Sensors & Transducers, Vol. 176, Issue 8, August 2014, pp. 196-202

Sensors & Transducers

http://www.sensorsportal.com

Authentication Test-Based the RFID Authentication Protocol with Security Analysis

[1] Minghui Wang, [2] Junhua Pan

[1] School of information engineering, YanCheng Institute of Technology,
No. 9, Xiwang Avenue, Yancheng, 224051, China
[2] Library, YanCheng Institute of Technology, No.9 Xiwang Avenue, Yancheng, 224051, China
[1] Tel.: 0515-88302735
[1] E-mail: wmh@ycit.edu.cn

Received: 21 May 20014 /Accepted: 31 July 2014 /Published: 31 August 2014

Abstract: To the problem of many recently proposed RFID authentication protocol was soon find security holes, we analyzed the main reason, which is that protocol design is not rigorous, and the correctness of the protocol cannot be guaranteed. To this end, authentication test method was adopted in the process of the formal analysis and strict proof to the proposed RFID protocol in this paper. Authentication Test is a new type of analysis and design method of security protocols based on Strand space model, and it can be used for most types of the security protocols. After analysis the security, the proposed protocol can meet the RFID security demand: information confidentiality, data integrity and identity authentication. *Copyright © 2014 IFSA Publishing, S. L.*

Keywords: Radio frequency identification, Authentication Tests, Protocol analysis, Key, Strand space.

1. Introduction

RFID (Radio Frequency Identification) technology has been widely applied in the field of logistics and supply management, manufacturing and assembly, networking, smart anti-theft. It is a non-contact automatic identification technology that uses radio signals to automatically identify the target and access to relevant data, making the system without any physical contact can be completed automatically identifies the specific target object. Its unique non-contact transmission make it a wide range of applications, but this feature is also brought some problems to the security of the system. The RFID system communication channel is divided into the cable channel in the back-end database and reader and the radio channel in reader and label by the researchers two shown in Fig. 1. Typically researchers believe that the cable channel portion having a relatively strong security to existing communication device is able to meet the security of wired communication, wireless RF channel is invulnerable to outside attacks, and thus pose a threat to the security of the entire RFID system.

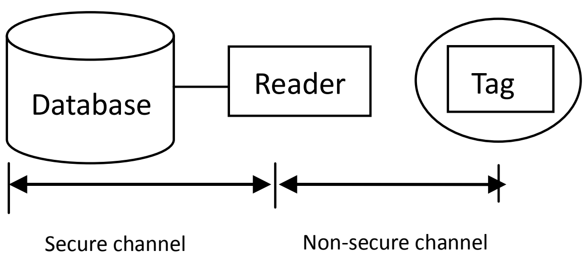

Fig. 1. The RFID system.

Radio frequency identification (RFID), based on the MIT Auto-ID project [1], is a technology that uses wireless transmission to identify an object. RFID technology has many advantages, such as without physical contact, quick reading, long recognition distance, obstacle-free and so on. But its application may have challenges to the security and privacy of individuals or organizations. For the limit of low cost RFID tag with low resources: low computing power and small memory size, Thus, it is very hard to apply existing and excellent security technologies that assumes very high computing power and large memory size to RFID tag, so that the security technologies of low-cost RFID systems urgently are developed.

1.1. Notations

The notations used for the entities and computational operations to simplify the description are as follows (Table 1).

Table 1. Node Parameters.

Notations	Meaning
T	Tag of RFID
R	Reader of RFID
D	Backend Server of RFID system
ID_D,ID_T	Identity of Server and Tag
PRNG	Random number generator
N_D,N_T	Random number generated by D and T
KP_D,KP_T	Public key of D and T
KE_D,KE_T	Private key of D and T
Query	Query request generated by R
H( )	one-way hash function, H: $\{0, 1\}^* \rightarrow \{0, 1\}l$
$\sum$	Strand Spaces
+M,-M	The Sent and received messages
$\Rightarrow$	The Transformed edge or Transforming edge
$\{M\}_{KP}$	Encryption to M with Public key

1.2. System Several Threats

These are attacks which are feasible just by observing and manipulating communications between readers and tags.

Eavesdropping: In the case of a third party does not know, the illegal user can listen in secret communication between reader and tag. In wireless communication, Eavesdropping is a common problem. An effective way to solve this problem is that both sides of each pass communication produce changing values. Therefore, the attacker cannot access to significant values even if he acquires data.

Traffic analysis: It is the process of intercepting and examining messages in order to deduce valuable information from patterns in communication between the reader and tag. In order to prevent an attacker from using this method to attack, we need to add a random number in the reader and tag communications data.

Replay attack: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it. Therefore, the random value, participated in the communication process, is generated by the common reader and tag.

Tracking attack: Through repeated analysis and comparison of multiple outputs between reader and tag, an attacker gets into a constant value (In some cases, the attacker can even get the tag's ID). In this way, the attacker can track the user's location information and even get more user privacy, which is one of the most serious privacy problems of the RFID systems. Application of the random number or timestamp is an effective way to solve the problem.

1.3. Authentication and Encryption

Authentication, which addresses the above-mentioned security threat, i.e. preventing the cloning or impersonation of legitimate tags, is probably the most explored topic in lightweight cryptography. Efficient authentication solutions for RFIDs are gradually emerging, even for the most constrained settings. To take into account the strong limitation of computing resources in the tags (3000 GE, is often considered as the upper limit for the area reserved to the implementation of security in low-cost RFID tags), dedicated lightweight block ciphers [2, 3, 4] have been developed [5].

Privacy is a hobbyhorse in media coverage of RFID. To some extent, it has overshadowed the equally significant problem of authentication. Loosely speaking, RFID privacy concerns the problem of misbehaving readers harvesting information from well-behaving tags. RFID authentication, on the other hand, concerns the problem of well-behaving readers harvesting information from misbehaving tags, particularly counterfeit ones.

RFID schemes cannot use computationally intensive cryptographic algorithms for privacy and security because tight tag cost requirements make tag-side resources (such as processing power and storage) scarce: The volume of data stored in a tag should be minimized because of the limited size of tag memory; Tag-side computations should be minimized because of the very limited power available to a tag; The volume of data that each tag can transmit per second is limited by the bandwidth available for RFID tags [6].

In Section 2, we detailed analysis of the research background and some of the existing domestic and international research, and the relationship and distinction of this work with these studies. Section 3 describes in detail the structure of the proposed RFID authentication protocol and implementation process. In Section 4, brief introduction to the basic concepts of the string space and certification testing (AT) and certification goals formal representation. In Section 5, we give a detailed analysis and security proof of the proposed RFID security by the strand space theory and certification testing method. Finally, a brief summary of the significance and role of the certification test protocol analysis and the idea of the next step are proposed.

2. Related Work

RFID system is widely used; many scholars have put a lot of effort in this regard, but due to different assumptions of each scholar on the ability of RFID systems, RFID-based authentication protocol vary widely. Currently, researchers have proposed protocol is divided into two categories: one is the HASH-based authentication protocol, and the other is based on the EPC Gen2 [7] standard protocol.

The Hash-Lock based RFID protocol, as defined by Weis et al. [8], is a scheme which involves locking a tag using a one-way hash function. A locked tag uses the hash of a random key as its metaID=Hash (key). When locked, a tag responds to all queries with its value of metaID. However, the scheme allows a tag to be tracked because the same metaID is used repeatedly [9].

The Random Hash-Lock [10] based RFID protocol is a modified form of the Hash-Lock Protocol. In addition to the Hash function, the label is also embedded in a pseudo-random number generator. The protocol utilizes the random numbers to solve the label positioning privacy issues. But a pseudo-random number generator is integrated in the Tags, the more difficult to achieve in the case of low-cost and limited computing capabilities. The Tag is still not able to respond to retransmission and spoofing attacks.

In the Hash-Chain protocol [11], an RFID privacy protection scheme was proposed with providing indistinguishability and back-ward intractability. The protocol utilizes the Tags to meet each update to identify indistinguishability and forward security. However, the hash chain protocol is a one-way authentication protocol only on the card for authentication, which is vulnerable to retransmission and spoofing attacks. Two different hash function operation increase the burden on the Tags.

Some researchers have proposed based on EPC Gen2 standard RFID authentication protocol [12-14]. Unfortunately, other researchers have found that either there is security vulnerability in the existing protocol, or did not give security.

Most RFID tags have several resource limitations, e.g. memory, computational power, etc. that prevent the use of public-key cryptography. On the other hand, strong privacy is a real need that must be achieved, and public-key cryptography seems to be the best way to tackle the problem. Lots of efforts have been devoted to the analysis of public-key protocols and their adaptation to RFID systems [15, 16].

An analysis of the security of cryptographic protocols is a very difficult issue, because an attacker can make different attempts repeatedly, and he can collect the messages sent by the communicating parties, to analyze the message, and then change the content of the message tampering, or the order of transmission of the message. However, in the design of cryptographic protocols, the behaviors of the communicating parties for effective control, and then identify the attacker's unreasonable action. At present, most secure routing protocol analysis of non-formal methods are based on subjective analysis or simulation, the analysis is not precise enough and strict, resulting in many of the original claim that "safe" routing protocols were later found security vulnerabilities. In recent years, formal analysis methods began to be used in the analysis of the secure routing protocol.

In order to achieve the safety goals of security protocols, researchers proposed a number of different methods. Some researchers use BAN logic [17] to formally prove some security protocols. Subsequently, it was discovered that BAN Logic is only suitable for communication bodies are credible, cannot guarantee for the participation of the untrusted party. Guttman, etc. proposed an Authentication Test method [18, 19] Based on Strand Space model [20], and gives an example of how to design the method based the Authentication test the security of e-commerce transactions Protocol (ATSPECT) [21].

In this paper, a method of Authentication tests is adopted to finish the formal analysis and the safety proof of the new proposed RFID protocol, effectively ensure the security of the proposed protocol.

3. The Proposed RFID Authentication Protocol

3.1. The Design of Protocol

In the process of design and safety analysis of the protocol we introduced the concept of Strand space and Authentication Tests. Its main symbols are described below, and other unspecified symbols are consistent with the definition in the article [20].

After analysis of the loopholes in the existing RFID authentication protocol other researchers found, in this article, we introduced the concept of public key cryptography to RFID authentication protocol, public key-based RFID authentication protocol is proposed. The protocol Fig. 2 shown as follows:

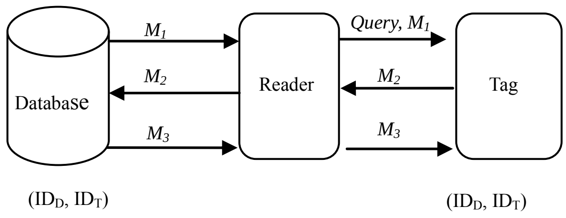

Fig. 2. The structure of RFID protocol.

3.2. The Authentication Phase

After system initialization, database D and tags T have each other's public key, D and T have each other's ID (the ID of the Tag said IDT; ID of the database known as IDD).Via cable transmission and clock settings, we can ensure that the database frequency of sending messages to the reader and the reader RF signals emitted by the same frequency.

D→R→T: By the reader R, Database D sends a certification request message Query and M1 to Tag T.

T→R→D: The Tag T generates a random number NT, calculates the value of M2 ($M_2 = \{N_T, N_D, ID_T\}_{KP_D}, h(N_T, ID_T)$), send M2 to D through R.

D→R→T: First, with their own private key Database D decrypts $\{N_T, N_D, ID_T\}_{KP_D}$, D will get the values of N_T, N_D, ID_T. Second, after the IDT values obtained, D can be authenticated T. The role of $h(N_T, ID_T)$ is signature of the data passed by T. Third, D calculated the value of M3 ($M_3=h(N_T, N_D, ID_D, ID_T)$), and send it to T.

T: After the receiving the data M3, with his own parameters N_T, N_D, ID_D, ID_T and hash function h (), Tag T calculates the value of $h(N_T, N_D, ID_D, ID_T)$. If the calculation results and M3 are equal, then the data is from the server D.

Remark: $M_1=N_D$; $M_2=\{N_T, N_D, ID_T\}_{KPD}$, $h(N_T, ID_T)$; $M_3=h(N_T, N_D, ID_D, ID_T)$.

4. Strand Spaces and Authentication Tests

The Strand space model is based on the mathematical foundations of algebraic invariant set theorems. It takes advantage of graph theory to depict the process of implementation of the agreement. The Set A is composed of all the messages exchanged between the bodies of the Strand space model. A subset of set A is called term, A term may contain multiple sub-terms, a random number contained in the message and the subject constitute set T; The all key K compose set K. K includes public and private key pairs of all legitimate subjects and the attackers [19]. The node relationship describes the order logic that the entity nodes send and receive messages. The model also presents the correctness definition of security protocols, the description of the attacker ability and the correctness method that a security protocol is proved. Because of its efficient, robust and intuitive features, it has been widely used in the field of security protocol analysis, it can not only prove the correctness of security protocols, and we can also construct protocol attacks, and reveal the inherent weaknesses of protocol.

Authentication tests that are developed based on Strand space model is a protocol analysis techniques of challenge - Response Concept. The basic idea is that the protocol body sent a specific messages, in which value a is included (plain text or cipher text), and later the changed form of the value a is received (encrypted or decrypted), and it is true that there is a general protocol body who holds the corresponding key is involved in the implementation of the protocol. In the abstract level, the design of an authentication protocol can be seen as a choice of Authentication tests, and is a process of building a transforming (or transformed) edge to meet the two entities.

4.1. Protocol Goals

In the RFID protocol, the goals of the participants are of three kinds: [21]

Confidentiality all data transmitted in the exchange is to remain secret, and data intended for a pair should not be disclosed to the third participant.

Authentication I: Each participant P should receive a guarantee that each partner Q has received P's data and Q accepted it.

Authentication II: Each participant Q should receive a guarantee that data purportedly from a partner P in fact originated with P, freshly in a recent run of this protocol.

4.2. Authentication Tests Ideas

Suppose a principal in a cryptographic protocol creates and transmits a message containing a new value v, later receiving v back in a different cryptographic context. It can conclude that some principal possessing the relevant key K has received and transformed the message in which v was emitted. If K ∈ S is safe, this principal cannot be the penetrator, but instead must be a regular principal. A transforming edge is the action of changing the cryptographic form in which such a value v occurs. The authentication tests [19] give sufficient conditions for transforming edges being the work of regular principals. There are three main types of authentication test [21]: outgoing tests, incoming tests and unsolicited tests. The outgoing tests and incoming tests can guarantee the freshness; compared unsolicited tests do not guarantee freshness.

Definition 1 (outgoing test): $n_0 \Rightarrow^+ n_1$ is an outgoing test edge for a if: (I) a originates uniquely on n_0; (II) there is a single $t_0 = \{|h|\}_k \in$ *TERMS* (n_0) such that $a \sqsubseteq t_0$ (a "occurs once" in n_0).

(III) $t_0 \notin$ *TERMS* (n_1) and $a \in$ *TERMS*(n_1).

(IV) k is not in the set of penetrator's keys (those it initially has or those it can obtain).

Definition 2 (incoming test): $n_0 \Rightarrow^+ n_1$ is a incoming test edge for a if: (I) a originates uniquely on n_0; (II) $t_1 = \{|h|\}_k$; (III) $t_0 \notin$ *TERMS* (n_0) and $a \in$ *TERMS*(n_1); (IV) $a \sqsubseteq t_1$; (V) k is not in the set of penetrator's keys.

Definition 3 (unsolicited test): If $\{|h|\}_k \in$ *TERMS*(n), occurs once there, and penetrator cannot get k, then there is a node *m* s.t.: (I)*m* is regular; (II) $\{|h|\}_k$ originates at *m* (If $\{|h|\}_k$ originates at a penetrator's node it must be an E-strand, and then penetrator has *k*).

5. The Security Proof of Protocol

5.1. The Formal Protocol

In Section 3.2 it can be seen that during the execution of protocol the reader R is not involved in the mutual authentication process of database D and tag T, and its role is to pass data and to initiate authentication to the tag T. The implementation process of the protocol is simplified as shown in Fig. 3.

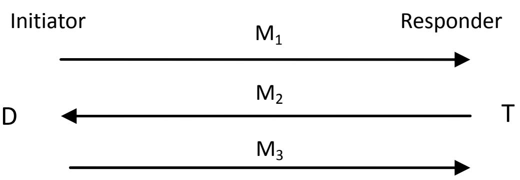

Fig. 3. The structure of RFID protocol.

Definition 4: Suppose (Σ, *P*) is a Strand Space If Σ is expressed by the following three strings; we call it the corresponding strand space of this RFID protocol.

The attacker strand *s*∈ *P*.

The initiator strand *t*O*RFIDInit*[N_D, N_T, ID_D, ID_T], traces of the form:

< +N_D, -{ N_T, N_D, ID_T }$_{KPD}$, $h(N_T, ID_T)$, +h(N_T, N_D, ID_D, ID_T)>.

In which, ID_D, ID_T, ∈ T_{name}, N_D, N_T, O*T*, N_DΠT_{name}, *RFIDInit*[N_D, N_T, ID_D, ID_T] represents the set of all the strands having the above traces, and the body of this correspond strand is ID_D.

The corresponding responder strand of initiator strand $t' \in RFID\,\mathrm{Re}\,sp[N_D, N_T, ID_D, ID_T]$, traces of the form:

$$< -N_D, +\{N_T, N_D, ID_T\}_{KP_D}, h(N_T, ID_T), -h(N_T, N_D, ID_D, ID_T) >$$

In which, $ID_D, ID_T \in T_{name}$, $N_D, N_T \in T$, $N_T \notin T_{name}$. $RFID\,\mathrm{Re}\,sp[N_D, N_T, ID_D, ID_T]$ represents the set of all the strands having the above traces, and the body of this correspond strand is ID_T.

From the above definitions, when given a strand, it can uniquely identify the attacker strand, initiator strand or the responder strand.

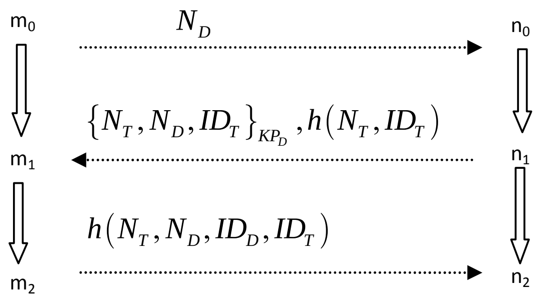

Fig. 4. The authentication test process.

5.2. The Security Proof with Authentication Tests

Proposition 1 (Confidentiality proof (for D)): Suppose that *C* is a bundle of *S*, in which ID_D, ID_T ∈ T_{name}, KE_T Π K_P; the same time, *C* contains both the initiator strand s∈ *RFIDInit*[N_D, N_T, ID_D, ID_T]. If S_I={N_T, ID_T} is uniquely generated, for any node *n*∈ *C*, we get *term*(*n*)∉ S_1.

Proof. Let k be the set of inverses of unsafe keys, i.e. $k=(K\backslash S)^{-1}$. Let *t*=S_1∪ *S*.

Theorem [22, Corollary 6.12]: if there is a node *m*∈ *C* with *term*(*m*) ∈ $I_K[t]$, then there a regular node *n*∈ *C* that is an entry point for $I_K[t]$. However, inspecting the positive regular nodes of RFID protocol, we see that no value in $\mathcal{T}$ is ever sent, unless protected by a key whose inverse is safe. The data to be sent is encrypted ($KE_T \notin K_P$) or protected by the hash function *h*(…*t*…). Therefore, the assumption *term*(*m*) ∈ S_1 does not hold, so the proposition is proved.

Proposition 2（Authentication I）: Suppose that *C* is a bundle of *S*, in which ID_D, ID_T, ∈ T_{name}, KE_T Π K_P; the same time, *C* contains both the initiator strand *s*∈ *RFIDInit*[N_D, N_T, ID_D, ID_T] and *C-height*≥2. If $N_D \neq N_T$ and N_D is uniquely generated, so the node *C* has a response strand *s'*∈ *Resp*[N_D, N_T, ID_D, ID_T], and *C-height*≥2.

Proof. In Fig. 4, N_D is sent in node m_0, $\{N_T, N_D, ID_T\}_{KP_D}, h(N_T, ID_T)$ is received at node m_1, so $m_0 \Rightarrow^+ m_1$ is the Transformed Edge for N_D. $\{N_T, N_D, ID_T\}_{KP_D}, h(N_T, ID_T)$ is a test component about N_D. Because $KE_T \notin K_P$ and definition 2, the edge $m_0 \Rightarrow^+ m_1$ constitutes is an outgoing test for N_D. N_D is uniquely generated at node m_0, so there must be a negative node n_0 to accept it. Because $\{N_T, N_D, ID_T\}_{KP_D}, h(N_T, ID_T) = term(n_1)$ and n_1 is a sending node (node positive), $n_0 \Rightarrow^+ n_1$ is the Transforming Edge for N_D, and There must be a node $\langle s',1\rangle$ of matching response strand $s' \in RFIDResp[N_D, N'_T, ID_D, ID_T']$. Because $\langle s',1\rangle \Rightarrow \langle s',2\rangle$ and $term(\langle s',2\rangle) = \{N_T, N_D, ID_T\}_{KP_D}, h(N_T, ID_T)$, so $N_T = N'_T$, $ID_T = ID_T'$, $C-height \geq 2$ for s'.

Proposition 3（Authentication II）: Suppose that C is a bundle of Σ, $ID_D, ID_T \in T_{name}$; $KE_D, KE_T \notin K_P$; the same time, C contains both the responder strand $s \in RFID\mathrm{Re}sp[N_D, N_T, ID_D, ID_T]$ and $C-height$ =3. The N_T is uniquely generated, so C has a responder strand $s' \in RFIDInit[N_D, N_T, ID_D, ID_T, M]$, and $C-height$ =3, the same time $\langle s,2\rangle \prec \langle s',2\rangle$.

Proof. In Fig 4, the nodes n_1, n_2 constitute an incoming test for N_T, i.e. $\langle s,2\rangle \Rightarrow^+ \langle s,3\rangle$ constitutes an incoming test to N_T for $\{N_T, N_D, ID_T\}_{KP_D}, h(N_T, ID_T)$, then there must be nodes $m_1, m_2 \in C$, such that $m_1 \Rightarrow m_2$ is a Transforming Edge for N_T. Because n_2 is a positive node, $term(n_2) = \{N_T, N_D, ID_T\}_{KP_D}, h(N_T, ID_T)$, and N_T is uniquely generated at node $\langle s,2\rangle$, there must be a negative node n_1 to accept N_T. The n_1 is a positive node, so there must be an initiator strand $s' \in RFIDInit[N_D, N_T, ID_D, ID_T', M']$ at node $\langle s',2\rangle$, and $\langle s,2\rangle \prec \langle s',2\rangle$. Because $\langle s,2\rangle \Rightarrow^+ \langle s',3\rangle$, and $term(\langle s',3\rangle) = \{N_T, N_D, ID_T\}_{KP_D}, h(N_T, ID_T)$ contains information of ID_T', N'_T, so $ID_T = ID_T', N_T = N'_T$, and $C-height$ =3.

About responder (Tag T), whose confidentiality, authentication features I, II have a similar parallel theorem and proof with the sender (server D).

5.3. The Analysis of Security Properties

Confidentiality: The proof of Proposition I effectively guaranteed that the data $\{N_T, N_D, ID_T\}_{KP_D}$ tag T send will not be forged by an attacker, because the private key is only stored on the server D ($KE_T \notin K_P$).

Resistance to tracking attack: In the protocol, when the message included ID_D is sending, every time there is a random value is transmitted with it. In the transfer process, ID_D is encrypted by key or one-way hash function, so the tracking of attacker to Tag is difficult to achieve.

Anti-replay attack: In the proof process of Proposition II, the edge $m_0 \Rightarrow^+ m_1$ constitutes an outgoing test for N_D. According to the literature [21] Definition 2.1 a strong guarantee of freshness is that the protocol initiator can effectively prevent attackers to do replay attacks.

Resistance to pretending attack: The proof of Proposition 3 ensures that in the authentication process of communicating two parties the third party is not involved, which can effectively prevent pretending attack of attackers. Attacker would have no way to get any party's private key; and there is no way to break the one-way hash function. Therefore, the attacker does not have the ability to successfully pretend server or Tag.

The Mutual Authentication: In our protocol, the server side and the Tag side through each other's public key to encrypt their identity information, a private key can authenticate each other, and in the protocol a hash function is used for confirmation to authentication.

Analysis combined with the appeal, our proposed protocol can resist most of the attacks on RFID, and can effectively ensure the security of RFID protocol.

6. Conclusions

Existing most of RFID authentication protocols, in which there are some security risks, or their safety cannot be given a strong guarantee, and they cannot be actually available RFID security solutions. Based on protocol analysis of previous research, in this paper, the method of the Authentication tests are used to propose a new authentication protocol with the formal safety analysis, and gives strong evidence of safety. It shows that the proposed protocol can meet the basic safety requirements of the RFID system.

Through the analysis of security threats of RFID systems with Authentication tests, we have mastered the methods against these threats and worked on a security model, by which we can design a safe and effective RFID authentication protocol.

Acknowledgements

This work was supported in part by a grant from 2013 Yancheng industrial supporting projects (The application security of RFID technology in the emerging industry, the intelligent management system of Campus network) and 2013 National Statistics research project (2013461).

References

[1]. MIT Auto-ID, retrieved Sep. 10, 2009 from World Wide Web: http://autoidlabs.mit.edu

[2]. Songsen Yu, Yun Peng, Jian Yang, Jiajing Zhang, The design and realization of a Lightweight RFID Mechanism Integrating Security and Anti-collision, *Journal of Software*, Vol. 6, Issue 7, 2011, p.1235-1240.

[3]. Minbo Li, Hua Li, Research on RFID Integration Middleware for Enterprise Information System, *Journal of Software,* Vol. 6, Issue 2, February 2011, pp.167-174.

[4]. De Cannière C., Dunkelman O., Knežević M., KATAN and KTANTAN—A Family of Small and Efficient Hardware-Oriented Block Ciphers. In: Clavier, C., Gaj, K. (eds.) CHES 2009. *LNCS*, Vol. 5747, 2009, pp. 272–288.

[5]. Billet Olivier, Etrog Jonathan, Gilbert Henri, Lightweight Privacy Preserving Authentication for RFID Using a Stream Cipher, *Lecture Notes in Computer Science*, Vol. 6147 LNCS, 2010, pp. 55-74.

[6]. Song Boyeon, Mitchell Chris J., RFID Authentication Protocol for Low-cost Tags, WiSec'08: *Proceedings of the 1st ACM Conference on Wireless Network Security*, 2008, pp. 140-147.

[7]. EPCglobal: Class-1 generation 2 UHF air interface protocol standard version 1.2.0: "Gen 2". http://www.epcglobalinc.org/standards

[8]. Sarma S. E., Weis S. A., Engels D. W., RFID systems and security and privacy implications, *Lectures Notes in Computer Science* 2523, 2003, pp. 454-469.

[9]. H. Chien and C. Chen, Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards, *Computer Standards & Interfaces*, Vol. 29, Issue 2, 2007, pp. 254–259.

[10]. Sarma S. E., Weis S. A., Engels D. W., Radio-frequency identification: Secure risks and challenges, *RSA Laboratories Cryptobytes,* Vol. 6, Issue 1, 2003, pp. 2-9.

[11]. Duc D. N., Park J., Lee H., Enhancing security of EPCglobal GEN-2 RFID tag against traceability and cloning, in *Proceedings of the Symposium on Cryptography and Information Security (SCIS 2006)*, Hiroshima, Japan, January 17-20, 2006.

[12]. Feng Xiao, Yajian Zhou, Jingxian Zhou, Hongliang Zhu, Xinxin Niu, Security Protocol for RFID System Conforming to EPC-C1G2 Standard, *Journal of Computers*, Vol. 8, Issue 3, March 2013, pp. 605-612.

[13]. C.-L. Chen, Y.-Y. Deng, Conformation of EPC class 1 and generation 2 standards RFID system with mutual authentication and privacy protection, *Engineering Applications of Artificial Intelligence* Vol. 22, Issue 8, 2009, pp. 1284–1291.

[14]. H. Chien and C. Chen, Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards, *Computer Standards & Interfaces,* Vol. 29, Issue 2, 2007, pp. 254–259.

[15]. L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls and I. Verbauwhede, Public-key cryptography for RFID-tags, in *Printed Handout of Workshop on RFID Security*, 2006, pp. 61-76.

[16]. P. Tuyls and L. Batina, RFID-Tags for Anti-counterfeiting, in Topics in Cryptology-CT-RSA (ed. by D. Pointcheval), Lecture Notes in Computer Science 3860, *Springer Verlag*, 2006, pp.115-131.

[17]. Buttyan L., Staamann S., Wilhelm U., A simple logic for authentication protocol design, in *Proceedings of the 11th IEEE Computer Security Foundations Workshop,* Rockport, Massachusetts, 1998, pp. 153-162.

[18]. Guttman J. D., Fábrega F. J. T., Authentication tests, in *Proceedings of the IEEE Symp. on Security and Privacy*, 2000, pp. 96−109.

[19]. Guttman J. D., Fábrega F. J. T., Authentication tests and the structure of bundles, *Theoretical Computer Science*, Vol. 283, Issue 2, 2002, pp. 333−380.

[20]. Fábrega F. J. T., Herzog J. C., Guttman J. D., Strand spaces: Proving security protocols correct, *Journal of Computer Security*, Vol. 7, Issue 2-3, 1999, pp. 191−230.

[21]. Guttman J. D., Security protocol design via authentication tests, in *Proceedings of the IEEE Computer Security Foundations Workshop,* 2002, pp. 92−103.

[22]. F. J. Thayer Fabrega, J. C. Herzog, and J. D. Guttman, Strand spaces: Proving security protocols correct, *Journal of Computer Security*, Vol. 7, 2/3, 1999, pp. 191–230.