Design and Implementation of Mobile Commerce Security System Based on SMS

Yan Li
School of business
Jiangxi Science and Technology Normal University
Nanchang, China
E-mail: hanter3@163.com

Lan Bai
Computer and information branch
Jiangxi Modern Polytechnic College
Nanchang, China
E-mail: ilovexz0802@163.com

Abstract—With the popularity of mobile communication technology and mobile terminals, a new e-commerce model---mobile commerce emerges as time requires which has become the focus of e-commerce development research. M-commerce develops rapidly nowadays, yet its security problem has become an important factor which limits its development. This paper designs and creates a M-commerce security system based on SMS while analyzing its security problems, which has theoretical value and significant meaning for guaranteeing the information security throughout the whole process of business activities and promoting its healthy development.

Keywords-Network Security; Mobile Commerce; SMS; STK; Security System

I. INTRODUCTION

Mobile commerce refers to the data transmission via wireless communication networks, which is a new e-commerce module that adopts mobile terminals such as mobile phone and computers to carry out business activities. Its main business activities mainly adopt mobile communication technology and it is characterized by the use of mobile terminals. The wireless communication technology can help realize communication at anytime and everywhere which shall create endless business opportunities. The mobile service range becomes wider and wider with the development of mobile communication technology as well as the sky rocketing mobile users. Except from providing voice service, SMS is also widely adopted which is convenient and affordable. When carrying out trading service with e-commerce and online stock market, the trading security is an issue a glittering array of customers pay attention to. Mobile commerce based on SMS carries out business based on SMS, namely, and develops various applications based on the SMS system.

II. BASIC THEORIES FOR MOBILE COMMERCE BASED ON SMS

A. SMS system structure

SMS operates based on SMSC which is the message storage and forwarding center. The internet defines the Mo and MT between SMSC and mobile terminals. The structure of SMS systemstructure shows in Fig. 1:

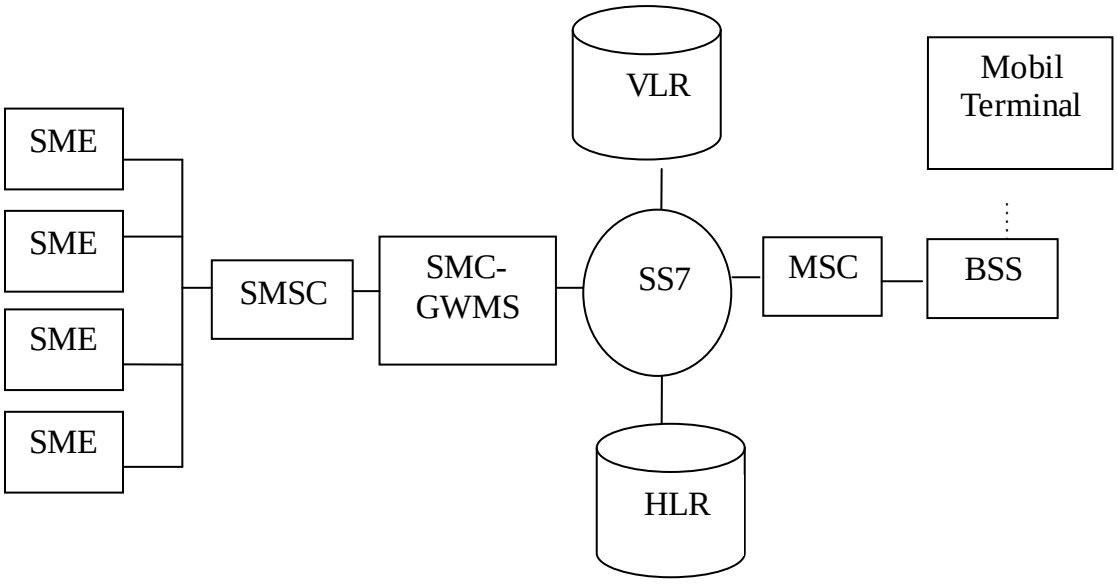

Figure 1. SMS system structure

The entities in Fig. 1 include: SME, SMSC, SMC-GWMS, VLR, HLR and MSC. SME refers to Short Messaging Entity, which is adopted to receive or improve the message, and is located inside the telephone system,

mobile base or other service centers. SMSC means Short Message Service Center, which is responsible for relaying, storing or forwarding messages between SME and bases. SMC-GWMS (SMS Gateway MSC) receives the message sent by SMSC and checks the routing information from HLR and then sends the message to the exchange center. HLR refers to Home Location Register, which is responsible for permanently manage and record the data which is generated by SMSC. SS7 refers to No.7 Agreement on Basic Tele-communications of signaling system, which adopts common channel signaling technology to provide independent packet switched network for signaling service. MSC refers to Mobile Switching Center, which is responsible for system management switching and controlling the connection service between telephone and data system. VLR refers to Visitor Location Register and VLR includes the database with temporary information.

While SMS sends messages to SMSC, it shall transmit the messages to SMS-GWMS and then the gateway checks the HLR to get the routing information, which is sent to MSC to finally get to the targeted mobile station. The application server deals with the customer service request and sends the result to short message gateway, which sends the result to SMSC and finally to the mobile phones of customers.

B. *The basic operating principle of STK*

STK is the abbreviation of SIM Tool Kit, which is used to develop value added service, actually a small programming language that allows SIM to apply its application software.

STK is a 32K card based on Java language platform which can be fixed in the SIM card and is able to receive and send GSM messages. As the connection between SIM card and short messages, it allows SIM card to apply its application software. At present, the regular system adopted in wireless trading system combines SIM and STK, which adopts 3DES encryption as well as MAC testing with friendly interactive interface and is written into STK. The working principle of STK shows in Fig. 2:

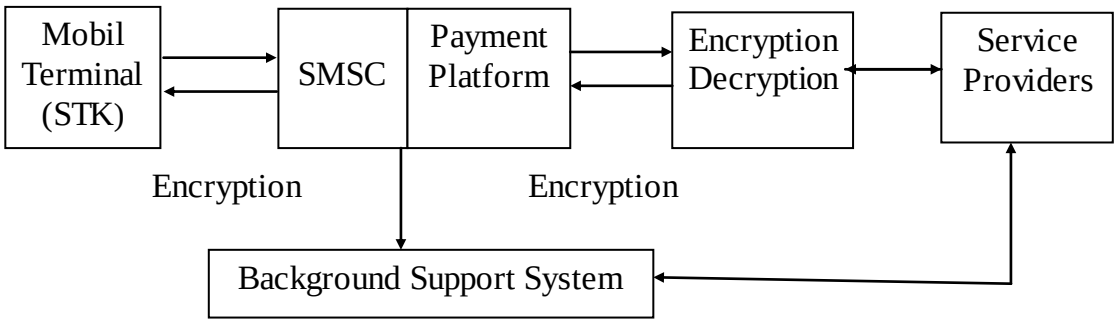

Figure 2. Working principle of STK card

Concerning a concrete short message business, the information data should be transited through GSM and internet. In the course of transiting, the internet should possess SSL and GSM should have security regulations and adopting point-to-point protocol between short message center and short message gateway can solve problems. SSL mainly provides security service for application layer and GSM regulation is mainly used to implement customer as well as internet verification and recognize the networks to ensure whether they are security users; the point-to-point protocol cannot ensure the security in the course of information transiting so the solution plan based on short message should adopt end-to-end solution.

III. THE SECURITY PROBLEMS OF MOBILE COMMERCE BASED ON SMS

The short message system is made up of access part, short message processing center and short message gateway. Therefore, researchers have to start from these three aspects in order to analyze the mobile commerce security problems based on SMS.

A. *The access part*

There are two phases: unlimited access between mobile users and mobile base as well as the wired network between the base and MSC, SMSC. The short message transmission in wireless channel exists in the form of text with wiretapping risk and attackers can wiretap and intercept information or carry out falsification. Even though the short message information transmitting is carried out based on text, the MSC and SMSC are internal networks, which are safe yet cannot guarantee the security.

B. *Short message center*

The security of short message center depends on the short message center and the information connection as well as the short message database. The short message center and short message gateway is connected via SS7 while the short message gateway is connected with short message center through TCP/IP. At present, the safety measures are mature, and the main threat is SMSC database. The database management is an important sector for database security, and the database should not allow unauthorized access and meanwhile operators cannot illegal use information data.

C. *Short message gateway*

Short message gateway is the media connecting short message center and external service provider. On the one hand, SP provides contents to SMSC and the on-demand service is provided to service provider through short message gateway. The network communication in terms of these two aspects adopts different protocols based on TCP/IP and the data confidentiality and integrity are still threatened.

Concerning the integrity of short message system, the protection between the short message center and short message gateway is weak and attackers can record the login password field by using network monitoring. In fact, between the short message gateway and information center, there are firewalls yet the operation is implemented without protection and attackers can counterfeit and enter into the short message center to deal with the short message.

IV. THE SECURITY SYSTEM DESIGN AND IMPLEMENTATION OF MOBILE COMMERCE BASED ON SMS

A. The security system design for mobile commerce based on SMS

The following should be taken into consideration in terms of the mobile commerce security system based on SMS:

Firstly, the system should possess the function to identify authentication and there should be a server between the short message gateway and service provider so as to determine the information source and information status.

Secondly, it should ensure the completeness and efficiency of data communication. By adding some software module as well as encryption technology researchers can test the integrity of short message.

Thirdly, retransmission detection: it can ensure that the information receiver can recognize the information state.

Fourthly: evidence preserving: it can prevent the condition if sender and receiver deny activities which have happened.

Communication safety has two implementation modules: point-to-point security module and end-to-end security module. The bottom encryption technology can only protect communication transmission and cannot guarantee the security of application data. Besides, the mobile commerce of short message cannot adopt point-to-point module which can help avoid the hacking or modifying in the course of trade transmitting.

B. The implementation of mobile commerce based on SMS

In traditional SMS, its server system shall provide relevant services based on the actual service requests. While providing service, the identification shall be confirmed, and users send the ID and password information to the server which may be hacked and intercepted and hackers shall get the information. The approach to prevent the hacking is to encrypt the password information and transmit based on cryptograph. However, this approach cannot prevent replay attack and hackers can steal the cryptograph and they can apply for the service by pass the users off.

In mobile commerce safety system based on SMS, researchers can adopt authentication means concerning the replay attack, namely when the sever responds to the request of users, it shall send a random number or timestamp. When users receive the random number, it adopts the password information to calculate the random number and then send the result to server; if the server receives the result, it adopts the password function to calculate the random number and if the calculation result is same as the result, the authenticity of customers is verified.

The calculation result of random number in the mobile commerce security system based on SMS is the computer information identifying code. The client and server side adopts same identification method, which is the password function. Concerning the same random number, the calculation result should be same. The system structure introduces the short message secure server and the mobile commerce systemstructure shows in Fig. 3:

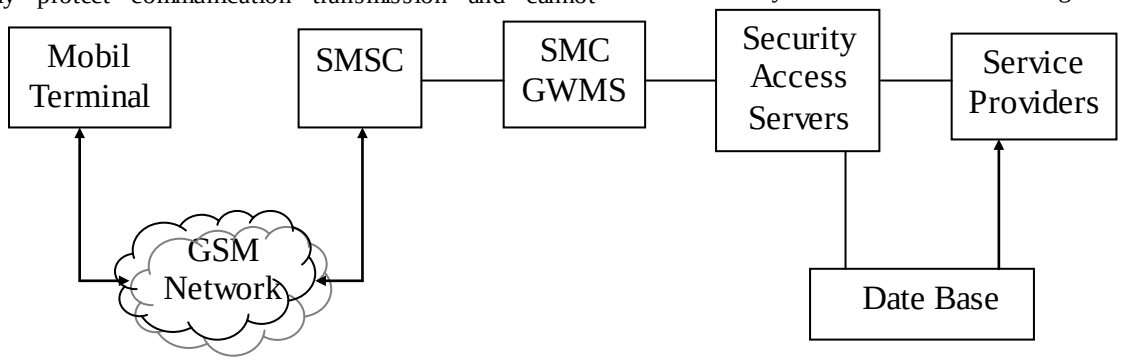

Figure 3. Mobile commerce system structure

As shown in Fig. 3, the Security Access Servers connect the short message gateway as well as the content provider and the information is encrypted. In addition to the encryption function, the short message security server can also test the Mac value so as to guarantee the integrity of information. Besides, the request message and the message format returned to users have serial number and the security server adopts the serial number to synchronize the technology and identify the authenticity. With the expanding of SIM card storage, it supports the OTA (Over the Air) loading mechanism which can timely update the menu.

Message security system can help encrypt and verify the data as well as to encrypt the result. According to the encryption algorithm, researchers encrypt the information so as to verify the authenticity, which can help us to carry out complete and effective analysis on the data.

While carrying out communication between users and service providers, researchers choose the menu of SIM card to input the information in the terminal; the SIM card has been encrypted and the message sent through the SIM card is also encrypted. The message is sent to SMSC and to the short message gateway and finally to the short message security server. When the short message server receives the information, it shall encrypt the information

content and determine the effectiveness of information so as to identify the customers. If the short message is verified, it shall be stored in the Data Base and sent to the server. Once the server receives the customer information and provides information service for customers, the short message security server can identify and encrypt the contents provided by the provider so as to guarantee the integrity of users.

Authentication process:

1. Users input the contents in the mobile which shall be stored in SIM card.

2. The SIM card carries out key dispersion and there shall be a password key K1.

3. SIM card uses K1 to encrypt the contents of SIM card.

4. After being encrypted, the SIM card carries out certification package to calculate the MAC value.

5. Mobile users send Data to the security server.

6. Once the server receives the Data, it shall decompose the keys and there shall be K1 which can test the MAC value. If the result is the same, it can implement the protocol steps and if the result is different, the system indicates mistake.

7. The serve implements the deciphering and stores into the database waiting for the SP application processing which shall be sent to the users.

In addition, the security server will also backup the information because it is important which can be improved.

C. The features of mobile commerce security system based on SMS

The mobile commerce security system based on SMS realizes the verification on mobile terminals, SMS gateway and server-side. The verification on mobile terminal is realized by the SIM card. While implementing the transaction, the operator server obtains the key information of SIM card by operator server so as to confirm the legality of identity; there are various service contents in the system and the short message system implements the CA verification on content server so as to ensure that users can receive the request context.

The mobile commerce security system based on SMS can realize multiple functions, including encryption, authentication, retransmission preventing and log etc. The system carries out encryption between the terminal and short message server so as to realize the privacy. In the course of certification, it adopts a two-way certification mechanism which can synchronize the serial number and can guarantee that the message is sent by the legal users. Concerning the retransmission prevention, this system tests the MAC value results as well as the synchronization state; the log function can be used to check and record the relevant transaction information.

The mobile commerce security system based on SMS has its unique advantages. To begin with, it costs less with diverse service contents which can be realized by SMS; secondly, the mobile terminal is portable and dynamic which can make it easier for users to acquire relevant business information can carry out business activities; finally, the services between users and operators can be customized based on their users' preferences so that the consumption demand can be met.

V. CONCLUSIONS

Mobile commerce security system based on SMS possesses the authentication function and both have regulated password keys and can confirm the identity; based on MAC value testing, it can guarantee the integrity of information; in the course of information transmitting, researchers encrypt the information which can prevent the retransmission attacking. Adopting MAC value testing and serial number synchronizing judgment can avoid resources wasting. The mobile commerce security system based on SMS can help establish safe and convenient commerce application environment.

REFERENCES

[1] Qin Zheng, Cao Yuhui. Mobile electronic commerce. [M]. Beijing: Tsinghua University press, 2012.113-121.

[2] Zhong Yuansheng. Mobile electronic commerce [M]. Shanghai: Fudan University press, 2012.221-235.

[3] Lv Tingjie. Mobile electronic commerce [M].Beijing Electronic Industry Press, 2011.313-316.

[4] Qin Chengde, Wang Rulin,. Mobile electronic commerce [M].Beijing: People's Posts and Telecommunications Press, 2009.339-341.

[5] Yang Qing etc. Principle and application of mobile commerce [M]. Beijing: Tsinghua University press, 2006.251-283.

[6] Yuan Yufei etc. Mobile commerce [M]. Beijing: Tsinghua University press, 2006.239-257.

[7] Qiu Huimin,Hu Chunyang. Analysis on the risk of short message security problem based on GSM [J], Computer and modernization, 2014, (12)

[8] Shu Kai. Research on the information security standards of e-commerce[J]. Standards and technology tracking, 2014, (8).

[9] Wang Weiguo. Security solution for mobile commerce [J]. Modern communications, 2013, (10).

[10] Qiu Huimin, Qin Lijin . Security framework mode for mobile short message content [J]. Computer security, 2012, (8)

[11] Tian Yinghua, Yang Jingsong, Zhou min. Research on the security problem of mobile commerce in 3G era [J]. Information science, 2010, (10).