Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding, 12-15 July 2009

SURVEY AND REMEDY OF THE TECHNOLOGIES USED FOR RFID TAGS AGAINST COUNTERFEITING

ALBERT B. JENG[1], LI-CHUNG CHANG[2], TE-EN WEI[2]

[1]Department of Computer Science and Information Engineering, Jinwen University of Science and Technology/ National Taiwan University of Science and Technology, Taipei, Taiwan
[2]Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan
E-MAIL: albertjeng@hotmail.com , lichung@mail.ntust.edu.tw, iverson2100@hotmail.com

Abstract:

RFID tags such as EPC tags have been used in some commercial sectors such as the pharmaceutical industry as an anti-counterfeiting tool. RFID tags are a powerful mechanism for object identification, and can facilitate the compilation of detailed object histories and pedigrees. Since RFID tags communicate with the reader through open air in an automated, wireless manner, they are poor authenticators. Furthermore, they have a small microchip on board that offer functionality that can be used for security purposes. This chip functionality makes it possible to verify the authenticity of a product and hence to detect and prevent counterfeiting. In order to be successful for these security purposes, RFID tags have to be resistant against many attacks, in particular against cloning of the tag. Therefore, RFID tags are vulnerable to elementary cloning and counterfeiting attacks. In this paper, we survey and remedy the technologies used for RFID tags against counterfeiting. In the first section, we present an overview of the RFID tags counterfeiting issue. In the second section, we survey the existing methods which investigate how an RFID-tag can be made unclonable. In the third section, we compare and contrast the pros and cons of those existing methods and also identify the discrepancy areas which require further enhancement. In the fourth section, we propose some design principles and guidelines for improvement of the existing methods. Finally, we draw a conclusion and suggest further research direction in this field.

Key words:

RFID; EPC; Anti-counterfeiting; Authentication; Clone

1. Introduction

Radio Frequency Identification (RFID) technology [1][2] has been used for over half a century since World War II. RFID was used in anti-counterfeiting area before it was used in retailers, the logistics and the global supply chains applications. In 2003, it was suggested using the RFID system plus Electronic Product Code (EPC) to prevent fake drugs by the U.S. Food and Drug Administration (FDA) [3][4], and in 2004, Pfizer and Purdue Pharma companies used RFID tag which attached to the item to prevent fake drugs of Viagra and OxyContin. In recent years, several technologies used for RFID tags against counterfeiting have been proposed. RFID consists of readers and tags. There is an antenna in the reader that is used to connect tags, and the antenna of the tag itself is connected to the micro-chip that was embedded into the tag. Due to the advancement of the technologies, the size of RFID tag becomes smaller, its speed becomes faster, its price becomes cheaper, and it can be used easily. The RFID antenna can also be printed on the product or embedded in them.

Generally speaking, RFID tags can used for identification as well as for anti-counterfeiting purpose. The attack which we hear most frequently is duplicating. That means the attacker can acquire RIFD tag easily and can study it and read the contents of its memory, and make another new tag with the same memory content of the valid tag. If a duplicated tag is used in the goods, the reader will not be able to discover that it is a fake tag. Therefore, our paper will survey anti-counterfeit technologies used on the RFID tags with special focus on three papers (i.e., Juels' strengthening EPC tags against cloning [5], Duc et al.'s enhancing EPC tags against Traceability and cloning [6], and Pim Tuyls and Lejla Batina's RFID tags for anti-counterfeiting [7]). However, these papers seem to be too academic such that they may not too suitable for practical applications. In the second section, we survey the existing methods which investigate how an RFID-tag can be made unclonable. In the third section, we compare and contrast the pros and cons of those existing methods and also identify the discrepancy areas which require further enhancement. In the fourth section, we propose some

978-1-4244-3703-0/09/$25.00 ©2009 IEEE

design principles and guidelines for improvement of the existing methods. Finally, we draw a conclusion and suggest further research direction in this field.

2. Overview of Existing Schemes for Anti-counterfeiting RFID tag

Electronic Product Code (EPC) is a global automated universal identification system service. EPC Class-1 Generation 2 UHF standard is the most commonly used. It is mainly the definition of the RFID system in the bandwidth of 860 MHz-960 MHz actual and logical requirements. When the Gen 2 standard was proposed, a number of security and privacy considerations was proposed gradually as well [8]. Juels first proposed a strengthen anti-counterfeiting tag that can be used against cloning attack [5]. However, Duc et al. think Juels' methods does not take into account the threat of information leakage and privacy issues, so they put forward another anti-counterfeiting mechanism to solve this problem [6]. In this section, we will also introduce an additional Pim Tuyls and Lejla Batina proposed PUF-Certificate-Identify-based Identification (PUF-Cert-IBI) mechanism [7]. It is a combination of Physical Unclonable Functions (PUF) and the microchip, in order to achieve an anti-counterfeit tag. The detail methods of these three papers are described as follows:

2.1. Basic setting

T represents RFID tags, R is the RFID reader, and S is the backend server, N is the number of tags, and finally A: means action at entity A, A → B is communication from A to B, and A ↔ B is interaction between A and B.

2.2. Basic Anti-counterfeiting EPC Tag

In this section, we will introduce a tag to identify the basis of the EPC system, and introduced at the beginning before a few important settings (i, PIN-test(K), b, K_i): (In a system with N tags)
i: The integer i (with 1 to N) denote the unique index of an EPC tag.
PIN-test(K): Let us denote by PIN-test(K) an EPC-tag (meta-)command that causes a tag to output a bit-response b.
K_i: Let K_i denote the currently valid kill PIN for tag T_i.
The authentication between reader and tag as follow:
1. T: $T \leftarrow T_i$
2. T→R: T
3. R: if $T = T_x$ for some $1 <= x <= N$ then $i \leftarrow x$
else output "unknown tag" and halt
4. R→T: PIN-test(K_i)
5. T→R: b
6. R: if b = 1 then output "invalid"
else output "valid"

2.3. Juels Anti-counterfeiting Tag

Due to the fact that the anti-counterfeiting mechanism of EPC tags is too simple with low security, so Juels proposed two anti-counterfeiting methods, namely, the basic and the enhanced anti-counterfeiting tag. The basic method emphasis on increasing the complexity of cloning the legitimate tag through eavesdropping by sending a set of q-1spurious *Kill* PINs plus a correct *Kill* PIN, which is randomly placed in this sequence of q *Kill* PIN commands to mislead the attacker. While the strengthen method focuses on the design of an extra *access* PIN command. It uses this new access PIN command to add one more layer of "authentication" to the basic anti-counterfeiting mechanism in order to achieve the overall "anti-cloning" protection. Below is a detailed description of these two RFID tags anti-counterfeiting methods and their operation methods.

2.3.1. Basic Anti-counterfeiting Tag

We are also beginning to introduce a few important settings (i, q, j, P_i, GeneratePINSet, PIN-test(P) , b, M): (In a system with N tags)
i: The integer i (with 1 to N) denote the unique index of an EPC tag.
q: The number of invalid Kill PINS. (error: q-1, correct: 1)
j: The position of correct kill PIN.
P_i: The positions of all kill PIN commands
GeneratePINSet: The function generates a set of q-1spurious PINs uniformly at random (without duplication).
PIN-test(P): Let us denote by PIN-test(P) an EPC-tag (meta-)command that causes a tag to output a bit-response b.
M: Result.
The authentication between reader and tag as follow:
1. T: $T \leftarrow T_i$
2. T→R: T
3. R: if $T = T_x$ for some $1 <= x <= N$ then $i \leftarrow x$
else output "unknown tag" and halt

4. R: (j,{ $P_i^{(1)}$, $P_i^{(2)}$,…, $P_i^{(q)}$,})←GeneratePINSet(i)[q];
M←"valid"
for n=1 to q do
5. R→T: PIN-test($P_i^{(n)}$)
6. T→R: b
7. R: if b = 1 and n != j then M←"invalid";
if b = 0 and n = j then M←"invalid"
8. R: output M;

2.3.2. Enhanced Anti-counterfeiting Tag

This section describes how to use the new access PIN command for identification system to increase more than one mechanism in order to achieve security protection, We begin to introduce a few important settings (i, A_i, K_i): (In a system with N tags)
i: The integer i (with 1 to N) denote the unique index of an EPC tag.
A_i: Let A_i denote the currently valid access PIN for tag T_i.
K_i: Let K_i denote the currently valid kill PIN for tag T_i.
The authentication between reader and tag as follow:
1. T: T←T_i
2. T→R: T
3. R: if T＝T_x for some 1 <= x <= N then i←x, A←A_i
else output "unknown tag" and halt
4. R→T: A
5. T: if A=A_i then K←K_i
else K← ϕ
6. T→R: K
7. R: if K = K_i then output "valid"
else output "invalid"

2.4. Duc Anti-counterfeiting Tag

In this section, we will introduce another method by Duc et al. Duc et al. thought Juels' methods did not take into account the threat of information leakage and the privacy issues, such as the threat of an eavesdropper located between the reader and the tag to intercet the communication between them. So they put forward another anti-counterfeiting mechanism to solve this problem. Because the EPC Gen 2 tag supports both the Pseudo-Random Generation (PRNG) and Cyclic Redundancy Code (CRC) functions to do computing on the chip. Therefore, this method uses these two operation functions to achieve anti-counterfeiting for the EPC tags.

2.4.1. The proposed method

Before introducing this method in a number of settings is necessary to know (EPC, f(.), CRC(.), K_i, PIN, r, M_1, M_2): (In a system with N tags)
i: The integer i (with 1 to N) denote the unique index of an EPC tag.
EPC: Electronic product code.
f(.): PRNG function.
CRC(.): CRC function.
K_i: Session Key for i-th Session.
PIN: Long-term Secret Shared between T and S.
r: A Pseudo-random Number
M_1: Message1
M_2: Message2
The authentication between reader and tag as follow:
1. R→T: Query request.
2. T: Compute M1 = CRC(EPC || r)⊕K_i and
C = CRC(M1⊕r) where r is a nonce.
3. T→R: M_1, C, r.
4. R→S: R and S authenticate each other and
then R forwards M_1, C and r to S.
5. S: For each tuple (EPC, K_i) in backend server's database, S : verifies that M_1⊕K_i equals CRC(EPC
|| r) and C = CRC(M_1⊕ r). If no tuple (EPC, K_i) is found, the tag is rejected. Otherwise, we assume that a tuple (EPC, K_i) is passed the check by S .
6. S→R: If R desires to perform read/write operations to T 's
memory, it requests an authentication token M_2 from S where M_2 = CRC(EPC || PIN || r)⊕K_i.
7. R→T: M_2
8. T: T receives M_2 and computes its own version of M_2 based on its knowledge (of PIN, r, EPC and K_i). If two are not matched, T rejects R's request and accepts otherwise.

2.5. Pim Tuyls and Lejla Batina Anti-counterfeiting Tag

In this section, we will introduce Pim Tuyls and Lejla Batina proposed PUF-Certificate-Identify-based Identification Scheme (PUF-Cert-IBI). It uses a combination of Physical Unclonable Functions (PUF) and the microchip in order to achieve an anti-counterfeit tag. Before introducing this method, a brief on PUF is given below.

2.5.1. Physical Unclonable Functions

Physical Unclonable Functions (PUF) is a function that maps challenge to response which is implemented in a physical object, just like Figure 1.

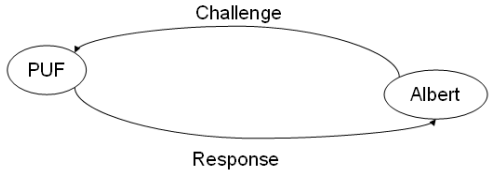

Figure 1. Physical Unclonable Functions

Please refer to [7] for a definition of PUF. However an integrated PUF have to satisfy the following properties:

1. The PUF is inseparably bound to a chip which means that any attempt to remove the PUF from the chip leads to the destruction of the PUF and the chip.
2. It is impossible to tamper with the communication between the chip and the PUF.
3. The output of the PUF is inaccessible to an attacker.

2.5.2. Key Extraction

Since the PUF-Certificate-Identify-based Identification of the method is divided into two parts to the operation, one is Enrolment phase, the other is Verification phase, and we first make a brief introduction.

1. Enrolment phase：The PUF is subjected to a challenge C and the response X is measured. Then a random key S_x and helper data W is computed by solving G(X,W) = S_x for W. G(.,.)： $R^n \times W$ function.
2. Verification phase：When the PUF is inserted into the reader the PUF's identity is sent to the verifier. The verifier chooses a random challenge C from his database and sends it to the PUF together with the corresponding helper data W. Then the PUF is subjected to the challenge C and its response Y is measured. A key S_y is then computed as S_y = G(Y,W).

2.5.3. PUF-Certificate-Identify-based Identification

Now, we will introduce the PUF-Cert-IBI scheme, and begin to introduce a few important settings:

SI = (K_g, P, V)： A standard identification scheme (SI-scheme) (K_g denotes the key generation algorithm, and P, V denote the interactive protocols run by the prover and verifier respectively.)

SS = (SK_g, Sign, V_f)： A standard signature scheme (SS-scheme) (SK_g denoting the key generation algorithm, Sign denoting the signing algorithm and V_f the verification algorithm run by a verifier.)

I： Assigning to each tag an identity (EPC code or serial number of product)

Identify-based Identification scheme (MK_g, UK_g, P', V')：

MK_g denotes master key generation algorithm, and UK_g denotes user key generation algorithm, P' and V' denote the interactive protocols run by the prover and verifier respectively. Then we will introduce PUF-Cert-IBI, this method is referred to as before. (Enrolment and Verification)

Enrolment Phase：

The issuer uses SK_g as the master key generation algorithm MK_g. This means that the master key msk is used for generating signatures and the corresponding public key mpk for verification of the signatures. The user key generation algorithm UK_g consists of the following steps. For each RFID tag, having identity I, the issuer then creates a public-secret key pair (pk, sk) using the algorithm K_g. The couple (pk, sk) is the public-secret key pair for the SI-scheme. The issuer runs the following protocol with the tags:

1. It requests the tag to challenge its PUF with a challenge c and to measure the response x(c).
2. The Tag sends x(c) to the issuer.
3. Based on the knowledge of x(c) and sk, the issuer determines the helper data w such that sk = G(x,w).
4. The helper data w are written into the ROM (EEPROM) of the tag.
5. Finally, the issuer creates the following certification that is also stored in the ROM of the tag. (Cert←(pk,Sign(msk,pk||I)), usk←(PUF,Cert))

Verification Phase：

In the authentication phase, the tag (in the role of the prover) runs the following steps with a verifier:

1. T runs the protocol P':
   a) It challenges the PUF with c, measures the response y(c) and computes sk←G((y(c), w).
   b) Initialization of the prover protocol P of the SI scheme with sk.
   c) It includes the certificate Cert in the first step of the algorithm P.
2. Then R uses (mpk, I) as input for the verification algorithm V':
   a) When R receives the Cert from the tag, it first verifies Cert by running V_f(mpk, pk || I, Sign(msk, pk || I)).
   b) If the certificate Cert is invalid the protocol is aborted.

c) If Cert is valid, the verifier initializes V with pk and runs it.
d) If V accepts, then R accepts. ◦

3. Comparison of the technologies for RFID Tags against counterfeiting

In this chapter we focus on the comparison of the three previously methods for RFID tags against counterfeiting, and enumerate the pros and cons of them. We will also point out a number of deficiencies which require further improvement. We will use the threat classification presented in [8] for the basis of comparison and discussion..

Duc in 2006 pointed out some problems about Juels' protocols, and described a number of attacks and threats which might be encountered in Juels methods. Among the top of these threats, eavesdropping and information leakage were considered most important. Duc thought Juels' methods did not take into account the threat of information leakage and privacy issues during the communication between the tags and the reader. However, Duc's method is neither complete nor perfect, because the theoretical foundation of their methods is the same. Consequently they are suffering from the same kind of security problems which are inherent in their design.

In 2006, Pim Tuyls and Lejla Batina proposed a PUF-Cert-IBI scheme which uses the PUF function of the microchip in the tag to achieve the effect of anti-counterfeiting. This method not only achieves the goal of anti-cloning in the RFID tags but also counters all the threats and attacks on counterfeiting and duplications via using a sophisticate bilateral authentication between the tags and the reader. Although the issuer of the tags are considered as a trusted party, it is possible this method is subject to attack during the tags fabrication and it also requires a large amount of computing resource to support this method. All these are potential problems which can not be neglected.

Now, we describe some existing anti-counterfeiting tag shortcomings, and list their pros and cons in Table 1. :

1. RFID tags communicate with the reader through open air in an automated, wireless manner, they are poor authenticators, because they communicate with each other that is easily eavesdropped. Because we did not know whether there is a third party that eavesdrops the secret of their communication. An attacker can obtain the correct PINs or other relevant information by eavesdropping. When an attacker owns these information, he/she will cause a great threat to the tags such as Replay attacks, Sniffing, and Denial of service. These attacks can cause great damage to information leakage and privacy violation of the tags through eavesdropping.
2. Item 1 addresses only the security issue between the tags and reader radio frequency communications in the open air regarding on anti-counterfeiting. We will also

Table. 1 Pros and cons of anti-counterfeiting RFID tag schemes

	Juels	Duc	Pim Tuyls and Lejla Batina
pros	■ In line with the EPC Gen 2 standards ■ Prevent forged tags ■ Prevent clone attack ■ Two-way authentication	■ Proposed improvements and some shortcomings that Juels have.	■ Unlike Juels' and Duc's scheme, focus on the chip of tag for anti-counterfeiting.
cons	■ Eeavesdropping ■ Spoofing ■ Tampering with data ■ Sniffing ■ Replay attacks ■ Repudiation ■ Denial of service ■ Memory duplication ■ Extract authentication keys ■ Bypass authentication process ■ Selective amnesia ■ Database breaches ■ Reverse engineering ■ Active attacks	■ Although the solution to the eavesdropping attack, but basically the structure is the same with Juels, even if the increased recognition of the complexity.	■ In production of tags, the eavesdropping attacks may happen that lead to pose as legitimate tags which attack ■ Excessive use of resources to complete this mechanism

need to talk about security problems in tag memory duplication. In Juels and Duc schemes, they started with the secure communication issues between the tags and the reader to address the cloning problem. However, they ignored the problems and consequences of memory and secure logic duplication of the tags. If tag memory can be duplicated, then the tags could be subject to fraud or data modification attacks. Although the production of tags are executed by trusted manufacturers, however during the production process it is possible that the tags are attacked by eavesdropping, database breaches, and other intentionally attacks. Therefore, even if they were protected by sophisticated and secure authentication protocols for anti-counterfeiting, then if there is no way to prevent memory of tag being copied, it is futile.

3. If an adversary can breach the database containing the PINs and other authentication information of the tags, then he/she may be able to duplicate a tag perfectly. Although in a RFID architecture with anti-counterfeiting mechanism, even if the legitimate reader and legitimate tags are working perfectly in performing authentication and anti-counterfeiting work, it is possible for an attacker to learn the security logic of the overall protection mechanism and the secret transmitted between the reader and the tags if the database of the backend sever was under attack and the important information was compromised. At this point, if an attacker wants to fake an identical tag to deceive a legitimate reader, or to make use of the learned security logic to launch a fraudulent or denial-of-service attack will be relatively easy which is a very big threat to the overall mechanism.

4 Proposed Remedy Principle and Suggestion

Although RFID tags are more focused on the security issue of anti-counterfeiting, but there are many possible threats or attacks can cause information leakage or other security damages to the tags. These three papers are proposed to solve RFID tags anti-counterfeiting problems, however they failed to address other threats and attacks germane to the certification and production problems of tags. Therefore, after analyzing the existing technologies for RFID tags against counterfeiting, we propose the following necessary principles and guidelines for ramification:

1. The communication content between the reader and tags must be as simple as possible, and it is more appropriate that the security critical information in the anti-counterfeiting RFID tag are irregular and unpredictable.
2. We need an RFID tag anti-counterfeiting mechanism which is suitable for various applications. The production of the tags must comply to the international recognized IT security product evaluation criteria (e.g., The Common Criteria and FIPS 140-2 Cryptographic Module Security Requirements) and must pass the security evaluation performed by a trusted, accredited evaluation facility..
3. The above three methods require a backend server RFID authentication database, Thus, it is necessary to protect the integrity of this database.
4. In general, we concur with the PUF-Certificate-Identify-based Identification (PUF-Cert-IBI) proposed by Pim Tuyls and Lejla Batina. However, it is necessary to improve the problem of excessive use of resources..

5 Conclusions

In order to achieve the objectives of the various securities, RIFD tags need to resist many types of attacks, especially the tag cloning and forgery attacks. In this paper, we survey and remedy three technologies used for RFID tags against counterfeiting.

We believe that the PUF-Cert-IBI proposed by Pim Tuyls and Lejla Batina is the best way to prevent the counterfeited RFID tag. However, because their method used too much computing resources to implement this scheme, it is necessary to cut down the overhead with further improvement and refinement.

References

[1] R. Weinstein, “RFID: A technical overview and its application to the enterprise,” IT Professional, Vol. 7, No. 3, pp.27-33, 2005

[2] K. Finkenzeller, RFID Handbook: Fundamentals and Application in Contactless Smart cards and Identification 2nd ed., John Wiley & Sons, UK, 2003.

[3] Editors, FDA Will Begin Enforcing Anti-Counterfeiting Law In December, in Medical News Today. 2006.

[4] United States Food and Drug Administration, COMPLIANCE POLICY GUIDE 160.900 Prescription Drug Marketing Act – Pedigree Requirements under 21 CFR Part 203. 2006.

[5] Juels, A. Strengthening EPC Tags Against Cloning. in

ACM Workshop on Wireless Security (WiSe). 2005.

[6] Duc, D.N., et al. Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning. in The 2006 Symposium on Cryptography and Information Security. 2006. Hiroshima, Japan.

[7] P. Tuyls and L. Batina. RFID-tags for Anti-Counterfeiting. In D. Pointcheval, editor, Topics in Cryptology - CT-RSA 2006, LNCS, San Jose, USA, February 13-17 2006. Springer Verlag.

[8] S.H. Choi and C.H. Poon, An RFID-based Anti-counterfeiting System, IAENG International Journal of Computer Science, 35:1, IJCS_35_1_12, 19 Feb. 2008.