$4,000 per tag) [1].

## Reference

- [1] Simson L. Garfinkel, Ari Juels, and Ravi Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions," *Security & Privacy Magazine*, Vol. 3, Issue 3, IEEE Computer Society Press, pp. 34-43, 2005.
- [2] "The History of RFID Technology," RFID Journal, [Online] Available: <http://www.rfidjournal.com/article/view/1338/1/129> [Accessed: Nov. 23, 2007]
- [3] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum, "The Evolution of RFID Security," *Pervasive Computing*, Vol. 5, Issue 1, IEEE Computer Society Press, pp. 62-69, 2006.
- [4] Hyangjin Lee and Jeeyeon Kim, "Privacy Threats and Issues in Mobile RFID," *Proceedings of the 1<sup>st</sup> International Conference on Availability, Reliability, and Security*, ARES '06, IEEE Computer Society, pp. 510-514, 2006.
- [5] Ari Juels, "RFID Security and Privacy: A Research Survey," *IEEE Journal on Selected Areas in Communication*, Vol. 24, Issue 2, IEEE Press, pp. 381-394, 2006.
- [6] Lan Zhang, Huaibei Zhou, Ruoshan Kong, and Fan Yang, "An Improved Approach to Security and Privacy of RFID Application System," *Proceedings. 2005 International Conference on Wireless Communications, Networking, and Mobile Computing*, Vol. 2, IEEE Communication Society, pp. 1195-1198, 2005.
- [7] Simson L. Garfinkel, "An RFID Bill of Rights," Technology Review Inc., Oct. 2002, [Online] Available: <http://www.technologyreview.com/Infotech/12953/> [Accessed: Nov. 23, 2007]
- [8] Ted Phillips, Tom Karygiannis, and Rick Kuhn, "Security Standards for the RFID Market," *Security & Privacy Magazine*, Vol. 3, Issue 6, IEEE Computer Society Press, pp. 85-89, 2005.