Security and User Privacy for Mobile-RFID Applications in Public Zone

Divyan M. Konidala, Hyunrok Lee, Dang Nguyen Duc, Kwangjo Kim
Information and Communications University (ICU),
International Research Center for Information Security,
R504, 103-6, Munji-Dong, Daejeon 305-714, Republic of Korea.
{*divyan, tank, nguyenduc, kkj*}@*icu.ac.kr*

Abstract

To make RFID technology assist people in their daily lives, a new technology called "Mobile-RFID" (mRFID) is being considered. The mRFID technology incorporates RFID-reader functionality into portable handheld devices. In a public zone (e.g., street, shopping mall) we can use our mobile phone as an mRFID-reader to scan tagged merchandize and quickly download information about that merchandize. In this paper we emphasize that, with the ubiquitous presence of mRFID-readers all around us, in the form of mobile phones, we also need to consider some special security and privacy threats. We propose a security framework, which addresses issues such as: identifying cloned fake tags attached to counterfeit products, consumer authorization, secure and anonymous communication with only genuine information-servers that provide information about a particular tagged item, blocking malicious mRIFD-readers from snooping on the tagged items in our possession, and finally, a simple and secure mRFID payment scheme.

1. Introduction

1.1. RFID Technology

Radio Frequency IDentification (RFID) [1] technology offers strategic advantages for businesses because it can provide efficient real-time product track and trace capability. VeriSign [2] gives a detailed description about advantages of RFID technology for supply chain management. With RFID technology, manufacturers attach Passive-RFID tags to their products. To prevent corporate espionage, and leakage of sensitive tag data to malicious RFID readers, most of the tags contain a unique Electronic Product Code (EPC) number and further information about the product (e.g., product description, manufacturing date, packaging, shipments, product arrival and departure details, *etc.*) is stored on a network of databases, called the EPC-Information Services (EPC- IS). A RFID reader uses EPC number to locate the right EPC-IS, from where it can download and upload data about the product it scanned. Therefore, EPC-IS assists geographically distributed supply chain stakeholders to easily and efficiently access and share information on any product they are handling. EPCglobal Inc [3] is leading the development of industry-driven standards for the EPC to support the use of RFID in supply chain management. We composed this paper based on the following ratified standards: (i) EPCglobal Architecture Framework [4], (ii) EPCglobal Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz 960MHz [5].

1.2. Mobile RFID Technology

Currently RFID tags are still expensive, but very soon it would become economical for large-scale use of tags on consumer goods. As a result, objects can provide real-time information about themselves. RFID technology will have a tremendous impact on our society, once it starts to assist people in their daily lives. A right step in this direction is Mobile-RFID (mRFID) technology, where a RFID-reader chip is embedded into handheld portable devices like mobile phones and PDAs. A mobile phone can also behaves as an mRFID-reader. By bringing a mRFID-reader near to a RFID-tagged object, we can quickly and easily scan the tag and download information represented by that tag and view the information on our mobile device's display screen. For example: information from tagged signposts, and movie posters, price information from tagged merchandize, and verifying a merchandize is genuine or counterfeit by checking the authenticity of the tag attached to it, *etc.*

2. Motivation and Goals of this Paper

With the advent of RFID and mRFID technology we can find a public zone, where Service Providers (SP) *e.g.*, manufacturers, shopping malls, department stores, cinema halls, *etc.*, deploy tagged items such as consumer goods, posters, sign boards, and shopping catalogs, *etc.*, all around us. There would also be a ubiquitous presence of mRFID-readers. This development leads to the following security requirements and threats. In this paper we assume that most of the consumer goods are tagged with EPCglobal C-1 Gen-2 UHF tags. Therefore, in order to achieve the below mentioned security goals, we propose a security framework that also adheres to the EPCglobal standards.

Tag and mRFID-reader Mutual Authentication

The EPC number on a genuine tag can be easily scanned, copied and be embedded onto a fake tag. These cloned fake tags can be attached to counterfeit products. Therefore before purchasing a product, a consumer should use his/her mRFID-reader to authenticate the tag, in order to prove beyond doubt that the tag attached to a product is indeed from the original manufacturer/SP of the product. On the other hand malicious mRFID-readers can also corrupt and modify the tag's data. Therefore, a tag must also be able to authenticate its mRFID-reader.

mRFID-reader must Securely and Anonymously Communication with Genuine SP's EPC-IS

After scanning a tag, consumer's mRFID-reader must be protected from being directed to, accessing, and downloading information, from malicious EPC-IS, which can either induce virus code or extract sensitive data off the mRFID-reader. Also the true identity of the consumer must never be revealed (Anonymity) to the SP, otherwise SP can generate detailed profiles of the consumer, his buying interests and trace all his actions.

mRFID-reader (Consumer) Authorization

As per the privileges of the consumer *e.g.* juvenile, adult, VIP member, *etc.*, EPC-IS must categorize which mRFID-reader is entitled to download what kind of information. This requires efficient authorization and access-control.

Consumer Privacy Protection from Malicious mRFID-readers

An adversary can use his mRFID-reader to scan and retrieve sensitive information off any tagged item that the consumer is carrying in her shopping bag/purse. Therefore we need to protect the privacy of the consumer.

Simple, Secure, and Anonymous Payment Scheme for a mRFID-reader Purchase Transaction

If a consumer wants to buy a tagged product, we also propose a scheme where a mRFID-reader can be used to securely and anonymously pay for the product and the consumer can walk away from the store with the product, without having to wait in the queue at the point-of-sale (cashier).

3. Related Work

Our previous work on mRFID technology [6] provides detailed description on only the security challenges pertaining to various mRFID applications at Location-based Services zone (Public Zone), Enterprise Zone, and Private Zone. In this paper we focus on mRFID applications at a Public Zone and propose a detailed security framework.

Table 1. Notations.

Notation	Description
Req_R	Command Requesting 16bit Random No.
R_{Tx}	16bit Random Generated by Tag
R_{Mx}	16bit Random Generated by Manufacturer
APwd	Tag's Access Password
KPwd	Tag's Kill Password
$APwd_M$	16 MSBs of APwd
$APwd_L$	16 LSBs of APwd
$CCPwd_M$	Cover-Coded $APwd_M$
$CCPwd_L$	Cover-Coded $APwd_L$
PAD_x	Generated Pads for Cover-Coding
$\|$	Concatenation
$\oplus$	Bit-wise XOR Operation

However to achieve our first goal *i.e.* "Tag and mRFID-reader Mutual Authentication", we improved the one-way weak reader-to-tag authentication scheme proposed by EPCglobal C-1 Gen-2 UHF RFID protocol standard [5]. In the following subsection we provide a detailed description of the EPCglobal scheme and also its security weaknesses. Table 1 provides the list of notations we used in this paper. Juels [7] summarized many previously proposed tag-reader authentication schemes. Most of the proposed solutions [8], [9] depend on hash function. But due to constrained resources, C-1 Gen-2 tags are not capable of executing cryptographic hash function like MD5 and SHA-1. LMAP [10], and M^2AP [11] are two ultra-lightweight RFID mutual authentication protocols, which use only simple bitwise operations. But Li and Wang [12] proved that these two protocols fail under de-synchronization attack, and full-disclosure attack. Therefore, unlike these schemes, the main advantage of our proposed scheme is that it does not require the implementation of any special cryptographic hash functions/keys within the tag. There is also no need for the tag and the mRFID-reader to synchronize any values.

3.1. Security Assessment of EPCglobal C-1 Gen-2 UHF RFID Protocol [5]

As per EPCglobal Class 1 Gen 2 UHF RFID Protocol standard, a tag's chip has four memory banks: Reserved, EPC, TID, and User. Reserved memory bank is used to store 32-bit *Access Password* (APwd) and 32-bit *Kill Password* (KPwd), and EPC memory bank for EPC number. The reserved memory bank is permanently locked by the manufacturer; therefore APwd and KPwd can neither be read nor modified by any reader. The tag has the capability to verify these two passwords. A reader that presents the right APwd, is allowed to carry out mandatory commands such as Read, Write, and Lock on the tag. If a reader sends the right KPwd, the tag enters the *Killed State*, where it is permanently disabled. The standard does not provide details on how to securely communicate the APwd and KPwd to the readers. Tags can generate 16-bit random or pseudo-random numbers R_{Tx}. While powered, tags can temporarily store at least two R_{Tx}. Reader first issues a command Req_R requesting a random number, rest of the scheme is fairly easy to understand by studying the multi-step procedure shown in Fig. 1. R_{Tx} is used has XOR pad to obscure APwd, this is known as Cover-Coding APwd (CCPwd). Each XOR operation shall be performed first on APwd's 16-Most Significant Bits (MSB) $APwd_M$, followed by 16-Least Significant Bits (LSB) $APwd_L$.

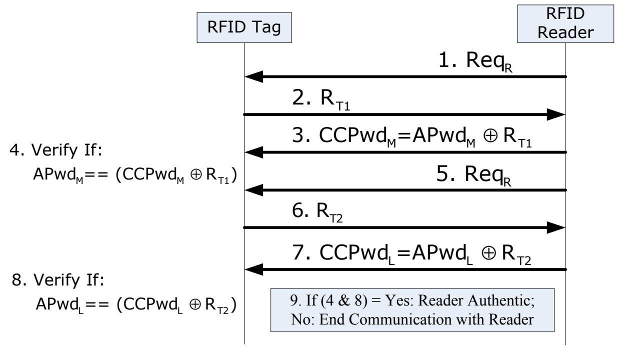

RFID Tag
RFID Reader
1. Req_R
2. R_{T1}
3. $CCPwd_M = APwd_M \oplus R_{T1}$
4. Verify If:
$APwd_M == (CCPwd_M \oplus R_{T1})$
5. Req_R
6. R_{T2}
7. $CCPwd_L = APwd_L \oplus R_{T2}$
8. Verify If:
$APwd_L == (CCPwd_L \oplus R_{T2})$
9. If (4 & 8) = Yes: Reader Authentic;
No: End Communication with Reader

Figure 1. Security Weakness of EPCglobal C-1 Gen-2 UHF RFID Protocol

Security Weakness: This scheme is not at all secure, as the tag sends both the R_{Tx} in open and un-encrypted form. Therefore any eavesdropping malicious reader, a disgruntled or compromised employee can easily capture these R_{Tx}, and by carrying out $R_{Tx} \oplus CCPwd$ gives away the APwd. An exposed APwd also allows malicious reader to illegally access, corrupt and modify tag's data. An exposed APwd would easily assist an adversary to create cloned fake tags with the same APwd.

4. Proposed Security Framework

Entities: In our proposed security framework we consider the following entities:

(i) mRFID-reader

(ii) RFID-Tags attached to consumer goods

(iii) Mobile Operator (MO): In the current mobile communications paradigm we have already put in a great deal of trust in MO. Our framework extends this trust in MO to secure and provide privacy protection for consumers. This approach is very practical and easily deployable, as the current mobile communications infrastructure is widely spread and highly stable. MO takes responsibility on behalf of mRFID-reader to select, identify, and authenticate genuine SP's ECP-IS. MO behaving like a Trusted Proxy processes the request on behalf of the mRFID-reader, greatly reducing the communication and computational burden on the consumer's mobile phone/PDA and also provides consumer privacy protection.

(iv) Manufacturer's EPC-IS (M): For commercial gains both MO and SPs (whom MO trusts) mutually agree to provide mRFID services to consumers. In the following framework we consider a product Manufacturer as our Service Provider, who manages EPC-IS.

Assumption: We assume that the communication channel between (i) Consumer and Mobile Operator and (ii) Mobile Operator and Manufacturer's EPC-IS is secure (use of Public-Key cryptosystem, and HTTP-Transport Layer Security (TLS)).

4.1. Description

Our proposed scheme can be easily understood by looking at Fig. 2. Steps 1-5 details mRFID-reader Authentication Process. Steps 6-9 describe Tag Authentication Process. Please note that Steps 1-9 are carried out in one interrogation session between the tag and the reader.

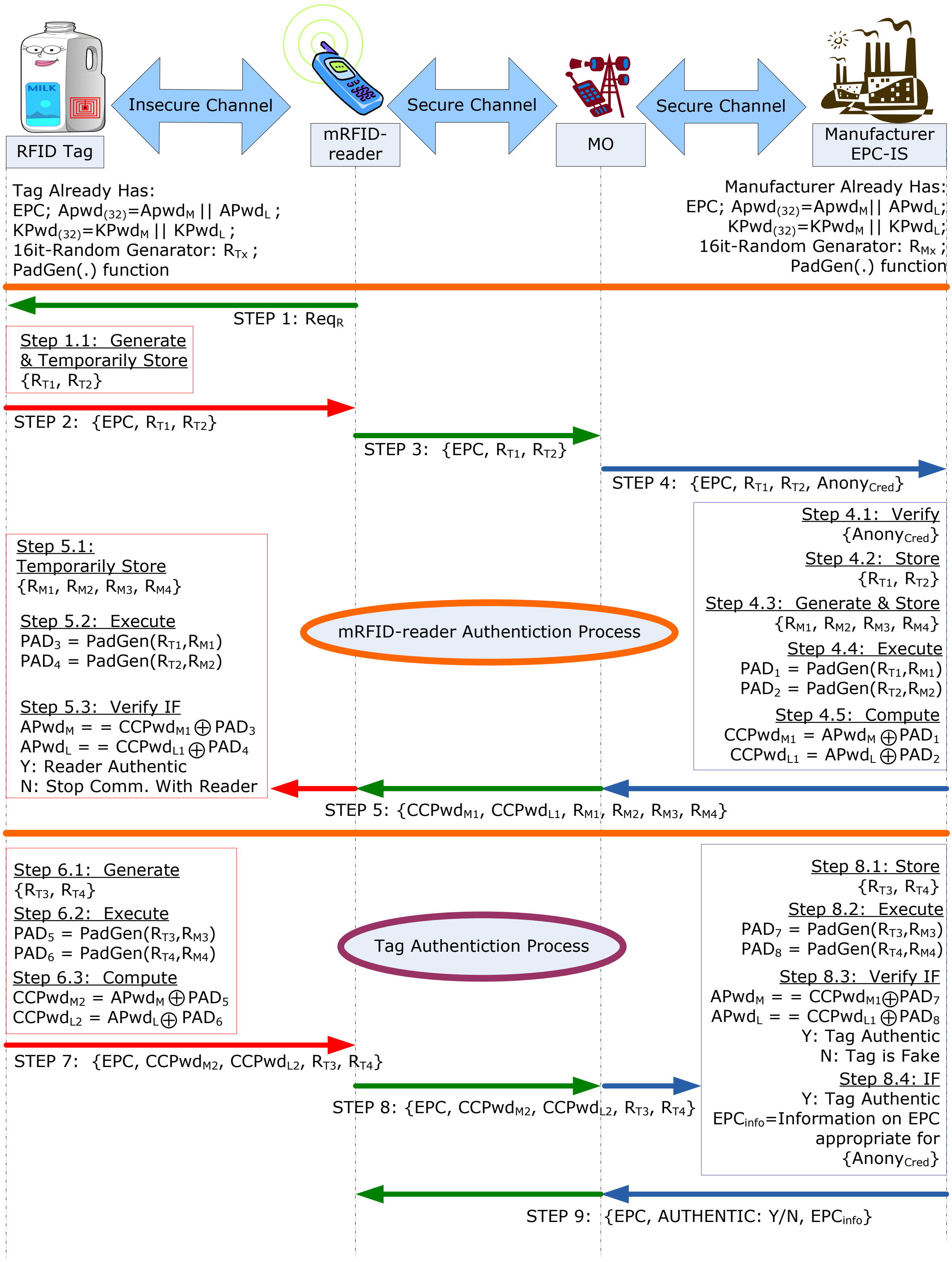
Pad Generation Function - PadGen(.):
Formula:
$CCPwd_M = APwd_M \oplus PAD$
$PAD = PadGen(R_{Tx}, R_{Mx})$
$= KPadGen(APadGen(R_{Tx}, R_{Mx}), R_{Tx})$

Let us represent the 32-bit APwd as:
Binary (Base 2) Notation: $a \in \{0,1\}$
APwd = $APwd_M \| APwd_L$
$APwd_M = a_0 a_1 a_2 \cdots\cdots a_{13} a_{14} a_{15}$
$APwd_L = a_{16} a_{17} a_{18} \cdots\cdots a_{29} a_{30} a_{31}$

Let us represent the 32-bit KPwd as:
Binary (Base 2) Notation: $k \in \{0,1\}$
KPwd = $KPwd_M \| KPwd_L$
$KPwd_M = k_0 k_1 k_2 \cdots\cdots k_{13} k_{14} k_{15}$
$KPwd_L = k_{16} k_{17} k_{18} \cdots\cdots k_{29} k_{30} k_{31}$

Let us represent the 16-bit random R_{Tx} by Tag as:
Hexadecimal (Base 16) $ht \in \{0,1,\cdots,9,A,\cdots,F\}$
$R_{Tx} = ht_1 ht_2 ht_3 ht_4$
Decimal (Base 10) $dt \in \{0,1,\cdots,15\}$
$ht_i = dt_i$
$R_{Tx} = dt_1 dt_2 dt_3 dt_4$

Let us represent the 16-bit random R_{Mx} by Mfr. as:
Hexadecimal (Base 16) $ht \in \{0,1,\cdots,9,A,\cdots,F\}$



RFID Tag
Insecure Channel
mRFID-reader
Secure Channel
MO
Secure Channel
Manufacturer EPC-IS
Tag Already Has:
EPC; $Apwd_{(32)}$=$Apwd_M$ || $APwd_L$;
$KPwd_{(32)}$=$KPwd_M$ || $KPwd_L$;
16it-Random Genarator: R_{Tx} ;
PadGen(.) function
Manufacturer Already Has:
EPC; $Apwd_{(32)}$=$APwd_M$|| $APwd_L$;
$KPwd_{(32)}$=$KPwd_M$ || $KPwd_L$;
16it-Random Genarator: R_{Mx} ;
PadGen(.) function
STEP 1: Req_R
Step 1.1: Generate & Temporarily Store
{R_{T1}, R_{T2}}
STEP 2: {EPC, R_{T1}, R_{T2}}
STEP 3: {EPC, R_{T1}, R_{T2}}
STEP 4: {EPC, R_{T1}, R_{T2}, $Anony_{Cred}$}
Step 4.1: Verify
{$Anony_{Cred}$}
Step 4.2: Store
{R_{T1}, R_{T2}}
Step 4.3: Generate & Store
{R_{M1}, R_{M2}, R_{M3}, R_{M4}}
Step 4.4: Execute
PAD_1 = PadGen(R_{T1},R_{M1})
PAD_2 = PadGen(R_{T2},R_{M2})
Step 4.5: Compute
$CCPwd_{M1}$ = $APwd_M \oplus PAD_1$
$CCPwd_{L1}$ = $APwd_L \oplus PAD_2$
Step 5.1:
Temporarily Store
{R_{M1}, R_{M2}, R_{M3}, R_{M4}}
Step 5.2: Execute
PAD_3 = PadGen(R_{T1},R_{M1})
PAD_4 = PadGen(R_{T2},R_{M2})
Step 5.3: Verify IF
$APwd_M$ = = $CCPwd_{M1} \oplus PAD_3$
$APwd_L$ = = $CCPwd_{L1} \oplus PAD_4$
Y: Reader Authentic
N: Stop Comm. With Reader
mRFID-reader Authentiction Process
STEP 5: {$CCPwd_{M1}$, $CCPwd_{L1}$, R_{M1}, R_{M2}, R_{M3}, R_{M4}}
Step 6.1: Generate
{R_{T3}, R_{T4}}
Step 6.2: Execute
PAD_5 = PadGen(R_{T3},R_{M3})
PAD_6 = PadGen(R_{T4},R_{M4})
Step 6.3: Compute
$CCPwd_{M2}$ = $APwd_M \oplus PAD_5$
$CCPwd_{L2}$ = $APwd_L \oplus PAD_6$
Tag Authentiction Process
Step 8.1: Store
{R_{T3}, R_{T4}}
Step 8.2: Execute
PAD_7 = PadGen(R_{T3},R_{M3})
PAD_8 = PadGen(R_{T4},R_{M4})
Step 8.3: Verify IF
$APwd_M$ = = $CCPwd_{M1} \oplus PAD_7$
$APwd_L$ = = $CCPwd_{L1} \oplus PAD_8$
Y: Tag Authentic
N: Tag is Fake
Step 8.4: IF
Y: Tag Authentic
EPC_{info}=Information on EPC
appropriate for
{$Anony_{Cred}$}
STEP 7: {EPC, $CCPwd_{M2}$, $CCPwd_{L2}$, R_{T3}, R_{T4}}
STEP 8: {EPC, $CCPwd_{M2}$, $CCPwd_{L2}$, R_{T3}, R_{T4}}
STEP 9: {EPC, AUTHENTIC: Y/N, EPC_{info}}

Figure 2. Tag & mRFID-reader Mutual Authentication, Secure & Anonymous Communication with Genuine EPC-IS, and Consumer Authorization

$R_{Mx} = hm_1 hm_2 hm_3 hm_4$
Decimal (Base 10) $dt \in \{0, 1, \cdots, 15\}$
$hm_i = dm_i$
$R_{Mx} = dm_1 dm_2 dm_3 dm_4$

Let us compute: $APadGen(R_{Tx}, R_{Mx})$
$= a_{dt_1} a_{dt_2} a_{dt_3} a_{dt_4} \| a_{dt_{1+16}} a_{dt_{2+16}} a_{dt_{3+16}} a_{dt_{4+16}} \|$
$a_{dm_1} a_{dm_2} a_{dm_3} a_{dm_4} \| a_{dm_{1+16}} a_{dm_{2+16}} a_{dm_{3+16}} a_{dm_{4+16}}$
$= hv_1 hv_2 hv_3 hv_4$ [where $hv \in \{0, 1, \cdots, 9, A, \cdots, F\}$]
$= dv_1 dv_2 dv_3 dv_4$ [where $dv \in \{0, 1, \cdots, 15\}$]

Let us compute:
$KPadGen(APadGen(R_{Tx}, R_{Mx}), R_{Tx})$
$= KPadGen(hv_1 hv_2 hv_3 hv_4, R_{Tx})$
$= k_{dv_1} k_{dv_2} k_{dv_3} k_{dv_4} \| k_{dv_{1+16}} k_{dv_{2+16}} k_{dv_{3+16}} k_{dv_{4+16}} \|$
$k_{dt_1} k_{dt_2} k_{dt_3} k_{dt_4} \| t_{dt_{1+16}} k_{dt_{2+16}} k_{dt_{3+16}} k_{dt_{4+16}}$
$= hp_1 hp_2 hp_3 hp_4$ [where $hp \in \{0, 1, \cdots, 9, A, \cdots, F\}$]

$\therefore PAD = hp_1 hp_2 hp_3 hp_4$ [Base 16]

4.2. Payment Phase

After the consumer has got the confirmation that product in question is genuine, he can decide to buy and pay for the product using his mRFID-reader.

Step 1: Consumer authorizes MO to pay for the product. mRFID-reader sends the EPC number, Pay Command, and Price.

Step 2: MO communicates with EPC-IS and sends EPC number, Buying Command, and Price to the EPC-IS

Step 3: EPC-IS sends the SP's bank account details to the MO. EPC-IS sends EPC number, Bank Name, and Bank Account No. to MO.

Step 4: MO transfers the money to the Bank Account and sends the Unique Money Transaction No. and Successful command to both the mRFID-reader and EPC-IS.

Step 5: EPC-IS after receiving the Unique Money Transaction No. and Successful command, it then flags the EPC number of the product as a sold item. After which the consumer can walk out of the store with the product.

Step 6: mRFID-reader can pay back the MO via monthly telephone bills. Our approach is very advantageous to both the MO and the SP to gain some profit in this transaction.

4.3. Consumer Privacy Protection

Killing the Tag: Once a tagged item is purchased by consumer, the clerk at the point-of-sale can use the KPwd and kill the tag permanently. But with this approach Alice cannot make use of the tag capabilities at her smart home environment, *e.g.* RFID enabled refrigerator or book shelf.

Locking the Tag: Based on the above-mentioned APwd and locking features available with UHF tags, we propose the following approach, where the tag need not be killed permanently. Once a tagged item is purchased by the consumer, the trustable clerk at the point-of-sale can retrieve the tag's access password from the EPC-IS and using this access password, the clerk can lock all the memory banks of the tag including the EPC memory bank. Consumer can download and store the EPC number of the item and its corresponding access password into mRFID-reader. This can be made possible via Bluetooth or Infra-Red (IR) communication between the mRFID-reader and the point-of-sale terminal. When the consumer arrives at home, he can use access password stored in the mRFID-reader to unlock the tag. With this proposed approach, an adversary with a mRFID-reader can no longer get any information (even the EPC number is not emitted by the tag) from the RFID tagged items possessed by the consumer, as all the memory banks of the tags are locked and the adversary does not have the access passwords.

5. Security Analysis

5.1 Tag & mRFID-reader Mutual Authentication

Tag's access password never exposed: One of the main components of our proposed scheme is PadGen(.): *Pad Generation Function*. In short, this function takes two 16-bit random numbers each, from the Tag (R_{Tx}) and the Manufacturer (R_{Mx}), and utilizes the *Access* (APwd) and *Kill* (KPwd) *Passwords*, to generate two 16-bit Pads (PAD_x). Since ONLY the tag and the manufacturer know (APwd) and (KPwd), just by sharing the random numbers among themselves (via mRFID-reader), both the tag and the manufacturer can generate the same pads. Later these two pads are in-turn used to cover-code (XOR) the two 16-bit (APwd) chunks $(APwd_M,\ APwd_L)$. This approach prevents the major drawback of the one-way reader-to-tag authentication scheme proposed by EPCglobal. Therefore we can fend off threats like exposed tag's APwd, malicious mRFID-readers, and cloned fake tags. Our proposed scheme involves the EPC-IS to authenticate the tag rather than giving away the true access password to every mRFID-reader.

Light-Weight Tag-Reader Mutual Authentication: Our scheme does not use any special cryptographic functions,it utilizes only those features that exist the EPCglobal C-1 Gen-2 UHF RFID Protocol standard [5] such as, the tag has the capability to compute XOR operations, generate random numbers, temporarily store random numbers and fetch the APwd and KPwd embedded within its Reserved Memory bank. Therefore our proposed scheme is light weight and requires minor changes to the EPCglobal Class 1 Gen 2 UHF RFID Protocol standard.

5.2. mRFID-reader Secure & Anonymous Communication with Genuine SP's EPC-IS

In our proposed framework we extend our trust in MO to secure and provide privacy protection for consumers. MO takes responsibility on behalf of mRFID-reader to select, identify, and authenticate genuine Service Provider's ECP-IS. MO behaving like a Trusted Proxy processes the request on behalf of the mRFID-reader, greatly reducing its communication and computational and also providing consumer privacy protection.

5.3. mRFID-reader (Consumer) Authorization

Based on the consumer's current privileges, MO can create a Anonymous digital Credential/Certificate $Anony_{Cred}$. In simple terms an anonymous credential does not contain the true identity (*e.g.* Full Name) of the consumer. It only contains some common and general information about the consumer, such as his age, and membership privileges. $Anony_{Cred}$ is digitally signed by MO. $Anony_{Cred}$ will be verified by the Service Provider's EPC-IS to authorize the consumer. Konidala *et al.* [13] describes the generation of Anonymous Capability/Credential for ubiquitous computing environment. $Anony_{Cred}$ is different from the digital certificates issued by the Certificate Authority (CA). Digital Certificates issued by the CA contain the true identity of the consumer, and also the public-key of the consumer and the CA.

6. Conclusion

In this paper we introduced a new application for RFID called the mRFID technology, which is being considered as a viable option to assist people in their daily lives. mRFID technology enables mobile phones/PDAs to scan and read RFID tags attached to consumer goods. In this paper we described the various security requirements and security threats that must be considered while deploying mRFID technology. We also proposed a security framework that allows a consumer to distinguish genuine products from fake products by authenticating the RFID tag attached to that product, consumer authorization, secure and anonymous communication with genuine information servers in order to download information about a particular RFID tagged item, blocking malicious mRIFD-readers from snooping on the RFID tagged items in our possession, and simple and secure mRFID payment scheme.

Acknowledgement

This work was supported by the IT R&D program of MIC/TTA. [2008-P1-05-08I92, Mobile and next generation RFID technology standards development]

References

[1] Patrick J. Sweeney II, "RFID for Dummies", Wiley Publishing,Inc. ISBN: 0-7645-7910-X, 2005.

[2] VeriSign, "The EPCglobal Network: Enhancing the Supply Chain", White Paper 2005, http://www.verisign.com/stellent/groups/public/documents/white_paper/002109.pdf

[3] EPCglobal Web site, 2005, http://www.EPCglobalinc.org

[4] EPCglobal Specification, "The EPCglobal Architecture Framework", http://www.epcglobalinc.org/standards/

[5] EPCglobal Ratified Standard, "EPC^{TM} Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz - 960MHz Version 1.0.9", http://www.epcglobalinc.org/standards/

[6] Divyan M. Konidala and Kwangjo Kim, "Mobile RFID Applications and Security Challenges", The 9th Annual International Conference on Information Security and Cryptology, ICISC 2006, LNCS 4296, pp.194-205, 2006.

[7] Ari Juels (2005), "RFID Security and Privacy: A Research Survey", RSA Laboratories.

[8] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita, "Efficient Hash-Chain Based RFID Privacy Protection Scheme", Proceedings of International Conference on Ubiquitous Computing, Workshop Privacy, September 2004.

[9] Gildas Avoine and Philippe Oechslin, "A Scalable and Provably Secure Hash-Based RFID Protocol", Proceedings of Workshop on Pervasive Computing and Communications Security PerSec'05, March 2005.

[10] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags", Proceedings of 2nd Workshop on RFID Security, July 2006.

[11] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Rib agorda, "M^2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags", Proceedings of Ubiquitous Intelligence and Computing UIC'06, LNCS 4159, pp. 912-923, 2006.

[12] Tieyan Li and Guilin Wang, "Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols", Proceedings of IFIP SEC 2007, May 2007.

[13] Divyan M. Konidala, Dang N. Duc and Kwangjo Kim, "A Capability-based Privacy-preserving Scheme for Pervasive Computing Environments", Proceedings of IEEE PerSec2005, pp.136-140, Mar. 2005.