ATLANTIS PRESS
Advances in Social Science, Education and Humanities Research (ASSEHR), volume 130
2nd International Forum on Management, Education and Information Technology Application (IFMEITA 2017)

Design and Application of RFID Security Middleware Model Based on Elliptic Curve Digital Signature

Qiyue Wang[1, a], Ping Zhang [1, b]

[1] School of Mathematics and Statistics, Henan University of Science and Technology, Luoyang 471023 China

[a]332087807@qq.com, [b]zhangping76@126.com

Keywords: RFID system, Elliptic curve digital signature, Middleware, Security model.

Abstract. A RFID (Radio Frequency Identification) security middleware model based on the traditional RFID system is proposed in this paper. The elliptic curve digital signature module in the model has the characteristics of guaranteeing the effectiveness and non-tampering of the original information. By analyzing the correctness and feasibility of the signature algorithm and applying the improved RFID security middleware to the E-commerce system, it can effectively help the users to identify the authenticity of the goods and protect the legitimate rights and interests of the merchants and users.

Introduction

RFID is a non-contact automatic identification technology [1]. Most of RFID systems are implemented using inductive or inductive coupling transmission characteristics, and it is one of the main technologies of the Internet [2]. In recent years, with the development of information security, network communications and other technology, RFID technology has shown a huge space for development gradually, and it has been widely used in our daily life. For example, the technology is used in business automation, industrial automation, transportation management and many other areas currently. So it's very important to strengthen the security of RFID systems.

With the development of E-commerce, more and more people like to shop online. In order to buy all over the world of goods at home, a large number of people choose the Overseas Taobao in China. But how to verify the authenticity of goods has become a big problem in the Overseas Taobao. However, due to the natural security vulnerabilities of RFID systems [3], there are some security risks in the information transmission process. The attacker can track or tamper the information, which causes information to be leaked, and even makes the RFID system crash.

In view of the security problem of RFID system, this paper will be different from the traditional RFID improvement mode. We will divide the middleware into modules in the RFID system, and propose an improved RFID security middleware model based on elliptic curve digital signature algorithm. The model makes the recipient of the information can identify the authenticity of the identity of the sender, and improves the security of the system and the effectiveness of storage [4], and then ensures that the legitimate interests of consumers and merchants.

The Basic Structure and Security of RFID System

A complete RFID system consists of tags, readers, Middleware, back-end servers [5]. As shown in Fig. 1, there is a wireless channel between the tag and the reader, and there is a wired channel between the reader and the back-end server. The tag carrying a unique RFID code is placed on the object to be identified, the object can use the reader's Radio Frequency Technology to read the information carried in the label, the information transmitted over the wired channel is finally stored in the back-end server.

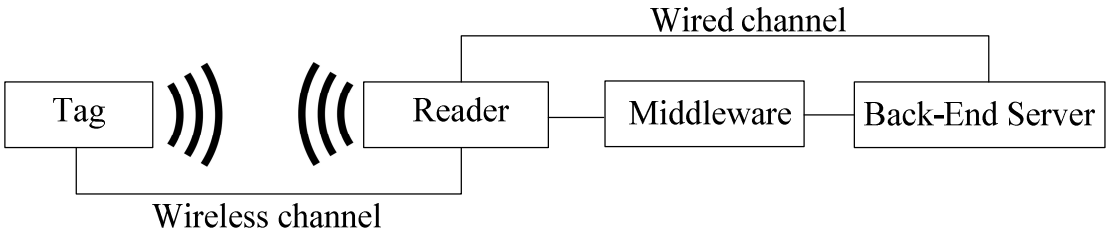

Fig.1 Structure Diagram of RFID

The RFID system is open completely, and it will inevitably bring the user privacy exposure when it is attacked. As the tags in the system respond to any reader with standard protocol access, although this feature can be used to track objects or users at a far distance, it also allows intruders to access a tag using a standard protocol, which causes user privacy exposure of the RFID system [6]. Therefore, there are insecurity factors in RFID system, which provides the attacker with operating space, poses a great threat to the system security and affects the promotion speed of the system application. Such as traditional IC cards or barcodes, which record information about users or articles. If the signals of the RFID system radio channel are intercepted by the attacker, it will cause the disclosure or tampering of information and great losses.

The role of RFID middleware in RFID systems:

（1） It can well deal with data transmission between a system and the other system [7];

（2） It has a strong computing and storage capacity;

（3） When the intruder attacks the wireless channel, it can play a role in prevention and discovery.

Thus, labels, readers and middleware are an important part of the RFID system. Therefore, the safety of RFID middleware becomes important particularly [8]. The main security risks of middleware are as follows:

（1） Data is vulnerable to be attacked in the network;

（2） The attacker steals legitimate users' personal information through middleware security vulnerabilities, or tamper information settings of middleware.

（3） An attacker steals operational privileges and manipulates middleware to access unauthorized access by illegal means.

section headings are in boldface capital and lowercase letters. Second level headings are typed as part of the succeeding paragraph (like the subsection heading of this paragraph).

Elliptic curve digital signature algorithm

ECC is a kind of cryptosystem which is obtained by using this principle that the points in the elliptic curve E on a finite field F_q can constitute a finite group [9]. The equation for the elliptic curve E is:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \quad (1)$$

Where $a_1, a_2, a_3, a_4, a_6 \in Fq$, and $\Delta \neq 0$, Δ is the discriminant of E [10]. The equation is Weierstrass equation, and it has different forms of equations under different characteristics. In this paper, we want to discuss the elliptic curve equation:

$$y^2 = x^3 + ax + b. \quad (2)$$

At this time, $ch(F_q) \neq 2,3$, $ch(F_q)$ is the characteristic of the finite field F_q , and $a, b \in F_q$, $\Delta = 4a^2 + 27b^2 \neq 0$. The points $P(x_1, y_1)$, $Q(x_2, y_2)$ and $R(x_3, y_3)$ on an elliptic curve in a finite field satisfy the scalar multiplication.

When $P \neq Q$,

$$P+Q=\begin{cases} x_3 = l^2 - x_1 - x_2 \\ y_3 = l(x_1 - x_3) - y_1 \end{cases}, l = \frac{y_2 - y_1}{x_2 - x_1} \qquad (x_2 \neq x_1). \tag{3}$$

When $P = Q$,

$$2P=\begin{cases} x_3 = l^2 - 2x_1 \\ y_3 = l(x_1 - x_3) - y_1 \end{cases}, l = \frac{3x_1^2 + a}{2y_1} \qquad (y_1 \neq 0). \tag{4}$$

ECDSA is an encryption method that applies elliptic curve cryptosystem to digital signature. Firstly, an elliptic curve E is chosen which based on a finite field Fq, the order of the elliptic curve E is $\#E(Fq) = fn$, where n is a large prime number, f is usually small integers such as 1,2,4 and so on, this ensures the efficiency of the algorithm. In addition, it is necessary to ensure the intractability of the discrete logarithm problem on $E(Fq)$. In ECDSA, the parameters of the elliptic curve is $D = (\mathrm{q}, \mathrm{a}, \mathrm{b}, \mathrm{G}, \mathrm{n}, \mathrm{P})$, where q is the number of elements in the finite field Fq, $a, b \in Fq$ is the coefficient of the elliptic curve equation, G is the base point of the elliptic curve and $O(\mathrm{G}) = \mathrm{n}$ [11] where n is the order of the finite field Fq. Choose a confidential integer $k \in \{1, 2, \mathbf{L}, n-1\}$, use k as a private key, calculate $P = kG$, use P as a public key, use an integer m to represent the information we want to sign, where we specify $m < n$.

Signature process:

（1） $\forall k_1 \in \{1, 2, \mathbf{L}, n-1\}$,

（2） Use the scalar multiplication algorithm to calculate $R' = k_1 G = (x_r, y_r)$,

（3） Calculation $s = k_1^{-1}(m + kx_r) \pmod{n}$,

（4） The signature of the output is $m' = (m, \mathrm{R}', s)$.

Where m and s are integers and R' is the point on the curve E.

Verification of signatures:

（1） Calculation $v_1 = s^{-1}m(\mathrm{mod}\, n)$, $v_2 = s^{-1}x_r(\mathrm{mod}\, n)$,

（2） Calculation $V = v_1 G + v_2 P$,

（3） When $V = R'$, we claim the signature is valid.

After the encryption algorithm is determined, we want to ensure that the valid signatures is verified, and the invalid signatures can be filtered out during the validation process.

Substituting $v_1 = s^{-1}m(\mathrm{mod}\, n)$, $v_2 = s^{-1}x_r(\mathrm{mod}\, n)$ into $V = v_1 G + v_2 P = s^{-1}mG + s^{-1}x_r P$.

Because $P = kG$, $V = v_1 G + v_2 P = s^{-1}mG + s^{-1}x_r P = s^{-1}(m + x_r k)\mathrm{G} = k_1 G = R'$. So the correctness of the signature is proved.

RFID security middleware model

Traditional middleware can be divided into four parts, which are data layer, implementation layer, service layer and application layer according to the different functions. In order to improve the security of RFID middleware, in this paper we divide the implementation layer into four different functional modules according to functional modules. The security middleware model of the improved RFID system is shown in the Fig. 2:

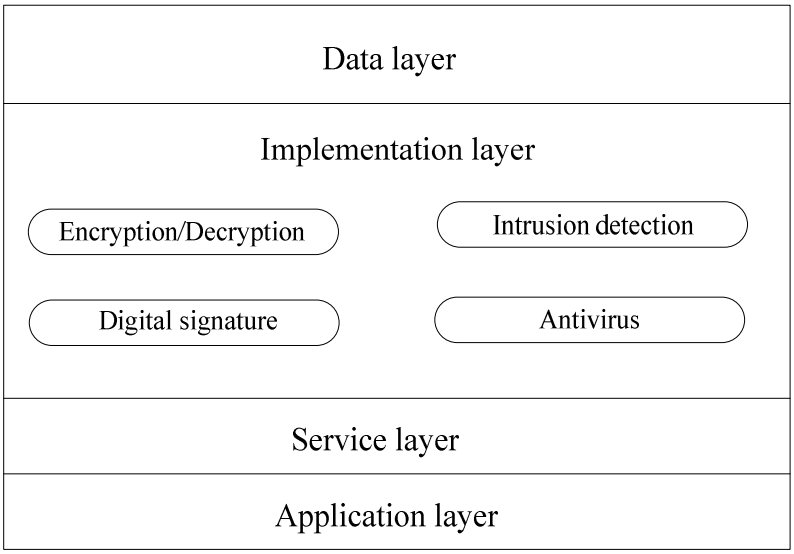

Fig. 2 Security Middleware Model of RFID

The data layer can collect information according to the request of different users, and it can ensure the confidentiality of information and transmission efficiency at the time of information transmitted. It is the main aspects to achieve the function of cache, aggregation, filtering and collection of information. When the signed information firstly arrived at the data layer through the middleware with the reader, and it is stored in the date layer.

The implementation layer is the main level to achieve of RFID systems and it provides an important guarantee for the user authorization at the same time. The implementation layer decrypts the information received from the upper layer and verifies the identity of the user who sent the message. Though this, it can make sure that among the authorized users, they can only access authorized information. Though the partition of the functional modules, we divide the implementation layer into four modules: Encryption or decryption module, it can encrypt and decrypt the information to improve the security of middleware; A digital signature module that authenticates the signed information to ensure the authenticity of the information source; the intrusion detection module can detect the information carrying virus and the malicious access; Anti-virus module, when the information carrying virus or the malicious access are detected, starting this module can ensure the security of the middleware. Here we mainly use the digital signature module. In the digital signature module of the RFID system middleware, we add a verification algorithm for the digital signature. We say that the identity of the signer is valid if the signature can be output. On the contrary we say that the signature is ineffective when the signature can't be output.

The service layer is the transit of the implementation layer and the application layer. It greatly reduces the complexity of middleware. It can call the underlying module for the received request and replace the module without affecting the system. After outputting the effective information to the service layer, the service layer can call the appropriate underlying module according to different types of information for it. So that it can reduce the complexity of middleware.

The application layer may provide the interface of the next user and transmit the information processed by the middleware to the user of the connection interface. If the information is transmitted remotely, it is filtered by the manager during the transmission process. The manager needs to connect the middleware to ensure the security of the requested data transmission [12].

Security Analysis and Application Based on ECDSA Middleware

The improved RFID security middleware divides out the digital signature module in the implementation layer. We have embedded the verification process of the elliptic curve digital signature scheme in the digital signature module. Because the security of the elliptic curve digital

signature scheme is based on the problem of discrete logarithm, the prime field Fq which we choose is big enough to ensure the security of the private key.

When the signed label is close to the reader, the reader will scan the signature information carried by the tag over the wireless channel. At this time if the attacker obtain the label m', which carried by the signature information through the wireless channel. In order to forge a signature, the private key k of the tag must be known, but the private key k is confidential. If the attackers want to speculate the private key though the signed public key and the base point is not feasible too in practice. First when we choose the finite field, we will choose the prime field as big as possible, the difficulty of discrete logarithm problem can greatly enhance the security of the algorithm, so it's almost impossible to speculate the private key though the signed public key and the base point. At the same time in order to ensure the security of the signature, we make sure that every signature has its own random number which is different to others. If we choose the same k_1 as the random number in the signature process of information m_1, m_2, then the two signature information are $m_1' = (m_1, \mathrm{R}_1, s_1)$, $m_2' = (m_2, \mathrm{R}_1, s_2)$. When the attacker intercepts the signatures m_1' and m_2' at the same time, the signed private key k can be obtained by the same R_1 in the signature information, so it is also necessary to select a different random number k_1. The digital signature algorithm relies on the difficulty of discrete logarithm problem, and it can also be well resisted by the Pohlig & Hellman algorithm. The hash value of the information was normally used by encrypted information in a digital signature.

The signature information is stored along the wired channel into the data layer of middleware by readers, and then enters the implementation layer where the digital signature module is validated. When the signature is valid, it will be passed to the application layer through the next port service layer. The valid information after the final processing can be transferred to the appropriate back-end server to be saved, and invalidated information will be discarded.

Conclusion

In this paper, the digital signature algorithm based on elliptic curve is applied to the RFID system, and the signature process of the algorithm is given and the correctness of signature is verified. The improved RFID system can help consumers verify the authenticity of the product well. First of all, we provide different genuine business different private key, the original product information to be signed in the factory is added to the label of goods. When the consumer have bought the goods, they can judge the authenticity of the goods by using the RFID reader to scan the signature code of the goods, in this way it can protect the interests of genuine merchants and consumers.

Acknowledgements

This research was financially supported by Science and Technology Projects of Henan Provincial Department of Education (16A520009, 17A520006), Science and Technology Projects of Henan Science and Technology Department (152102210329, 152107000101, 162102210047, 162102310474).

Finally, thank Yamin li, Zhen Xu and Ping Han for their help in grammar and proofreading. They all supported the publication of this paper.

References

[1] Vegendla A, Seo H, Lee D, et al. Journal of information and communication convergence engineering, 2014, 12(1): 19-25.

[2] Chui, Michael, Markus Loffler, and Roger Roberts. McKinsey Quarterly, 2010, 2: 1-9.

[3] Haidong Yang, Chun Yang. Microcomputer Information, 2008(8): 238-240. In Chinese.

[4] Zhao K, Ge L.A Survey on the Internet of Things Security[C]. Computational Intelligence and Security (CIS), 2013 9th International Conference on .IEEE, 2013:663-667.

[5] Christian Floerkemeier and Sanjay Sarma, An Overview of RFID System Interfaces and Reader Protocols, IEEE International Conference on RFID, 2008:232-240.

[6] Weimin Lang, Jianjun Li. Technical frontier, 2007(9): 55-58. In Chinese.

[7] Yuanchun Zhou, Miao Li. Computer Engineering and Applications, 2002,38(15):80-82. In Chinese.

[8] Zhenhua Ding, Jintao Lin. Computer engineering, 2006, 32(21)：9-11. In Chinese.

[9] IEICE Trans on Fundamentals, 1994 , 77(1):98-105

[10] Dongdai Lin. Algebraic Foundation and Finite Field [M]. Higher Education Press, 2006. In Chinese.

[11] Wang Li. Research and Design of Security Authentication Protocol for RFID System[D]. YangZhou University, 2012. In Chinese.

[12] Xiaoyan Wang. ShangHai Standardization Monthly, 2002, Z2(018):36-39. In Chinese.