Research on Security Design of Electronic Commerce System Based on Android Platform

Yangxia Shu

Business School, Jiangxi Institute of Fashion Technology, Jiangxi, China

Keywords: android platform, electronic commerce system, security design.

Abstract: With the popularity of the Internet, e-commerce has been fully developed over the past few years, especially Android mobile devices emerge in endlessly, mobile e-commerce has become a trend of development. At the same time, the development of electronic commerce has brought great influence to our life and put forward higher requirements for transaction security. This paper will study the security design of e-commerce system based on Android platform.

1. Introduction

In recent years, with the popularity of computers, smart phones and the Internet, people's consumption habits have changed in an subtle manner. From physical stores to online shopping, we utilize computers to buy everything in the mall. With the popularization of the Internet, e-commerce has been developed in an all-round way, especially the mobile e-commerce on Android mobile devices has become a trend of development. Like Internet electronic commerce, mobile electronic commerce is attached to information technology, mobile terminal technology and Internet network technology. It integrates management information, office paperless, financial electronization and commerce information networking to realize the new trade model integrates the logistics, commercial flow, capital flow and information flow. Due to the wireless communication access mode is very flexible, and the network has the characteristics of openness, low cost, global and high efficiency, mobile e-commerce proposes higher requirements for security design. Although wireless communication technology adopts security technology such as transmission encryption protocol and CA authentication signature, there are still some mobile terminals being stolen and counterfeit, so the problems of communication disclosure and transaction denial occur. Therefore, this paper will study the security design of e-commerce system based on Android platform.

2. Construction of the Network Communication Module

Based on Linux, Java, Android adopts software stack architecture, which is divided into three parts. The underlying work uses the Linux kernel to provide only the most primitive functions; other applications are developed according to the user's own needs, and the program development is based on Java. The communication between Android and server is mainly based on http communication or Socket communication and socket provides a special channel for data transmission between the two parties. Based on electronic commerce, the communication between Android client and server is connected through TCP protocol family. The main Socket type in this

protocol family is streaming socket and Datagram socket. Streaming socket uses TCP as its end-to-end protocol, thus establishing a reliable byte stream service, and finally implementing data communication based on extensible markup language (XML, Extensible Markup Language). XML data is stored in full text format, which is a kind of shared data method which has no relation with software and hardware. So XML is introduced into many network protocols in order to provide a better standard method to communicate with software. The architecture of the server and client is shown in Figure 1.

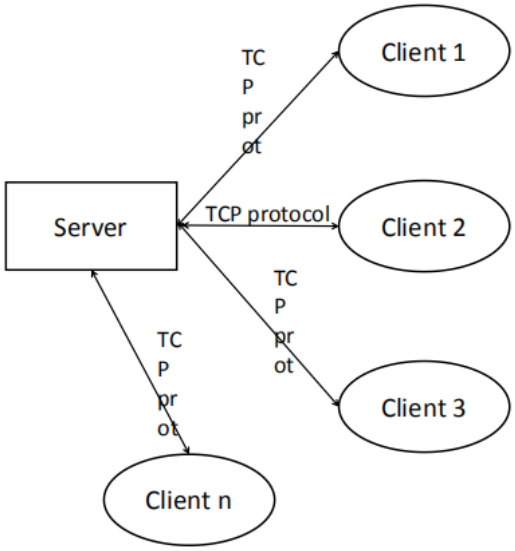

Figure 1: Block diagram of server and client architecture.

The communication protocol between client and server is mainly implemented by Client_Info class (Msg class of user information) and Msg_Type class (enumeration of message type). The Client_Info class (user information class) describes the user identification, user name and password communicated through the server, and the Msg class describes the data type and information mode of the communication between the client and the server.

3. Common Security Problems in Mobile E-commerce

Under the background of mobile e-commerce, fraud, tampering, privacy information leakage and other problems occur from time to time. Although people have access control specifications in the MAC layer and data have encryption mechanisms, PKI provides a series of technologies related to encryption and digital certificates. However, it is difficult to realize PKI in the wireless e-commerce communication environment.

3.1. Terminal Access Layer Security

The terminal access layer here mainly refers to mobile devices based on Android platform, user interface. The main manifestations of the security problems that have arisen are: First, the mobile terminal processing capacity is weak. Due to its small size and limited configuration, mobile communication terminals have low processing capacity, slow data transmission and are affected by geographical location signals, which lead to the limitation of electronic commerce transactions and the existence of certain security risks. Second, the mobile terminal SIM card is copied. In the process of electronic commerce transaction, SIM card is used to authenticate the user, the mobile device is lost, the outsider can attack with the important information in the SIM card, at the same

time, pretend to be the real user to participate in the electronic commerce activity to carry on the deception.

3.2. Communication Link Layer Security

The function of communication link layer is to provide many communication networks for mobile e-commerce transactions. The biggest difference between mobile wireless network and wired network is that it is not restricted by geographical environment, but it is prone to eavesdropping, tampering, counterfeiting, replaying and so on.

3.3. Application Service Layer Security

The function of the application service layer is to provide the services about mobile e-commerce transactions to the final consumer. The security problems mainly focus on the authentication and non-repudiation characteristics of the mobile e-commerce services. At present, the authentication feature of mobile e-commerce business is based on user name and static password. The problem of such authentication is poor security, user accounts and passwords are easily stolen and forged.

4. Security Strategy of Electronic Commerce System Based on Android Platform

4.1. Mobile Terminal Layer Design

One is to increase the capacity of SIM cards. With the increasing integration of the internal motherboard of the intelligent mobile device and the more powerful resource processing ability of the hardware, people are making use of the intelligent mobile device to do more and more things, including storing more and more information and application services. However, the current problem is that battery life technology can not break through the technical bottleneck in a short period of time, so it can only be treated by reducing the area of SIM card, increasing the capacity and extending the existing capacity of SIM card to 1G or more. Second is to strengthen the ability of SIM encryption. With the development of computer technology, its computing ability is becoming higher and higher, and the previous encryption technology is also easy to be brutally cracked, such as: DES encryption is cracked, so in order to enhance the security of data, we must improve the encryption technology ability. The 3DES encryption algorithm is embedded into the SIM card, which can make the end-to-end mobile e-commerce security come true. 3DES (Triple DES) technology is a symmetric algorithm based on DES, that is, to encrypt a piece of data three times with three different keys to improve the encryption ability. Third, the use of mobile phone anti-theft subsystem. The main function of the system is that the mobile terminal and the dynamic password generator are used together. When the mobile terminal is lost or stolen, the SIM card is easily copied and the identity of the mobile e-commerce participant is fake. Using this function can physically isolate the loss of mobile terminal or the risk of SIM card being copied in the process of electronic commerce transaction, because in the aspect of identity authentication, not only the user name and static password mechanism are required, dynamic passwords are also needed for authentication, which can effectively eliminate the risk of counterfeiting. Fourth, strengthen the mobile terminal virus scanning function. The security of mobile terminals is a matter of great concern to users. They should be vigilant at any time. Whether the mobile terminal has been infected or not is concerned about whether its information is leaked, including its location, its own chat content, pictures, videos and other information. Using virus scanning function, click scan, mobile terminal system can automatically scan all applications.

4.2. Enhancing the Security of Communication Link Layer

In order to avoid the problem of eavesdropping or intercepting in the process of network transmission, we can set the functions of file encryption, file digital signature, file decryption, file signature verification and program locking. Firstly, file encryption between physical communication links. The physical communication link layer implements a point-to-point security model. File encryption begins before the end of the link layer and the beginning of the physical layer. File encryption protection is only point to point security, for the message on the host node as clear text, this requires end-to-end encryption. Second, file encryption in the gateway protocol layer. Gateway protocol layer implements end-to-end encryption security. End-to-end communication between the two sides of e-commerce transactions is guaranteed. Before all kinds of information transmitted into the communication sub-net, the application layer or the presentation layer has been encrypted, and the information in the transmission process of the network exists in the form of ciphertext. It is only when the user reaches the end that it is decrypted to clear text.

4.3. Strengthen the Security Guarantee of Application Service Layer

Identity authentication mechanism and non-repudiation are the problems that must be solved in application service layer. The authentication mechanism is realized by combining dynamic password and challenge. Step: the terminal device initiates the authentication request, then enters the user name and the static password→Authentication server begins to authenticate. First, the user of the user database is queried whether the user is a legitimate user. If the user is not a legitimate user, he does not handle it. The legitimate user generates a random number and sends the text "challenge" to the mobile terminal device.→The mobile terminal device combines the user name with the random number, generates a string with a single Hash function, encrypts the string with a dynamic password, and returns the encryption result to the server→The authentication server uses the same time-based cipher algorithm to calculate the dynamic password, which is then used to decrypt the received response.→The authentication server starts to verify, if the decryption result is the same as its calculation result (Hash value), the authentication passes; otherwise, it fails.

References

[1] Qi Jing Design of Telephone Software Module Based on Android Platform [D]. Harbin Institute of Technology, 2013

[2] Xue Libin Research on Security Technology of Smart Phone Based on Android Platform [D]. Qinghai Normal University 2014

[3] Wang Jiaxu. Research on Application Development of Smart Phone Based on Android [J]. Computer CD Software and Applications 2014 (22)

[4] Wang Jiaxu. Research on Application Development of Smart Phone Based on Android [J]. Computer CD Software and Applications 2014 (22)

[5] Pan Gangchao, Jiao Jiapeng, Ye Ping. Development of Campus Electronic Commerce Platform Based on Android System [J]. Computer Programming Skills and Maintenance. 2015 (03)