An Overview of RFID Technology, Application, and Security/Privacy Threats and Solutions

Chia-hung Huang

Masters in Computer Engineering

Scholarly Paper, Spring 2009

George Mason University, Electrical and Computer Engineering Department

{chuang5@gmu.edu}

Advisor: Dr. Jens-Peter Kaps

Abstract – Radio Frequency Identification (RFID) has been around for nearly 50 years. RFID was first used during World War II in Friend-or-Foe identification system. Ever since then, RFID has caught the attention of many scientists, academics, and enterprises around the world. In addition, the announcement of requiring its top suppliers to adopt RFID technology made by Wal-Mart Cooperation in June, 2003, has once again heated up the topic of RFID. In this paper, I am going to give a brief overview of RFID technology, application, and security/privacy threats and solutions. In addition, I will also briefly introduce the security/privacy issues and solutions in EPCglobal Class 1 Generation 2 (C1G2).

1. Introduction

In the era of World War II, radar was used to "detect" aircrafts when they were still distance away. The problem with radar was there was no way to identify friendly aircrafts or non-friendly aircrafts. Then the Germans noticed the radio signal reflected back to base would be different if the pilots rolled their planes while they returned to base. The method that the Germans discovered was actually the first usage of RFID technology (first passive RFID system) [1]. Later on, the IFF (identify friend or foe) system was developed by the British. In IFF, every British plane was equipped with a transmitter. When British planes were returning to base, they would receive signals from radar station in the base. After receiving signals from radar station, they transmitted signals back to identify themselves [1]. Ever since then, the RFID technology has been noticed by scientists, academics, enterprises all over the world. This paper is organized as follows: the basic components of RFID in section 2, RFID standards in section 3, RFID applications in section 4, RFID security and privacy threats in section 5, proposed solutions of the threats in section 6, and a conclusion will be presented in section 7.

2. Basic components of RFID

A general RFID system contains three major components, the tag, the reader, and the backend system.

2.1 Tag

There are three fundamental components, the antenna, the integrated circuit, and printed circuit board/substrate, in all RFID tags. The antenna mainly is responsible for transmitting and receiving radio waves and sometimes collecting the energy from radio waves if the tag is a passive tag (types of tag will be explained shortly.) The main purpose of integrated circuit (IC) is to transmit the tag's unique identifier. Moreover, the printed circuit board (PCB) is to hold the tag together [4].

In modern RFID technology, there are 4 types of tag, passive tag, semi-passive tag, active tag, and semi-active tag.

- Passive tag: This type of tags contains no power supply on board; therefore, they are very cheap and small. Passive tags absorb their energy when they enter an electromagnetic field (also called Near Field) created by RFID reader's antenna. The Near Field can be proximately calculated by the following equation: $r = \lambda / (2*\pi)$, where λ is the wavelength. Due to the reason of no power supplied on board, the read range of passive tags is very short. Once a RFID reader has interrogated passive tags, and passive tags have absorbed enough energy, they use backscatter (an RF technique) to send their data back to RFID reader [3] [4].
- Active tag: Unlike passive tags, this type of tags comes with power supplied on board such as battery. Since they have their own power supply, they don't need to be powered by the Near Field of RFID readers' antennas. Therefore, passive tags have longer read range than passive tag. The drawbacks are that they are more expensive and bigger in size. Active tags send out signals which are encoded with their identifiers at regularly scheduled rate usually between 1 to 15 seconds (known as beacon rate) [3] [4].
- Semi-Passive/active Tag: Both types of tag contain power supplied on board. The main difference is how the battery is used. Batteries in semi-passive tags are only used to power the internal circuitry. The semi-passive tags still need to be presented inside the Near Filed in order to absorb power for data transmission between RFID readers and themselves. The advantage of semi-passive tags is longer read ranges than passive tags because the energy they absorb from Near Field is fully used to transmit data only. Batteries in semi-active tags are used exactly the same as those in active tags; however, the energy will only be released to power the tags when the tags are being interrogated by RFID readers. The benefit of semi-active tags is that semi-active tags can last longer than active tags since the batteries will only be activated when the tags are being interrogated by RFID readers [3] [4].

2.2 RFID Reader

An RFID reader can be in any forms such as pricing gun in store, toll plaza in highway, and so on. An RFID reader is considered as a middle man in between tags and backend systems. It interrogates (usually call “read”) the data encoded in tag and sends the data to backend system for application wirelessly or through wire. Therefore, an RFID reader should, of course, contains an antenna and an RS-232 serial port or an Ethernet jack. Generally, there are two types of RFID readers, read-only readers and read/write readers. A read-only reader only can read tag’s data. A read/write reader can read tag’s data and also write data to tag if the tag contains a read/write memory [4] [5].

2.3 Backend System

As I mentioned before, the RFID reader serves as a middle man between tags and backend systems. Once a backend system receives data transmitted by a RFID reader, the system runs application based on the data it received. Several RFID applications will be introduced in section 3.

3. RFID Standards

Standardizing RFID technology includes three layers, the data link layer, the physical layer, and the application layer. Data link layer deals with anti-collision, initialization, data content, and tag addressing protocol. Physical layer copes with the communication between tags and RFID readers. Application layer organize how standards are used on shipping labels. Conformance is another protocol in application layer. It mainly deals with testing whether the products meet the standard or not [8]. Moreover, developing international standards for RFID technology can bring up three major benefits. First, an international standard will make sure that interoperability among RFID readers and tags manufactured by different venders and improve interoperation across national boundaries. Secondly, having an international standard will decrease the cost due to compatibility and exchangeability. Third, an international standard will help dramatically on proliferation of RFID technology worldwide [8] [9]. Currently, there are four major organizations involving in developing standards for RFID technology. There are International Standard Organization (ISO), EPCglobal Inc^{TM7}, European Telecommunication Standards Institute (ETSI), and Federal Communication Commission (FCC). Among them, the International Standard Organization (ISO) and EPCglobal Inc^{TM7} have done an incredible job over the past few years. In fact, ISO approved EPCglobal Class-1 Gen-2 as an 18000-6C extension in 2006. This event has opened the way to a single UHF global protocol [10].

3.1 EPC Standards [6] [7]:

EPCglobal is a joint venture between Uniform Code Council (UCC) and EAN International. The organization carries the mission of the former Auto-ID Center at MIT. It’s primarily goal is to make the final EPC standard an official global standard. The EPC class types are summarized in Table 2 and an example of Electronic Product Code (EPC) structure is presented in Table 3.

EPC Class Type	Features	Tag Type
Class 0	Read Only	Passive (64 bit only)
Class 1	Write Once, Read Many (WORM)	Passive (96 bit min)
Class 2 (Gen 2)	Read/Write	Passive (96 bit min)
Class 3	Read/Write with battery power to enhance range	Semi-Active
Class 4	Read/Write active transmitter	Active

Table 2- EPC class types [7]

01	Version of EPC (8 bit header)
115A1D7	Manufacture Identifier 28 bit (> 16 million possible manufactures)
28A1E6	Product Identifier 24 bit (> 16 million possible products per manufacture)
421CBA30A	Item Serial Number 36 bit (>68 billion possible unique items per product)

Table 3- EPC Code Structure [7]

3.2 ISO Standards [6] [7]:

ISO has been working on RFID applications in several areas such as proximity cards, RFID air interface, animal identification, supply chain.

ISO Standards for Proximity Cards:

- ISO 14443 proximity cards – Offering a maximum range of only a few inches. It is primarily utilized for financial transaction such as automatic fare collection, bankcard activity and high security application. These applications prefer a very limited range for security.
- ISO 15693 vicinity cards or smart cards – Offering a maximum usable range of out to 28 inches from a single antenna or as much as 4 feet using multiple antenna elements and high performance reader systems.

ISO Standards for RFID Air Interface:

- 18000 – 1 part 1 – Generic Parameters for Air Interface Communication for Globally Accepted Frequencies.
- 18000 - Part 2 – Parameters for Air Interface Communication below 135 KHz
    - ISO standard for Low Frequency

- 18000 - Part 3 - Parameters for Air Interface Communication at 13.56 MHz
    - ISO standard for High Frequency
    - Read/Write capability
- 18000 - Part 4 - Parameters for Air Interface Communication at 2.45 GHz
    - ISO standard for Microwave Frequency
    - Read/Write capability
- 18000 - Part 5 - Parameters for Air Interface Communication at 5.8 GHz
- 18000 - Part 6 - Parameters for Air Interface Communication at 860 – 930 MHz
    - ISO standard for UHF Frequency
    - Read/Write capability
    - Targeted for same market as EPC standards.
- 18000 - Part 7 - Parameters for Air Interface Communication at 433.92 MHz
    - Manifest tag for Department of Defense (DoD)

ISO Standards for Animal Identification:

- ISO 11748 / 11785 - Standard for Animal Identification

ISO Supply Chain Standards:

- ISO 17358 – Application Requirements, including Hierarchical Data Mapping
- ISO 17363 – Freight Containers
- ISO 17364 – Returnable Transport Items
- ISO 17365 – Transport Unit
- ISO 17366 – Product Packaging
- ISO 17367 – Product Tagging (DoD)
- ISO 17374.2 – RFID Freight Container Identification

4. RFID Applications

The very first commercial usage of RFID technology was introduced in the late 1960s to the early 1970s. The system is called the Electronic Article Surveillance (EAS). Its primary function is to avoid shoplifting by using the simplest form of RFID with 1-bit tags. Moreover, both Wall-Mart Corporation and US Department of Defense (DOD) had issued the requirement for their suppliers to adopt RFID technology in June 2003 and October 2003 respectively [4]. Those actions are considered the biggest push for commercially using RFID technology in recent years. Nowadays, RFID technology has been applied in many areas commercially such as in health care, retailing, automotive industry, payment transaction, and so on. Some of the successful RFID applications in different areas will be introduced below.

- Automotive Industry:
  Perhaps, one of the most common RFID applications in automotive industry is vehicle immobilizer. A vehicle immobilizer is basically a system that prevents a vehicle from being driven if a wrong RFID tag is provided. Almost over 40 percent of new cars produced in North America are equipped with some sort of RFID-enable immobilizer. Besides this antitheft system, RFID technology is also applied to the inventory management in automotive industry to maintain inventory status [3].

- Payment Transactions:
  In the United States, many RFID-based payment system can be found in marketplaces such as Speedpass offered by ExxonMobil and ExpressPay conducted by American Express. In addition, RFID-based payment systems can also be found in transportation areas around the world such as SmarTrip used in Washington D.C. Metro system, EasyCard for Taipei Metro in Taiwan, Nagasaki Smart Card system in Japan, Oyster Card for London Transportation, and so on. Perhaps, the most remarkable RFID-based payment system in the world is the Octopus system in Hong Kong. The Octopus system allows users to use just a single smart card to pay for not just transportation fares but almost everything around users [3].

- Retailing:
  RFID-based applications in retailing are mainly for product tracking and inventory management. In June 2003, Wal-Mart Corporation issued a mandates for its top 100 suppliers to adopt passive RFID tag to all the shipments sent to three of its Texas distribution centers by January 2005. One month after the deadline, the CIO of Wal-Mart stated that more than 5 million tag reads had been taken. Also, the read rate at the case level has passed 90 percent for cases on carts, but the read rate at the case level were very low (averaging in 66 percent) for cases on pallets. Adopting RFID technology has benefited Wal-Mart in a 16 percent reduction in out-of-stock items. Moreover, replenishment for out-of-stock items is three times faster than using bar code system, and stores equipped with RFID are more effective at replenish out-of-stock items. Overall, an estimation shown by Research firm Sanford C. Bernstein & Co. stated that annually over $8 billion could be saved once Wal-Mart has fully deployed RFID through all its locations [4].

5. RFID Security and Privacy Threats

5.1 System Point of View

In [14], a taxonomy model of RFID security threats is presented. This model has two levels. There are three layers in the first level, threats of application layer, threats of communication layer, and threats of physical layer. In the second level, types of system-specific attacks associated with each layer are presented there. The taxonomy mode of security threats is shown in Fig.1.

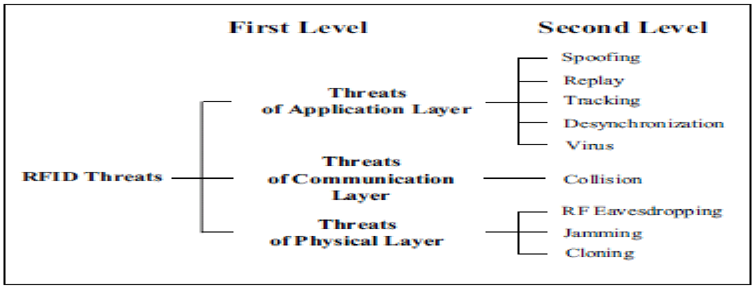


Figure 1- Taxonomy Model of RFID Security Threats [14]

- Physical Layer:
  Type of attacks in physical layer included RF eavesdropping, jamming and cloning, generally violate electromagnetic properties (RF signal) in the physical layer. Due to the reason that RFID tags and readers communicate wirelessly, RF eavesdropping can be achieved by simply using an antenna to listen to the communication. RF eavesdropping can also lead to Spoofing, Replay, and Tracking attacks if an adversary can figure out the encoding method. Jamming attack can be accomplished by constantly broadcasting RF signals. Doing so, any nearby RFID readers' operations will be disrupted. Therefore, avoiding RF signals from RFID readers reach tagged items. Cloning can be attained by reverse engineering the tags or by building a device that mimic the tag's signal.

- Communication Layer:
  Collision is the main threat in communication layer which violates the way the RFID reader single out a particular tag for communication. When more than one tag responds to RFID reader's query, collision takes place. An attacker can send out one or more signals at the same time to respond RFID reader's query in order to create collision. When collision happens, the communication between RFID tags and readers stalls. Therefore, a collision attack is also a type of Denial of Service attack (DOS).

- Application Layer:
  Spoofing, Replay, Tracking, Desynchronization, and Virus are associated to application layer. They basically violate the properties of applications such as the identification of tag, the operation related to backend system, and personal privacy (in [14], privacy threat is considered a type of security threat). Spoofing attack can be achieved by forging a tag to act as a valid tag. Doing so, an attacker can use the forged tag to fool the RFID reader and backend system to gain products and services. Replay attack focus on consuming the computing resource of the whole system. Tracking attack is related to user's personal privacy. For example, a user with a tagged item which might be read by an attacker's

reader if the reader is compatible with that tag. This will lead to several privacy issues such as location disclosure, purchase history, and so on. Desynchronization attack is a threat of desynchronizing the ID between backend system and tag's ID. This can make the tag useless. Desynchronization attack occurs when the RFID reader is failed to write ID to tags or when backend system can not transmit ID to RFID reader. Virus attack can be accomplished by injecting virus into the tag and then use SQL injection to attack the backend system.

5.2 Information Security Point of View

In [13], a different point of view looking at RFID related threats is presented. An RFID system is considered as a distributed and/or data processing system. Therefore, threats are classified using the principle of information security: Confidentiality, Availability, and Integrity. The method of attack tree is used to show lists of threats in breaching data confidentiality, availability, and integrity in a general RFID system which contains elements including tag, RFID reader, backend system, link between RFID reader and backend system, and link between RFID reader and tag. An abstract model of RFID system is depicted in Fig. 2.

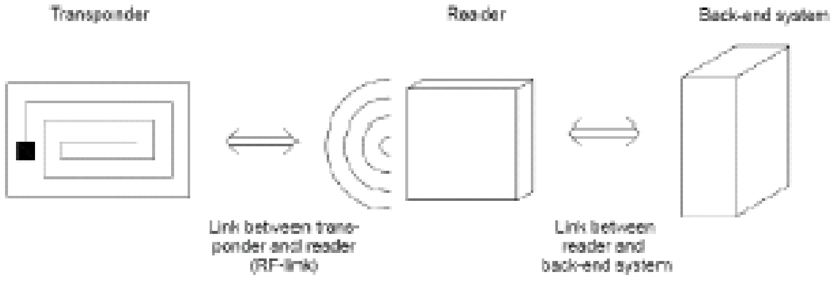

Transponder
Reader
Back-end system
Link between trans-ponder and reader (RF-link)
Link between reader and back-end system

Figure 2- Abstract Model of an RFID-System [13]

- Confidentiality:
  In a general RFID system, confidentiality of data can be breached by an attacker through the five elements described above. A listing of threats again confidentiality is shown in Fig. 3. Gaining data through tag, RFID reader, and backend system, an attacker needs to have physical access. In gaining data through links, close proximity is required for an attacker to listen to the communication. Example of attacks to breach confidentiality through link (RF link) between tag and RFID reader are tracking/tracing, sniffing, and spoofing. Tracking and tracing attacks can use the sniffed ID to track a person. This also implies privacy issues. In addition, sniffed ID can be used to clone tags. Spoofing attack can be accomplished by replay and relay attacks. Due to the size of figure, the attack tree for threat of compromising data through links can be found in Fig.4 in [13].

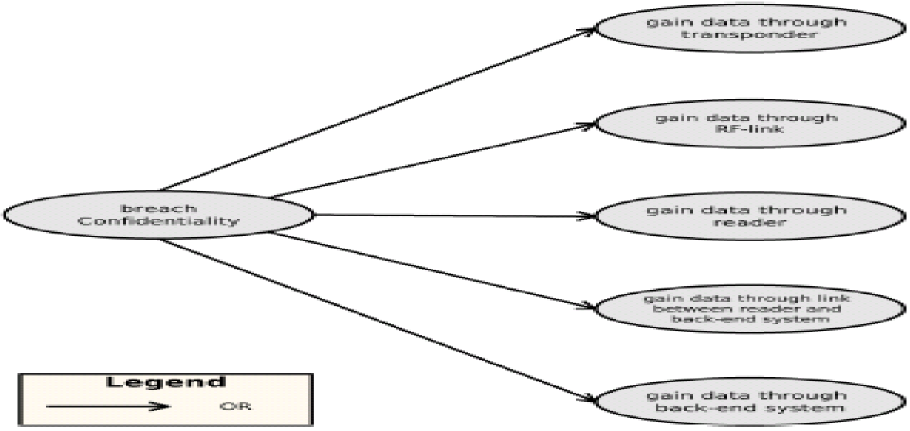

breach Confidentiality
gain data through transponder
gain data through RF-link
gain data through reader
gain data through link between reader and back-end system
gain data through back-end system
Legend
OR

Figure 3-Llisting of threats again confidentiality [13]

- Integrity:
  Fig.5 shown in [13] shows that breaching integrity of data can be achieved in four ways including: Gain permanent component authority, Component replacement, Impersonate components, Data altering. Gaining permanent component authority can happen in every one of the five elements (even sub-component of each of the five elements). Backend system and RFID reader would be the most vulnerable targets because of the realization of parts and the availability of interfaces. Gaining permanent access to links is less vulnerable since for getting permanent access to link, it requires permanent close proximity which would eventually be suspicious. Moreover, the lack of interfaces in tags (the only interface is the link) also makes it less vulnerable for an attacker to get permanent access. In addition, all components in a RFID system suffer from data altering. As to component replacement and impersonate component, they probably will only happen to the tags since they are the cheapest and the most noticeable physical component in the system.

- Availability:
  Denial-of-Service (DOS), component theft, and physical destruction of component are types of threat that could lead to violation of system availability. By covering the tags with metal or jamming the RF-channel with a blocker tag, DOS can be achieved. In addition, denial of energy of either the RFID reader or backend system can also lead to DOS. Component theft and physical destruction of component are very difficult to avoid especially for tags since the tags are the most notable one in the environment, and the ICs embedded in them are very easy to be destroyed by applying high energy field. A listing of threats against availability can be found in Fig. 6 in [13].

By examining all the attack trees of a general model of RFID system, a conclusion can be made as that every element in the system is vulnerable to threats; it is just the matter of difficulty. Table 1 in [13] forms a risk assessment. High (H): the attack is achievable with few resources or was already successfully performed. Medium (M): No successfully performed attack reported, but it is likely to happen. The required resources are kept within limit and the result benefits the attacker. Low (L): The attack requires vast resource or outweighs the attacker’s benefit.

5.3 Security and Privacy Issues in EPCglobal Class 1 Generation 2 (G1C2)

Even though C1G2 supports security mechanisms like Kill command, Access command (optional), and XOR, it is unfortunately that C1G2 still has some serious security and privacy issues. Before addressing these issues, an understanding of how C1G2 operates is necessary. A C1G2 operation steps is depicted in Fig. 4 below. There are eight steps. First, a query is sent by the reader to the tag. Second, the tag generates a 16-bit random value (RN16). Then puts the RN16 into a slot counter and starts the counter. The tag only sends the RN16 to the reader when the RN16 in the slot counter decreases to zero. Third, the reader responds to the tag with an ACK and the same RN16. Fourth, the tag compares the two RN16s. Then the tag transmits PC (Protocol-Control), EPC (Electronic Product Code), and CRC (Cyclic Redundancy Check) to the reader only when the two RN16s are matched. The reading process is done up to this point. And if the reader wants to access the tag, the following steps are needed. Fifth, the reader sends ReqRN (containing RN16) to the tag. Sixth, the tag gives the handle to the reader only if the RN16 in ReqRN is the same as RN16 in the tag. Seventh, when the reader gets the handle of the tag, it XORs the PIN with RN16. Then it sends the XORed PIN to the tag. Eighth, the tag executes the command if the PIN received from reader matches the PIN stored in the tag.

Figure 4- Process of EPCglobal Class-1 Gen-2 RFID [33]

By examining the steps, it is clear that the pseudo-random number is designed to single out a tag from a tag population. Thus the collision is taken care of in C1G2. However, the data transmitted between tag and reader is in plain text. This leads to serious problems in security and privacy such as impersonation, information leakage, and tracking/tracing threats. Besides that, the PIN being disclosed by an attacker could also happen if he/she can get the RN16 and the XORed PIN.

6. Proposed Solutions to RFID Security and Privacy Threats

6.1 Proposed Solutions to tags with no encryption capability

- Kill Command:
  Killing a tag after it has done its duty is probably the most effective and straight-forward way to protect end-user's privacy. In EPCglobal class 1 Generation 2, a kill command can be triggered by sending a 32-bit KILL PIN to the tag. When tags receive the KILL PIN, tag will be deactivated (dead) permanently. One major disadvantage about this method is that it also eliminates the future applications of the tag.

- Faraday Cage:
  Using materials like metal or foil that are impenetrable to radio signals is the basic idea of this approach. By covering a tag with those materials, it mainly blocks the communication between tags and readers. Therefore, it can provide privacy and security in certain ways. However, this approach is quite expensive and sometimes requires human interactions such as removing the material. This approach is probably the most suitable method for addressing security and privacy issues in passports since passports are usually opened when they need to be checked.

- Active Jamming:
  Using a radio frequency device to broadcast radio signals randomly in order to prevent unauthorized reads is the basic idea of active jamming. However, this approach could also lead to unstable reads from legitimate readers. Thus, this method is usually not in favored.

- Blocking:
  Blocking approach corporate with a tag's modifiable bit (called privacy bit). When the privacy bit in tags sets to 0, tags are subject to authorized or unauthorized scanning. On the other hand, if the privacy bit sets to 1, tags are in their privacy zone. In addition, the blocking method led to a specific tag called blocker tag. Its main purpose is to prevent unwanted reading of tags whose privacy bits are set to 1.

For more information about current proposed solutions for tags with or without encryption capability, please refer to [3], [8], [12], and [34].

6.2 Proposed Solutions to EPCglobal Class 1 Generation 2

Many researchers have proposed solutions to the security and privacy problems in passive tags especially in C1G2; however, most of the proposed solutions required hash function, symmetric key, and public key algorithms. This will lead to the requirements of modifications of the standard and increase the cost. In this section, a proposed protocol using Advanced Encryption Standard (AES) as well as two proposed secure schemes for C1G2 without any modifications will be discussed.

A method to integrate a one-way authentication protocol (using AES-128 encryption) into existing RFID standard (ISO 18000 and EPC) is introduced in [35]. This interleaved challenge-response protocol has two commands, sending a challenge to the tag, and requesting the encrypted value.

Procedure:

Before going into the details, an understanding of both the reader and tags share a secrete key should be established. The authentication begins after the reader has received all unique IDs of the tags. The reader first sends challenges (C1 to Cn, where n is number of tag) to tags (tag1 to tag n) one by one. Then each tag instantaneously encrypt the challenge number (Rn = Ek (Cn)) it has received. When the reader has finished sending the challenge number to the last tag, it starts to request the response of encrypted value (R1) of the first tag (T1). When the reader receives R1, it encrypts C1 and then verifies the encrypted value with R1. Note that the encrypted value of each tag will not be sent without the reader's request. The rest of tags' authentications follow the same manner. A simple example of this protocol showing authentication of 3 tags is depicted in Fig. 5.

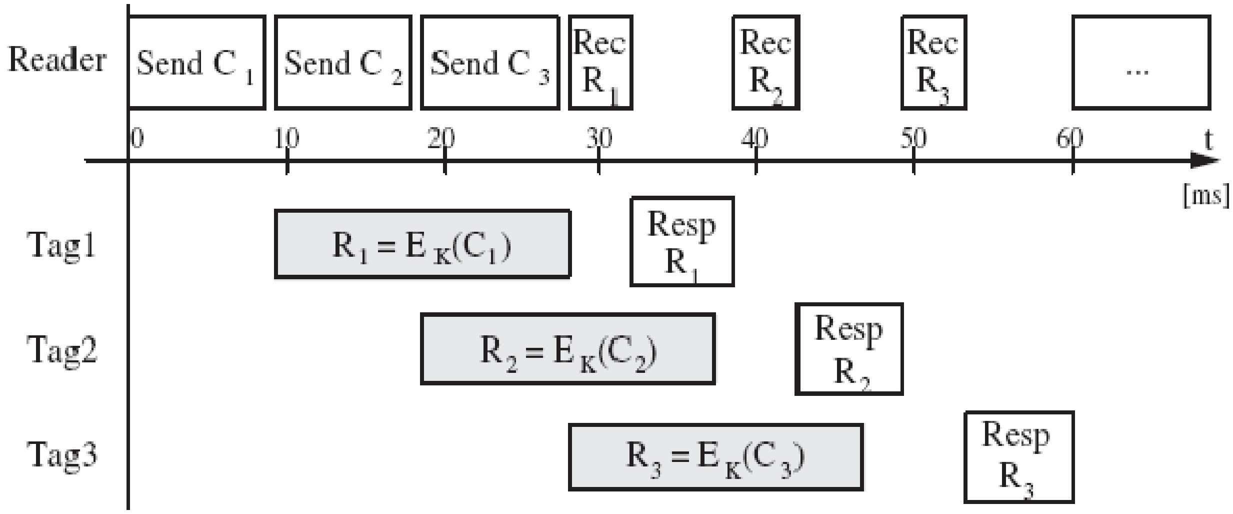


Figure 5- Interleaved challenge-response protocol in RFID systems [35]

Result:

This protocol provide very strong authentication of tag, and it mainly prevent tag from being cloning. In another word, it makes sure that the tags being read by the reader are legitimate. This protocol allows each tag to have at least 18 ms for encryption (1800 clock cycles operating at a clock frequency of 100 kHz), and at most 50 tags can be authenticated in one second. With only the AES module implementation, the current consumption needed is 8.15µA, and the encryption of 128-bit data block needs around 1000 clock cycles operating at 100 kHz. Also, estimation of 3595 gate equivalents (GEs) is required for the hardware complexity.

A secure mechanism against security and privacy issues in C1G2 without modifying the standard is proposed in [33]. The mechanism assumes that the communication between reader and backend server is secure. In addition, 32-bit pseudo-random number generator is assumed to be used in both C1G2 reader and tag. A notation table is formed below and is used to describe the procedures of this mechanism.

Notation	Description
RT32	32-bit random number generated by a tag
RR32	32-bit random number generated by a reader
PIN1, PIN2	Two EPCglobal C1G2 PINs (access, kill)
EPC	Electronic Product Code
f	32-bit pseudo-random number generator
n	The number of tags in the system
||	Concatenation of two inputs
⊕	Exclusive of two inputs

Procedures:

First, a reader sends query request to a tag Ti. Second, the tag sends M1 to the reader where RT32 is the pseudo-random number generated by the tag, PIN1i is the access pin of the tag, and M1 = RT32 ⊕ PIN1i. Third, the reader sends ACK(M1) and RR32 to the tag after it has received M1. Forth, the tag calculates M2, M3, T, and E then forwards PC, E, CRC16 to the reader, where M2 = RR32 ⊕ PIN2i ⊕ RT32, M3 = f(M2), T = 0||RT32||M2||M3 (the last bit of T is removed), and E = (T + Si) ⊕ EPCi (the first bit of Si is always 0). Fifth, the reader sends E, M1, and RR32 to a backend server. Sixth, the backend server starts to decrypt the message by calculating RT32', M2', M3', and T' then searches for a match E, where RT32' = M1 ⊕ PIN1j, M2' = RR32 ⊕ PIN2j ⊕ RT32', M3' = f(M2'), T' = 0||RT32'||M2'||M3' (the last bit of T' is removed), and E = (T'+Sj) ⊕ EPCj.

If the reader wants to operate commands such as killing the tag, the PINs will be transmitted. To prevent PINs from revealing, the following process should be taken.

Seventh, the reader sends a PIN request to the backend server. Eighth, the backend server calculates P and then forwards P to the tag through the reader, where P = PIN ⊕ M3'. PIN could be PIN1j or PIN2j. It depends on operations. Finally, the tag verifies PIN = P $\oplus$ M3. If the PIN matches, the tag carries out the command. The process of this mechanism is shown in Fig.6.

Figure 6- Process flow chart [33]

Result:

Since T (96 bits) is equal to 0||RT32||M2||M3, M2 and M3 is calculated using random numbers, and E is equal to (T + Si) $\oplus$ EPCi, it is very difficult for an attacker to attain any useful information. Literally, an attacker needs to guess 96 bits in order to get the EPC code. The probability for an attacker to successfully get all the correct 96 bits in first try is $\frac{1}{2^{96}}$. In addition, every parameter involved in E changes every session. Therefore, it is nearly impossible for an attacker to get in EPC code. This addresses the privacy and tag-cloning problems. Moreover, PIN is totally secure in this solution since P = PIN $\oplus$ M3’ and M3’ never be transmitted in plant-text in the communication.

In [29], a security scheme using only the commands and security components defined in C1G2 standard is introduced. This scheme involves two phases, the Setup phase and the Secure Inventory phase, and its main focus is to prevent traceability and tag cloning. Moreover, three assumptions are made in this scheme including: all C1G2 tags implement ACCESS passwords and their values are unique to each other, the tags’ memories should be written before distribution, and the DB (database) stores all information about tags and security information.

Before getting into the details, it is essential to review the logical memory map of C1G2 tag and the notations used in this scheme. The memory map and notation table are show below.

Memory Map	Description
The reserve memory (Bank 00)	Contains 32-bit KILL and ACCESS password.
The code memory (Bank 01)	Has code, PC (Protocol Control) and CRC16 necessary for identifying the item where a tag is affixed, code parsing, and protection of (code +PC) and certain backscattered sequences, respectively.
The TID memory (Bank 10)	Consists of 32-bit of TID values which may include tag model number, vendor information, etc.
The user memory (Bank 11)	Allows user-specific storage, so the memory organization is user-defined.

Notation	Description
Ti	Gen2 tag which has I index
R	Gen2 reader
S	Backend server with DB
I	Tag issuing system (e.g. Tag printer or tools for writing tags)
h	One-way hash function
$\oplus$	XOR operation
Codei	RFID code (e.g. EPC) for Ti
PCi	PC bits for Ti
ACCESSi	ACCESS password for Ti
KILLi	KILL password for Ti
PASSWORDi	ACCESSi or KILLi
RAND_A, RNAD_B	Random numbers

The Setup Phase:

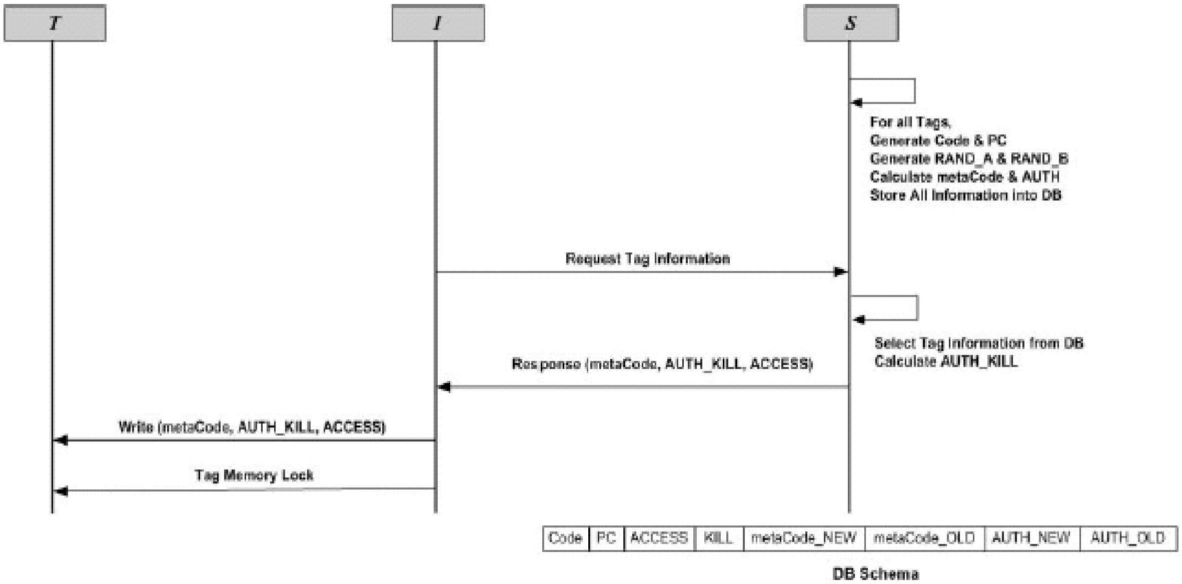
In this scheme, all the computations are done in the server. Before distributing the tags, there are six steps should be done in the Setup Phase. First, S generates Codes, PCs, RAND_A, and RAND_B for each Ti. After that, S calculates metaCodes and AUTHs using the equations shown below:

(1) metaCodei = h(Codei, PCi, RAND_Ai);
(2) AUTHi = h(Codei, PASSWORDi, RNAD_B);

All the information is stored in the DB (database). Second, I sends request to server for the information for Ti. Third, S computes AUTH_KILLi using the equation shown below:

(3) AUTH_KILLi = KILLi $\oplus$ AUTHi;

Forth, S sends metaCodei, AUTH_KILLi, and ACCESSi to I. Fifth, I writes the information sent by S to Ti. Sixth, I uses ACESS and LOCK commands with ACCESSi to configure Bank 00 to unreadable and un-writeable and the rest (Bank 01, Bank 10, and Bank11) to unreadable. After these steps, tags are ready to be used. The Setup Phase figure is shown in Fig.7.


T
I
S
For all Tags,
Generate Code & PC
Generate RAND_A & RAND_B
Calculate metaCode & AUTH
Store All Information into DB
Request Tag Information
Select Tag Information from DB
Calculate AUTH_KILL
Response (metaCode, AUTH_KILL, ACCESS)
Write (metaCode, AUTH_KILL, ACCESS)
Tag Memory Lock

Code	PC	ACCESS	KILL	metaCode_NEW	metaCode_OLD	AUTH_NEW	AUTH_OLD

DB Schema

Figure 7- The Setup Phase [29]

The Secure Inventory Phase:

An example of R trying to inventory Ti is used here to describe the process of the Secure Inventory Phase. At first, R requests the code from Ti. Second, Ti replies with its metaCode. This metaCode is then forwarded to S by R. Third, S generates a set of new RAND_A and RAND_B and then computes meatCode_NEWi, AUTH_NEWi, and AUTH_KILL_NEWi using equation (1), (2), and (3) after receiving metaCodei. Forth, S sends ACCESSi, metaCode_NEWi, and AUTH_KILL_NEWi to R. Fifth, R uses ACCESSi to change all memory banks of Ti to readable and writeable, and then R reads AUTH_KILLi. At this point, Ti can ensure that R is an authorized reader if the operation of R reading AUTH_KILLi is successful since only legitimate readers can acquire ACCESS of Ti from S. Sixth, Ti sends AUTH_KILLi to R after authentication is ensured. Seventh, R sends AUTH_KILLi to S. Eighth, S recovers the KILLi by performing KILLi = AUTH_KILLi ⊕ AUTHi and then matches the recovered KILL password with the original KILL password. If they match, S can ensure that Ti is a legitimate tag. Ninth, S sends the result of authentication to R. Tenth, R writes metaCode_NEWi and AUTH_KILL_NEWi to Ti and then changes the status of memory banks of Ti to unreadable/un-writable for Bank 00 and un-writeable for the rest if the result of the authentication comes back positive. Eleventh, R send an acknowledgement of completing writing and locking to S. Then S updates its DB. The Secure Inventory Phase figure is shown in Fig.8.

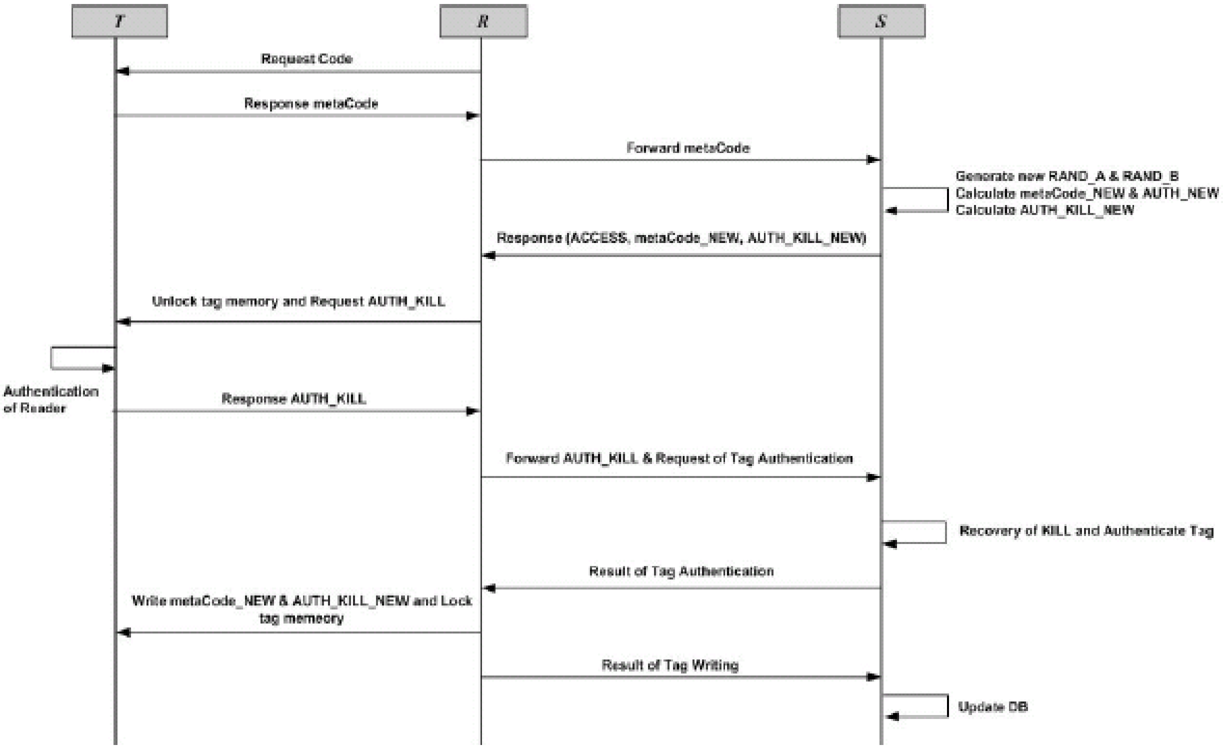

T
R
S
Request Code
Response metaCode
Forward metaCode
Generate new RAND_A & RAND_B
Calculate metaCode_NEW & AUTH_NEW
Calculate AUTH_KILL_NEW
Response (ACCESS, metaCode_NEW, AUTH_KILL_NEW)
Unlock tag memory and Request AUTH_KILL
Authentication of Reader
Response AUTH_KILL
Forward AUTH_KILL & Request of Tag Authentication
Recovery of KILL and Authenticate Tag
Result of Tag Authentication
Write metaCode_NEW & AUTH_KILL_NEW and Lock tag memeory
Result of Tag Writing
Update DB

Figure 8- The Secure Inventory Phase [29]

Result:

As shown in the Secure Inventory Phase, a mutual authentication between the tag and the backend server is accomplished. Therefore, the tag cloning problem, as promise, is addressed. In addition, the traceability and anonymity (privacy issues) are prevented since the metaCode and encrypted KILL password is changed in every inventory.

7. Conclusion

Although recent actions about RFID technology taken by Wal-Mart Corporation and Department of Defense has heat up the topic of RFID once again since WWII, the technology has not yet been proliferating as expects. This is mainly due to the reasons of the lack of standardization, the security/privacy issues, and more importantly the cost. To decrease the cost, standardization is a very important factor. In addition, security/privacy issues are barriers to people's acceptance of this technology. Therefore, more works have to be done in standardization and addressing the security/privacy issues in order to proliferate the adoption of RFID technology.

References

[1] "The History of RFID Technology," RFID Journal, 20 Dec. 2005; http://www.rfidjournal.com/article/view/1338/1/129.

[2] J. Landt, "Scrouds of Time: The History of RFID," 1 Oct. 2001; http://www.rfidconsultation.eu/docs/ficheiros/shrouds_of_time.pdf.

[3] J. Banks, David Hanny, Manuel A. Pachano, and Les G. Thompson, *RFID APPLIED.* NJ: John Wiley & Sons, Inc., 2007.

[4] F. Thornton, B. Haines, Anand M. Das, H. Bhargabva, A. Campbell, and J. Kleinschmidt, *RFID Security*. MA: Syngress Publishing Inc., 2006.

[5] M. Ward and R.V. Kranenburg, "RFID: Frequency, standards, adoption and Innovation," JISC Technology and Standards Watch, May 2006. http://www.jisc.ac.uk/media/documents/techwatch/tsw0602.pdf.

[6] "A Summary of RFID Standards," RFID Journal, 2005; http://www.rfidjournal.com/article/view/1335/1.

[7] "RFID Standards," http://www.scansource.eu/en/education.htm?eid=12&elang=en.

[8] Evsen korkmaz and Alp Ustundag, "Standards, Security & Privacy Issues about Radio Frequency Identification (RFID)" *RFID Eurasia 1st Annual,* pp. 1-10, Sept. 2007.

[9] N. C. Wu, M. A. Nystrom, T. R. Lin, and H. C. Yu, "Challenges to RFID Adoption" *Technology Management for the Global Future, PICMET,* vol. 2, pp. 618-623, July. 2006.

[10] A. Razaq, Wai Tong Luk, Kam Man Shum, Lee Ming Cheng, and Kai Ning Yung, "**Second-Generation RFID"** *Security & Privacy, IEEE,* vol. 6, no. 4, pp. 21-27, July-Aug. 2008.

[11] Syed Ahson and Mohammad Ilyas, *RFID HANDBOOK*. FL: Taylor & Francis Group, 2008.

[12] A. Juels, "**RFID security and privacy: a research survey"** *Selected Areas in Communications, IEEE Journal,* vol. 24, no. 2, pp. 381-394, Feb. 2006.

[13] T. Schaberreiter, C. Wieser, I. Sanchez, J. Riekki, and J. Roning, "An Enumeration of RFID Related Threats" *Mobile Ubiquitous Computing, Systems, Services and Technology, UBICOMM,* pp. 381-389, Oct. 2008.

[14] Ding Zhen-hua, Li Jin-tao, and Feng Bo, "A Taxonomy Model of RFID Security Threats" *Communication Technology, ICCT,* pp. 765-768, Nov. 2008.

[15] Park Joo-Sang, Kim Young-Il, and Lee Yong-Joon, "**Security considerations for RFID technology adoption"** ***Advanced Communication Technology, ICACT,*** **vol. 2, pp. 797-803, 2005.**

[16] M. Ohkubo, K. Suzuki, and S. Kinoshita, "**RFID Privacy Issues and Technical Challenges"** *Communications of The ACM,* vol. 48, no. 9, pp. 66-71, Sept. 2005.

[17] M.R. Rieback, B. Crispo, and A.S. Tanenbaum, "The Evolution of RFID security" *Pervasive Computing , IEEE,* vol. 5, no. 1, pp. 62-69, Jan.-March 2006.

[18] M. Meingast, J. King, D.K. Mulligan, "**Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport** " *IEEE International Conference on RFID,* pp. 7-14, March 2007.

[19] Y.-C. Lee, Y.-C. Hsieh, P.-S. You, and T.-C. Chen, "**An Improvement on RFID Authentication Protocol with Privacy Protection"** ***Convergence and Hybrid Information Technology, ICCIT,*** **vol. 2, pp. 569-573, Nov. 2008.**

[20] T. Phillips, T. Karygiannis, and R. Kuhn, **"Security standards for the RFID market"** ***Security & Privacy , IEEE,*** **vol. 3, no. 6, pp. 85-89, Nov.-Dec. 2005.**

[21] R. Weinstein, "**RFID: a technical overview and its application to the enterprise"** ***IT Professional,*** **vol. 7, no. 3, pp. 27-33, May-June 2005.**

[22] C. Floerkemeier and S. Sarma, "**An Overview of RFID System Interfaces and Reader Protocols"** *IEEE International Conference on RFID,* pp. 232-240, April 2008.

[23] Roy Want, "The Magic of RFID" **"** ***ACM Queue,*** **vol. 2, no. 7, pp. 40-48, Oct. 2004.**

[24] M.M. Hossain and V.R. Prybutok, "**Consumer Acceptance of RFID Technology: An Exploratory Study"** ***Engineering Management, IEEE Trans.,*** **vol. 55, no. 2, pp. 316-328, May 2008.**

[25] K.H.S.S. Koralalage and Jingde Cheng, "**A Comparative Study of RFID Solutions for Security and Privacy: POP vs. Previous Solutions"** ***Information Security and Assurance, ISA,*** **pp. 342-349, April 2008.**

[26] Sanjay Sarma, "Integrating RFID" ***ACM Queue,*** **vol. 2, no. 7, pp. 50-57, Oct. 2004.**

[27] Staake, Thorsten, Thiesse, Frédéric, and Fleisch, Elgar, "Extending the EPC network - The potential of RFID in anti-counterfeiting" *Proceedings of the ACM Symposium on Applied Computing*, vol. 2, pp. 1607-1612, 2005.

[28] S.C.g. Periaswamy, S. Bharath, M. Chagarlamudi, S. Estes, and D.R. Thompson, "**Attack Graphs for EPCglobal RFID"** ***Region 5 Technical Conference, IEEE,*** **pp. 391-396, April 2007.**

[29] Jaemin Park, Junchae Na, and Minjeong Kim, "A practical approach for enhancing security of EPCglobal RFID Gen2 tag" *Proceedings of the 15th International Conference on Advanced Computing and Communications, ADCOM*, pp. 436-441, 2007.

[30] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "LAMED - a PRNG for EPC class-1 generation-2 RFID specification" *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 88-97, Jan. 2009.

[31] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis, "**Analysis of Threats to the Security of EPC Networks"** *Communication Networks and Services Research Conference, CNSR,* pp. 67-74, May 2008.

[32] M. Feldhofer and C. Rechberger, "A Case Against Currently Used Hash Functions in RFID Protocol" *OTM 2006 Workshops, LNCS 4277,* p 372-381, 2006

[33] Kyoung Hyun Kim, Eun Young Choi, Su Mi Lee, and Dong Hoon Lee, "Secure EPCglobal class-1 gen-2 RFID system against security and privacy problems" *OTM 2006 Workshops, LNCS 4277,* p 362-371, 2006.

[34] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis, "**Security Threats on EPC Based RFID Systems"** *Information Technology: New Generations, ITNG,* pp. 1242-1244, April 2008.

[35] M. Feldhofer, S. Dominikus, and j. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm" *Cryptographic Hardware and Embedded Systems - CHES 2004. 6th International Workshop. Proceedings (Lecture Notes in Comput. Sci. vol.3156)*, p 357-370, 2004.