An Analysis of RFID (Radio Frequency Identification) Data Transmission Security

Lijie Wang

Chengdu Neusoft University, Chengdu, Sichuan 611844

22863991@qq.com

Keywords: Internet of Things; Data transmission security; RFID tags; Font encryption

Abstract. With the rapid development of Internet of Things technology, the RFID products can be found at every corner of our lives and work. On one hand, they bring us efficiency and convenience. On the other hand, they pose a great threat to our information security. This paper discusses a new encryption method - font encryption. Through the introduction of its working principle, a detailed analysis of its working methods is conducted.

Introduction

RFID products can be found at every corner of our lives and work. On one hand, they bring us efficiency and convenience. On the other hand, they pose a great threat to our information security. Because RFID reads data through radio waves, there is a risk of being intercepted and stolen. This paper discusses a new encryption method—font encryption, which generates a nonsensical content in the terminal by encrypting the original content of the data, and then decrypts and recovers the radio wave by the collector. This paper focuses on its principle, process and scope of use.

What is RFID?

The Concept of RFID

RFID (Radio Frequency Identification), also known as Radio Frequency Identification, identifies and performs data manipulation through radio signals without the need for direct contact between the system and the target.

The radio signal transmits the data on the tag through the radio frequency electromagnetic field to achieve the purpose of identification tracking. The tags are divided into two types: power supply support and no power supply support. No power passes through the electromagnetic field to obtain energy; a power tag must have power support to work. RFID tags contain stored data information that can be identified by long distances and penetration (non-metal material isolation).

Advantages of RFID

①: RFID tags are not limited by shape and volume. The reader can read multiple tags or transponders at the same time.

②: Strong environmental adaptability.

③: The reader scans quickly.

④: It can be read in long distance and through penetrating.

⑤: It can be reused for multiple times.

RFID Security Issues

The RFID system is divided into three parts: tags, readers, and communication channels. Because it transmits through radio waves, it is vulnerable to active or passive attacks. The current security issues are as follows:

① :User information security issues

The RFID tag contains the user's private information and needs to have a secure RFID tag to protect the data of the user and product information.

② :Data authenticity issues

In RFID systems, the identification of electronic tags is very important. It is a very important part of RFID work. Therefore, a malicious attacker can gain profits by obtaining tag content and reconstructing RFID tags.

③ :Security risks in information transmission

The signal transmission between the tag and the reader is via radio waves, so it is extremely easy to be monitored and stolen. According to the methods used by attackers in the signal transmission process, they can be divided into active attacks and malicious attacks.

④ :Data integrity

In the process of RFID data communication, how to ensure that data is not tampered with by attackers? It is currently achieved through digital signature technology. In the RFID system, a hash algorithm of the shared secret key is used to perform data integrity checking. The shared secret key and the authenticated message are linked together and hashed at the data receiving end, and any changes to the data during the data collection are performed. Impact on message authentication.

⑤:Malicious tracking

RFID is low cost and very popular, most people can make tags and use readers to track, plus RFID tags that are affected by the environment, small size, automatic acquisition of information and other characteristics are used to maliciously track hidden security risks have become more prominent.

Solutions to RFID Security Issues

There are two main methods for securing RFID systems: physical methods (kill commands, electrostatic shielding, blocking tagging methods) and security protocols (hash locks).

Physical method

① Kill command

The Kill command is a method of physically destroying an RFID tag so that it is not read by the reader. This command solves the security problem of RFID tags and also makes RFID not reusable. This command is only an 8-bit security mechanism and it is easy to decipher. Therefore, the kill command is not an effective solution to RFID data security.

② Metal shielding method

The method of metal shielding is to shield the electronic tag with metal equipment such as metal mesh or metal sheet. This method requires the addition of a metal device, and will affect the normal use of the RFID tag, at the expense of the long-term penetration of the RFID tag and its small size. Therefore, the method of electrostatic shielding is not an effective and widely used method for securing RFID data.

③ Block tag method

The Blocker Tag method is a method for protecting user information security by preventing the reader from reading the RFID tag, and it is a method of passive interference. The normal use of other RFID tags within the range protected by the Blocker Tag will also be affected. Therefore, it cannot be used effectively and widely to protect user's information security.

Security Protocol

There are two methods of hash locks used in RFID tags today: constant read control hash locks and random read control hash locks. In the method of reading the hash lock, the required metal ID is fixed. When communicating, the metal ID is verified to be consistent. If it is consistent, the tag will send the message to the reader. If it is inconsistent, the tag will not send the data to the reader. Although the information security during the transmission process can be guaranteed, since the metal ID is fixed and invariable, it is easy to be traced maliciously. Randomly reading control hash lock means that the metal ID is randomly changed. The method can not only solve the security problem in the transmission but also solve the maliciously tracked problem. However, because the key is randomly changed, more calculations and data are needed in the communication process, so this method is not applicable to a large number of RFID tags.

Conclusion

The above introduces the advantages of RFID, the security issues it faces, and the main technologies and methods for securing RFID information (protecting valid and correct data). Next, we will discuss how to ensure information security with another approach.

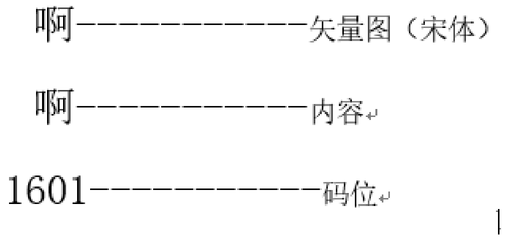
Font Encryption

What is font encryption?

Font encryption is also called content encryption. A piece of valuable and interesting content is encrypted into a piece of meaningless chaos written in the RFID tag. After the reader receives the data, it can decrypt the corresponding decrypted file.

How Font Encryption Works?

Fonts are the type of fonts that we need to use in our work. They can be understood as a vector set containing the following relationships. The font document is parsed as follows (Figure 1).



啊————————矢量图（宋体）

啊————————内容

1601————————码位

Figure 1 Font document analysis diagram

The font effects and content in the application are actually vector maps. The storage of daily files (word, email, etc.) is the font name and “code position information”. When the file is opened, the code position information and the font name are read to display the text content. The code position information is a content composed of digits, and the corresponding vector diagram is displayed by comparing the code points.

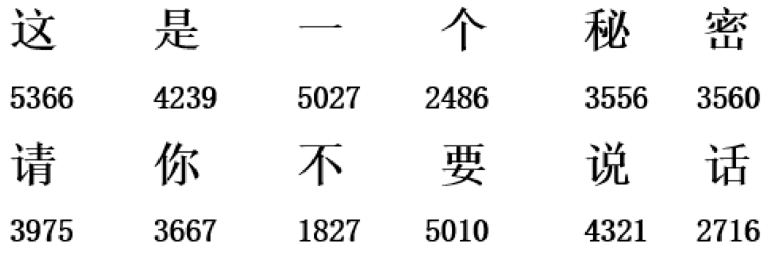
Font encryption method

How to encrypt data through this principle? The following two methods have their own advantages and disadvantages.

Method one, custom privatized character set encoding standard.

Method two, content mapping method.

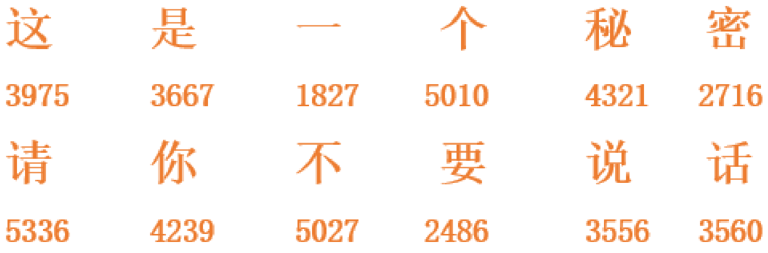
Develop a privatized character set coding standard. Use professional font tools to change the corresponding relationship between code points and text specified in the national standard. For example, according to the GB2312 standard, the text “This is a secret” is a comparison between the characters and code bits in the standard (as shown in Figure 2 GB2312 Partial Text Code Bit Correspondence Table). The code bit information stored in the document is “536642395027248635563560”. The correct data of “This is a secret” can be obtained by decoding this code position information through any computer.



这	是	一	个	秘	密
5366	4239	5027	2486	3556	3560
请	你	不	要	说	话
3975	3667	1827	5010	4321	2716

As shown in Figure 2 GB2312 partial text code bit correspondence table

Adapt the correspondence between text and code bits by customizing the privatized character set coding standard. As shown in Figure 3 Font Encryption Standard Comparison Chart, when the “This is a secret” message is output, the stored code point information is “397536671827501043212716”. When the code bit information is decoded by other devices, the read content is “please do not speak”. When interpreted by a device that also uses the private character set encoding standard, it is correctly interpreted as “This is a secret”.



这	是	一	个	秘	密
3975	3667	1827	5010	4321	2716
请	你	不	要	说	话
5336	4239	5027	2486	3556	3560

Figure 3 Font encryption standard comparison chart

Font mapping. This method does not need to change the corresponding relationship between the character set and the information encoding, and only needs to change the bitmap content corresponding to each Chinese character code bit, as shown in the following figure 4.

Please do not speak - Vector illustration
Please do not speak - Text
5336 4239 5027 2486 356 3560 - Code position

Figure 4 Font mapping method

The vector content corresponding to the Chinese character code bit is set to be different from the original content, and the correspondence relationship between the vector content and the original content is obtained, and a corresponding table of the vector image and the text is created.

When you output "please don't talk", first look up the correspondence between each word in the table. According to the GB2312 standard, what we actually output at this time is “this is a secret” (error message), and the code bit for storing its contents is "533642395027248635563560". When this piece of information is decoded by other computer devices, the content obtained is "this is a secret" (error message), and the device that uses the font can only obtain the correct content “please do not speak”.

How to make font encryption?

Due to the special expertise and tools required by Method 1, it is impossible to explain in detail here. This paper only explains method 2.

There are many font production tools. This paper describes the software CoreIDraw.

Start CoreIDraw, draw the figure to be used as a font, and combine the object as a single character into a single object using a welding or combination tool. After all the redemption combination operations are completed, select an object to be a character. Taking GB2312 as an example, a total of 6763 Chinese characters and 682 characters are all designed to be completed and exported. At the same time, record the relationship between each font and vector content and the original content of the code, and make a table file. For use in practical work.

Font encryption application

When data is written to the transponder, a customized font file is used to write data. The content to be written is encrypted content. After being received by the reader, the file is decrypted by the font file and the content can be restored.

Advantages and Scope of Usage of Font Decryption

Advantages of Font Decryption

①:There is no need to worry about being intercepted and intercepted during the data transmission process. Without the corresponding font encryption document, the correct information cannot be decrypted and the user's information security can be effectively protected.

②:The production process is simple and easy to operate and can be implemented without professional technical capabilities.

③:High degree of combination, not easy to crack.

Scope of Usage

In military, because of the high security requirements in the military field, font encryption can greatly improve the security of data.

In medical treatment, since medical information contains a lot of sensitive data, the font encryption method can also effectively protect data security in the field.

In individual field, personal information are more complex and sensitive and easily leaked. The use of font encryption can well protect the security of personal information.

In supermarkets, the method of font encryption can solve this problem for malicious scans to obtain competitive business information.

Conclusion

The traditional idea of protecting data security is to secure the correct data through software, hardware, and related protocol algorithms. In this paper, from another point of view, i.e., through the “font encryption” method, the correct data is encrypted into the wrong data, and then the data is saved and transmitted. After the receiving end obtains the data, the data can be decrypted through the “font encryption” document to get the correct data. Even if the other receiving terminal receives the data information, it cannot perform correct decoding and cannot obtain correct data information. It is hoped that this idea and method can provide new ideas for data security of transponders in RFID

References

[1] Qu Junsuo. *Internet of Things Communication Technology*. China Railway Publishing House, 2011, 33~48

[2] Ci Xinxin, Wang Subin, Wang Shuo. *Radio Frequency Identification (RFID) System Technology and Application*. People's Posts and Telecommunications Press, 2007

[3] Zhao Yufeng. *Radio Frequency Identification (RFID) Technology*. Telecommunications Technology. 2005.2

[4] China Standard Press. *Character Sets and Information Encoding*. National Standards Compilation. 1998

[5] Wang Weihong. He Sha. *Fonts • Books • Design*. China Textile Press. 1997.7.3

[6] Peng L, Xiaoping Z. Social Stratification and Cooperative Behavior in Spatial Prisoners' Dilemma Games [J]. PLOS ONE, 2015, 10(7): e0131005.

[7] Peng L, Xiaoping Z. Social Stratification and Cooperative Behavior in Spatial Prisoners' Dilemma Games [J]. PLOS ONE, 2015, 10(7): e0131005.