ISSN: 2688-8645

Design of Authentication Protocol Based on Hash Function

Yang Song[1] and Zhaohua Long[2]

[1]School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chong Qing 400065, China;

[2]School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chong Qing 400065, China.

Abstract

RFID technology has been widely developed in many fields such as health care, transportation, retail, logistics, national defense, etc, due to its excellent characteristics of fast reading, high reliability, and low manufacturing cost. However, security and privacy issues also arise in the process of system information transmission. This paper proposes a bidirectional authentication protocol based on the hash function for the application layer security of the RFID system, which can resist most attacks against the application layer of the RFID system. By establishing an idealized model of the protocol, the security of the protocol is proved by using BAN logic, and the correctness of the protocol is verified by simulation experiments.

Keywords

RFID, authentication protocol, security analysis, BAN logic.

1. Introduction

Radio Frequency Identification(RFID) is a technology that uses wireless electromagnetic waves of a specific frequency to realize automatic identification without physical or optical contact to identify and exchange information. At present, the research on RFID security is roughly divided into two directions, one is to study protection measures based on physical hardware, and the other is to study security authentication protocols based on encryption algorithms.

The principle of a hardware-based security mechanism is to protect private content from being leaked. Common methods include faraday cage [1], interference [2], blocking tag [3], and tag inactivation [4]. Although the physical method is directly effective, it is mandatory and not suitable for general application.

Common security authentication protocols based on hash function include hash-lock protocol [5], randomized hash-lock protocol [6], hash-chain protocol [7], and LCAP protocol [8].

The hash-lock protocol uses plain text transmission during communication, and the ID is fixed, which is vulnerable to counterfeit attacks, location tracking attacks, and retransmission attacks.

The randomized hash-lock protocol during each authentication process, the reader needs to obtain all IDs in the server database. It results in a low data processing rate, which affects the system's communication progress, and uses plain text transmission, which is vulnerable to counterfeit attacks and retransmission attacks.

The hash-chain protocol uses a shared key self-renewal mechanism, but only one-way authentication in the protocol process, which is vulnerable to counterfeit attacks.

The LACP protocol uses a self-updating mechanism, which transmits encrypted data and the authentication is bidirectional. It can well resist location tracking and counterfeit attacks, but it cannot resist asynchronous attacks.

Aiming at the shortcomings of the previous researches on the security of the RFID system, this paper proposes a lightweight authentication protocol based on the hash function. The protocol

ISSN: 2688-8645

introduces a disturbance value and a bidirectional authentication process, which can effectively resist eavesdropping attacks, location tracking attacks, retransmission attacks, and counterfeit attacks. At the same time, the complexity of the protocol and the implementation cost are low and easy to implement. Finally, BAN logic and software are used to verify and analyze the protocol. And the results proved the correctness and safety of the protocol.

2. RFID System

The RFID system generally consists of three parts[9]: electronic tag, reader, and server. The structure of the RFID system is shown in Figure 1.

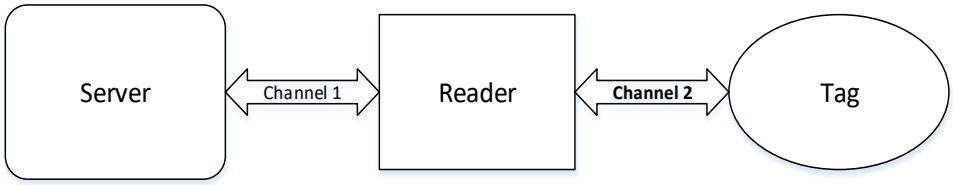

Figure 1. Structure of the RFID system

2.1. Tag

RFID electronic tag is mainly used for item identification and item information storage. It includes control arithmetic unit, storage unit, radio frequency unit, and antenna.

2.2. Reader

The main function of the RFID reader in the RFID system is data transmission and conversion. It is composed of a control unit, a storage unit, an external interface, a radio frequency unit, an antenna, and a power supply.

2.3. Server

The RFID server is composed of a database and arithmetic processing components. It has high data processing and storage capabilities, responsible for storing the information of readers and electronic tags, and managing the contents of the database. And it also deals with the identification process between tags and readers.

3. Lightweight Authentication Protocol Based on the Hash Function

This paper takes the LACP protocol and the has-chain protocol as reference bases introduces a bidirectional authentication process. And uses the secret information self-updating mechanism to propose a lightweight authentication protocol based on hash functions.

3.1. Protocol Principle

The tag stores its own ID and shared key K , in the beginning, the server calculates the $\mathrm{H(ID}\,||\,\mathrm{K}\,||\,\mathrm{TE)}$ of the tag and stores $\{\mathrm{ID},\mathrm{K},\mathrm{H}(\mathrm{ID})\}$ in the database as a data tuple and builds an index. The reader integrates a unit that generates a disturbance value TE based on time and sets a flag to assist in completing the authentication process. The database stores all the legally tuples and can be retrieved. At the same time, the server is responsible for the hash operation in the authentication process to complete the protocol authentication. The feature of the server is that the data unit is retrieved before the authentication message is calculated. The protocol flow is shown in Figure 2.

ISSN: 2688-8645

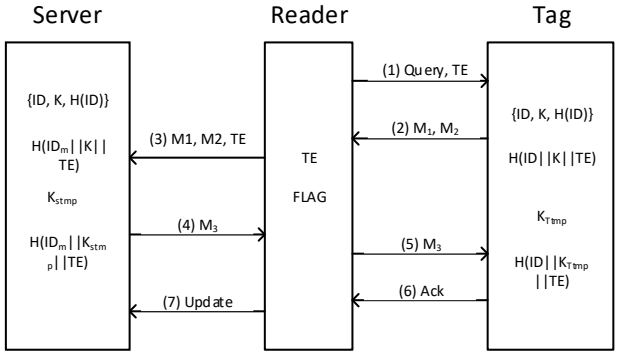

Figure 2. Flow chart of the protocol

3.2. Certification Process

(1) The reader sends an inquiry request and the generated disturbance value TE to the electronic tag and sets the $FLAG$ to N

(2) After receiving the inquiry request, the electronic tag calculates $H(ID)$ and $H(ID||K||TE)$, and sends them to the reader as M_1 and M_2, and then calculates K_{Ttmp} and $H(ID||K_{Ttmp}||TE)$ for standby.

(3) The reader sends the M_1, M_2 and TE to the server. The server retrieves the corresponding data tuple in the database according to M_1. If the retrieval fails, the authentication is unsuccessful and the authentication is terminated. Otherwise, execute (4).

(4) Extract the retrieved data tuple $\{ID_m, K, H(ID_m)\}$ from the database, calculate $H(ID_m||K||TE)$ and compare it with M_2. If the two values are not equal, the authentication of the tag fails and the authentication is terminated. Otherwise, execute (5).

(5) The server calculates K_{Stmp} and $H(ID_m||K_{Stmp}||TE)$, and forwards $H(ID_m||K_{Stmp}||TE)$ as M_3 to the electronic tag through the reader, and at the same time puts $FLAG$ in the ready state Y.

(6) The electronic tag compares $H(ID||K_{Ttmp}||TE)$ and M_3. If they are not the same, the authentication of the reader fails and the authentication is terminated. Otherwise, execute (7).

(7) The electronic tag replaces the original K with K_{Ttmp} and sends Ack it to the reader.

(8) After the reader receives Ack, it checks the $FLAG$ status. If $FLAG$ it is ready, send $Update$ it to the server. Otherwise, no action.

(9) After receiving $Update$, the server replaces K the original data tuple with K_{Stmp} and writes it to the database.

4. Experiment Analysis

4.1. Safety Analysis

Whether it can resist eavesdropping attacks, location tracking attacks, counterfeit attacks, and retransmission attacks is an important indicator for evaluating the security of RFID application layer protocols [10]. After analyzing the model, this protocol can achieve the following security effects.

(1) Data privacy protection

During the transmission of system information, the electronic tag ID and the shared key K are encrypted using a hash function. Moreover, the key uses a self-updating mechanism, so the

ISSN: 2688-8645

attacker cannot directly obtain the secret data of the tag, which protects the privacy of the tag data.

(2) Forward security

Since the shared key and the interference value both change and the hash function is unidirectional, this makes it impossible to deduce the message in the previous communication process even if the message in the current transmission process is intercepted.

(3) Bidirectional authentication

The server calculates $H(ID_m \| K \| TE)$ according to the information queried in the data tuple and compares it with the M_2 sent by the reader to complete the authentication of the tag. The tag calculates $H(ID \| K_{Ttmp} \| TE)$ and compares it with the message M_3 sent by the reader to complete the authentication of the reader and implements bidirectional authentication.

(4) Anti-eavesdropping attack

The ID and K of the electronic tag are encrypted by the operation of the hash function, so the attacker cannot directly obtain the ID and K of the tag through eavesdropping.

(5) Anti-location tracking attack

The communication shared key K and the disturbance value TE is dynamically refreshed. During each round of authentication, the information M_2 sent by the electronic tag changes. The attacker cannot determine the characteristics of the electronic tag's response information, so it cannot track the position.

(6) Anti-counterfeiting attack

The shared key K stored on the tag and the server will be updated after each round of authentication, so the attacker cannot forge the correct key and cannot generate the correct $H(ID \| K \| TE)$, and the server authentication cannot be completed. In the same way, the $H(ID_m \| K_{Stmp} \| TE)$ message generated by the forgery cannot be authenticated by the electronic tag, and neither the attacker can fake the tag nor the reader.

(7) Resistant to retransmission attacks

M_1, M_2 and M_3 are all unidirectional values calculated by the hash function through the secret information, and the K in the secret information is dynamically refreshed, so the values of M_2 and M_3 are not the same as before in each round of authentication It will be the same, even if an attacker steals all the messages in the previous authentication process, it cannot be used in the current authentication process, preventing retransmission attacks.

(8) Message symmetry

The reader has set the $FLAG$. It will send a request $Update$ to the server only after the tag authentication succeeds and sends a confirmation response Ack to the reader, otherwise the data will not be updated.

(9) Resistance to denial of service attacks

The server first uses the received M_1 to retrieve the tag information in the database. If there is no corresponding retrieval information, the server does not perform calculation processing, so the false message initiated by the attacker will be excluded when the server retrieves. This avoids server crashes caused by a lot of useless operations.

Based on the security analysis of the authentication protocol in this paper, it will be compared with the hash lock protocol, randomized hash lock protocol, hash chain protocol, and LCAP

ISSN: 2688-8645

protocol. The comparison results are shown in Table 1. " √ " in the table indicates that attributes are supported, "×" indicates that attributes are not supported.

The protocol proposed in this paper can complete the bidirectional authentication between the server and the electronic tag and can resist most types of attacks, and it is more secure than other protocols.

Table 1. Protocol security comparison

Attributes	Hash-Lock	Randomized Hash-Lock	Hash-Chain	LCAP	This Protocol
Data privacy	√	×	√	√	√
Forward security	×	√	√	√	√
Bidirectional authentication	×	×	×	√	√
Anti-eavesdropping	×	×	√	√	√
Anti-location tracking	×	×	×	√	√
Anti-counterfeiting	×	×	×	√	√
Anti-retransmission	×	×	×	√	√
Anti-denial service	√	×	×	√	√
Message symmetry	×	×	×	×	√

4.2. BAN Logic Analysis

4.2.1. Protocol Idealized Description

Subject object: T, R, S.

Message object: M1, M2, M3, TE

(1) R->T: Query, TE

(2) T->R: M1, M2

(3) R->S: M1, M2, TE

(4) S->R: M3

(5) R->T: M3

(6) T->R: Ack

(7) R->S: Update

4.2.2. Initial Assumption

(1) $S|\equiv S\overset{K}{\leftrightarrow}T$

(2) $T|\equiv T\overset{K}{\leftrightarrow}S$

(3) $S|\equiv T|\Rightarrow M_2$

(4) $T|\equiv S|\Rightarrow M_3$

(5) $T|\equiv\#(TE)$

ISSN: 2688-8645

(6) $S|\equiv \#(TE)$

4.2.3. Expected goal

(1) $S|\equiv ID_T$

(2) $T|\equiv ID_m$

4.2.4. Derivation

(1) The Known assumption $S|\equiv S\overset{K}{\leftrightarrow}T$, ideal model description $S\lhd\{M_2\}$, message $M_2=H(ID_T\|K\|TE)$. Using the rule $\dfrac{P|\equiv P\overset{K}{\leftrightarrow}Q, P\lhd\{X\}_K}{P|\equiv Q|\sim X}$ can be derived $S|\equiv T|\sim M_2$.

(2) The known assumption $S|\equiv \#(TE)$, $M_2=H(ID_T\|K\|TE)$. Using the rule $\dfrac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$ can be derived $S|\equiv \#(M_2)$.

(3) The result $S|\equiv \#(M_2)$, $S|\equiv T|\sim M_2$. Using the rule $\dfrac{P|\equiv \#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$ can be derived $S|\equiv T|\equiv M_2$.

(4) The Known assumption $S|\equiv T|\Rightarrow M_2$, result $S|\equiv T|\equiv M_2$. Using the rule $\dfrac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$ can be derived $S|\equiv M_2$.

(5) The result $S|\equiv M_2$, message $M_2=H(ID_T\|K\|TE)$. Using the rule $\dfrac{P|\equiv Q|\sim (X,Y)}{P|\equiv Q|\sim X}$ can be derived $S|\equiv ID_T$.

The goal (1) has been certified, and in the same way, the goal (2) can be certified.

4.3. Simulation Experiment

4.3.1. Experimental Design

The system development environment is in the Windows operating system, the database uses the MySQL relational database, and the C ++ program is used to design the simulation system. The schematic diagram of the system model is shown in Figure 3. The system is divided into three parts, namely the electronic label side, the reader side, and the server Use inter-process communication to simulate RFID communication process.

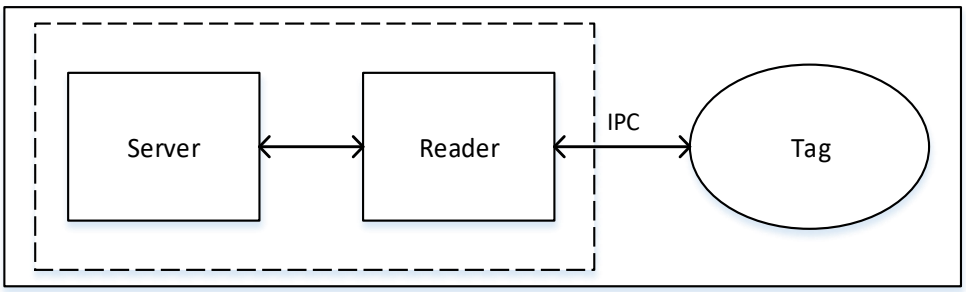

Figure 3. Simulation system model

ISSN: 2688-8645

4.3.2. Protocol Message Design

The protocol message is divided into header and body, and the message structure is shown in Figure 4. The protocol header is used to control the transmission of information and consists of three parts: protocol version number, message type, and message length, each part occupies one byte, a total of three bytes.

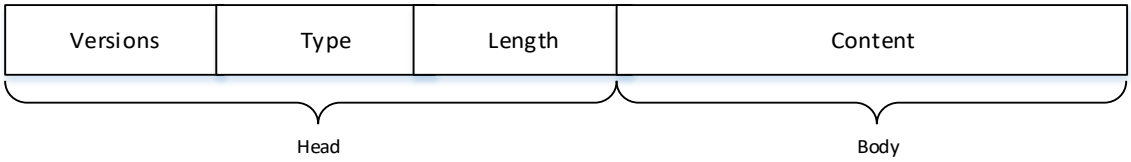

Figure 4. Protocol message structure

The detailed description of the protocol message is shown in Table 2, which is expressed in hexadecimal numbers.

Table 2. Protocol message specification

Version	Type	Length	Content	Explanation
0x01	0x01	0x08	TE	The reader generates TE and initiates an inquiry
0x01	0x02	0x08	TE	The reader sends TE to the server
0x01	0x03	0x10	M1, M2	Tag sending data
0x01	0x04	0x10	M1, M2	Reader forwarding data
0x01	0x05	0x08	M3	The server rings to send data
0x01	0x06	0x08	M3	Reader forwarding data
0x01	0x07	0x00	Ack	Tag confirmation response
0x01	0x08	0x00	Update	Reader update request

4.3.3. Analysis of Results

According to the process performed by the system, the operation results of the server, reader, and tag after a successful authentication process are shown in Figure 5, Figure 6, and Figure 7, respectively.

```
D:\programspace\Tag_1\bin\Release\Tag_1.exe
===Tag Process===
Inquiry received
Successfully connected to the reader
Start to work
Receive content of reader: 01011039400a13bd6be6c9
Tag sends content:         010320a7b89ff4dda7fbf6b254d809a1c33739
Receive content of reader: 0106100e62ad817fe20b02
Successful authentication
Tag sends confirmation response: 010700
```

Figure5. Tag process

ISSN: 2688-8645

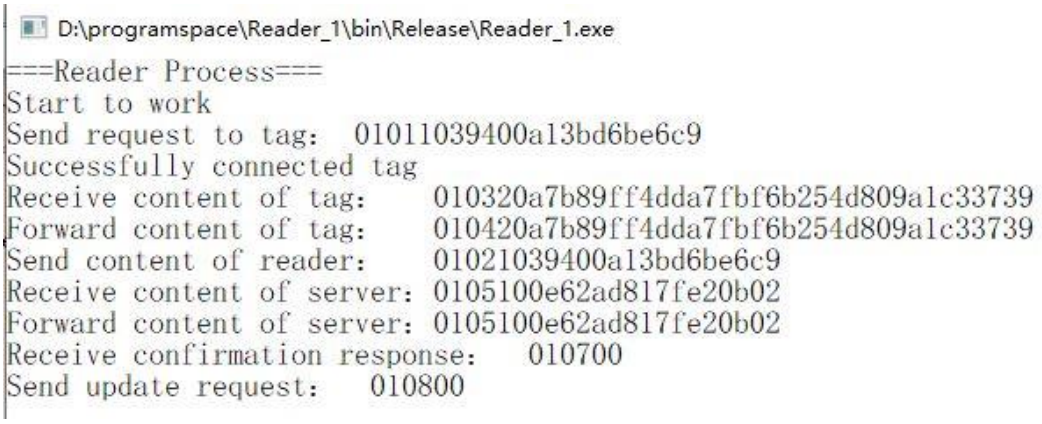

Figure6. Reader process

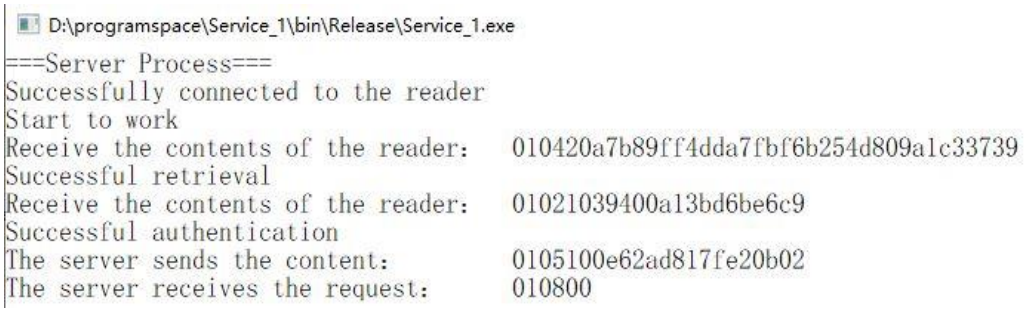

Figure 7. Server process

From the results of the experiment, it can be seen that the authentication process between the server and the electronic tag is bidirectional, that is, the server must authenticate the identity of the electronic tag and the electronic tag also needs to verify the identity of the server For authentication, subsequent data transmission can only be carried out after the mutual authentication between the two parties is successful, ensuring the security of the communication process. At the same time, the disturbance value and dynamic key refresh mechanism are introduced, so that the transmitted message is constantly changing, so the attacker cannot extract the fixed characteristics of the message, which improves the security of the data. The introduction of the message response also guarantees the symmetry of data updates at both ends.

5. Conclusion

This article first gives an overview of the research of RFID authentication protocol, summarizes some existing RFID authentication protocol loopholes, and leads to some basic needs of RFID security authentication protocol. Then, according to the existing security problems, the detailed design of the two-way authentication security protocol based on the hash function is proposed in this paper. After that, the correctness and security of the protocol were proved through formal language. Finally, simulation experiments verify the correctness of the protocol model.

The experiment was conducted under ideal conditions without considering the actual situation. In the future, actual interference factors can be added to verify the actual application value of the protocol.

ISSN: 2688-8645

References

[1] T. Dimitriou: A lightweight RFID protocol to protect against traceability and cloning attacks, First International Conference on Security and Privacy for Emerging Areas in Communications Networks (Athens, Greece, Sep 5-9, 2005), Vol. 2005, p. 59-66.

[2] A. Jules, R. L. Rivest, M. Szydlo The blocker tag: selective blocking of RFID tags for consumer privacy, Proceedings of the 10th ACM Conference on Computer and Communications Security (Washington D. C., USA, October 2003). Vol 2003, p.103-111.

[3] H. G Luo, G. J. Wen, J. Su, et al: SLAP: Succinct and Lightweight Authentication Protocol for a low-cost RFID system, Wireless Networks, Vol. 24(2018) No. 1, p. 69-78.

[4] K. Rhee, J. Kwak, S. Kim, et al: Challenge-response based RFID authentication protocol for distributed database environment, Lecture notes in computer science, Vol. 3450(2005) No. 1, p. 70-84.

[5] S. Kinoshita, M. Ohkubo, F.Hoshino: Privacy enhanced active RFID tag, Proc. International Workshop on Exploiting Context Histories in Smart Environments(Munich, Germany, May 11, 2005). Vol. 2005, p. 100-104.

[6] S. A. Weis, S. E. Sarma, R. L.Rivest: Security and privacy aspects of low-cost radio frequency identification systems (Spring, Germany 2004), p. 201-212.

[7] M. Ohkubo, K. Suzuki, S Kingships: Hash-Chain based forward-secure privacy protection scheme for low-cost RFID, Pro. SCIS2004, Vol. 2(2004) No. 3, p. 719-724.

[8] S. M. Lee, Y. J. Hwang, D. H. Lee, et al.: Efficient authentication for low-cost RFID systems, Proceedings of the International Conference on Computational Science and Its Applications (Singapore, May 9-12, 2005). Vol.3480, p. 619-627.

[9] Y. L. Huang: IoT RFID Core Technology Details (People's University of Posts and Telecommunications Press, China 2012), p. 19-20.

[10] Cui Tingting, K. Jia, K. Fu, et al: New Automatic Search Tool for Impossible Differentials and Zero-Correlation Linear Approximations, IACR Cryptology ePrint Archive, Vol. 2(2016) No. 3, p. 689.