2019 9th International Conference on Education, Management, and Computer (ICEMC 2019)

Analysis on Key Role of Wap and WPKI Technology in Construction of Mobile E-commerce Security Model

Qing Tan[a], Wuchao Zhao

Luoyang Normal University Luoyang, China

[a] Corresponding author: edutanqing@163.com

Keywords: Mobile E-commerce; Wap; WPKI; Information safety; GPS

Abstract: The security architecture of mobile electronic commerce consists of the following five parts: mobile bearer layer, encryption layer, security authentication layer, security protocol layer and application system layer. Mobile e-commerce technology based on WPKI is a perfect and feasible scheme at present. WAP is one of the core technologies of mobile e-commerce. WAP, mobile phone can connect to the Internet anytime, anywhere, conveniently and quickly, and realize the mobile electronic commerce which is not restricted by time and region. The paper presents analysis on key role of wap and WPKI technology in construction of mobile E-commerce security model.

1. Introduction

The main characteristic of mobile e-commerce is flexible, simple and convenient. It can be customized according to the individual needs and preferences of consumers, and the choice of devices and the way of providing services and information are entirely under the control of the users themselves. Through mobile e-commerce, users can access the required services, applications, information and entertainment anytime and anywhere. They can use their Smartphone's or PDA to find, select and purchase goods and services at their convenience.

There is little need to buy services online at this stage, and there is generally no security for the flow of funds. Security issues become extremely sensitive when mobile e-commerce reaches the second stage of the need to provide online payment services. However, in the mobile environment, the open PKI technology of mobile devices such as mobile phones and data exchange centers is applied in mobile electronic commerce [1]. The unencrypted transmission network between mobile gateway and application service provider creates a security hazard for mobile payment applications.

The content of mobile e-commerce, mobile e-commerce can not only provide direct shopping on the internet, but also a brand-new sales and promotion channel. It fully supports mobile Internet services and enables electronic payment of telecommunications, information, media and entertainment services. Mobile e-commerce is different from the current sales mode; it can fully meet the personalized needs of consumers. The combination of Internet and mobile communication technology creates new opportunities for service providers to provide diverse and fast services according to their location and personality, and to exchange information with customers frequently, thus strengthening their contacts with customers.

The first-generation mobile e-commerce technology based on short message has many serious defects, among which the most serious problem is that the real-time performance is poor, and the query request will not be answered immediately. In addition, some queries cannot get a complete answer because of the length of short message. These intolerable problems have also led some early users of SMS mobile e-commerce systems to demand upgrades and revamping of existing systems.

Different from the past, the quantity of products produced in the past need to be estimated, too much too little will have a negative impact. The production mode of the intelligent factory of mobile electronic commerce is to place the order first for the customer. After the enterprise receives the order, it can adjust the production line according to the different demand of the customer. Therefore,

DOI: 10.25236/icemc.2019.111

the enterprise can produce on demand, reduce the unnecessary waste of production capacity and insufficient problems caused by the miscalculation of sales volume, and improve the production efficiency. At the same time, the mode of the intelligent factory of mobile e-commerce integrates the logistics system, which can make the production to the logistics distribution one-stop, thus reducing the pressure of the enterprise inventory and saving the cost.

As soon as smartphones began to enter people's lives, those e-commerce platforms sniffed unlimited business opportunities from there with the unique sensitivities of businessmen, because mobile phones were a mass product and closely related to public life, except for children and the elderly. Basically, people all have one or two mobile phones. Mobile phone users with huge numbers of data present unlimited business opportunities. As a result, the major e-commerce operators rush forward, from JingDong Mall to Taobao, Tmall. While opening mobile electronic commerce, Ali and others also set their sights on those social products that can bring extraordinary traffic. Among them, Tencent WeChat, Weibo, Youjia and other community products are the most attractive.

The card number of SIM card is the only one in the world. Each SIM card corresponds to one user, which makes SIM card become a natural identification tool for mobile users. It can also store the bank account of users by using programmable SIM card. CA certificates and so on used to identify the user's valid credentials. It can also be used to implement digital signature, encryption algorithm, public key authentication and other necessary security means in the field of electronic commerce. With these means and algorithms, we can carry out a wider range of e-commerce applications than in the field of Internet.

2. Interaction of Mobile E-Commerce Based on Key Technologies of WPKI and WAP

WAP (Wireless Application Protocol) is a global network communication protocol. WAP is a common standard for mobile Internet. Its goal is to introduce the rich information and advanced services of Internet into wireless terminals such as mobile phones. WAP defines a general-purpose platform and converts the information from the current HTML language on the Internet network into the information described in WML (Wireless Markup Language). WAP only requires support for mobile phones and WAP proxy servers, and does not require any changes to existing mobile communication network protocols.

WPKI system is mainly composed of entity terminal, PKI portal, CA, PKI directory server and so on. In the application mode of WPKI, it also includes data provider server, WAP gateway and other service devices [2]. The basic structure and data flow of WPKI system. Terminal entity application program EE (wireless user). Terminal entity application is optimized software designed to run WPKI in WAP devices. It relies on WMLScryptAPI to implement digital signature key management and encryption operation.

Mobile IP realizes seamless roaming of mobile computer in Internet by changing IP protocol in network layer. Mobile IP technology enables a node to switch from one link to another without changing its IP address or interrupting ongoing communications. Mobile IP technology can support the application of mobile electronic commerce to some extent, but at present it also faces some problems, as is shown by equation(1), where m is such as the triangular path problem when mobile IP protocol is running, the security and power consumption of mobile host, and so on.

$$\begin{aligned} P^{(\chi)}(m+1|m) &= \Phi(m)P^{(\chi)}(m,M)\Phi^{T}(m)+\overline{Q}(m) \\ &= \Phi(m)P^{(\alpha)}(m,M)\Phi^{T}(m)+\overline{Q}(m) \\ &= P^{(\alpha)}(m+1|m) \end{aligned} \tag{1}$$

The security of mobile e-commerce faces several challenges, including terminal theft and counterfeiting, wireless network eavesdropping, retransmission of transaction information, man-in-the-middle attack, denial of service, trade denial, loss of mobile terminal, etc. To solve the security problems of mobile electronic commerce, there are mainly end-to-end policies, encryption technology, firewall, strict user authentication, single login, wireless PKI technology, authorization and secure transaction flow.

Mobile customer base: only a small number of leading fashion people will be experimenting with mobile e-commerce services, and the range and quality of services at this stage will be limited. The price of the mobile terminal and the cost of the e-commerce service are on the high side, so the acceptance of the mobile e-commerce service in the vast consumer market is generally low, and many people hold a wait-and-see attitude.

In the application model based on WAP, WPKI plays a key role in the operation of security protocol [3]. Applications based on WAP can usually be combined with WTLS (WirelessTransportLayerSecurity) to complete authentication, encryption, digital signature and other functions. (2) STK (SIMcardToolKit), a short message application model based on STK, is a small programming language. STK card is a kind of SIM card. Unlike SIM card, STK card allows the user identification module (SIM card) in mobile phone to run its own application software. STK card has a lot of flexibility. All kinds of services can be developed on the user's STK card and cooperate with the server. In use, STK technology is usually combined with OTA (OverTheAir, aerial download technology to update and upgrade the applications and various services in the STK card at any time.

WSP (Wireless Session Protocol): wireless session layer protocol. Provides connection-oriented, WTP based session communication services or WDP connectionless, reliable communication services for upper WAP applications. WTP (Wireless Transaction Protocol): wireless transaction protocol. WTLS (Wireless Transport Layer Security): wireless transport layer security protocols for wireless data networks. Secure transport protocol based on SSL, as is shown by equation (2), where n is providing encryption, authorization and data integrity.

$$\begin{cases} w_{j,\min}^{\xi}(m,n) = \frac{1}{2} - \frac{1}{2}\left[\frac{1-M_{j,AB}^{\xi}(m,n)}{1-T}\right] \\ w_{j,\max}^{\xi}(m,n) = 1 - w_{j,\min}^{\xi}(m,n) \end{cases} \tag{2}$$

Security is the key problem affecting the development of mobile electronic commerce: compared with the traditional mode of electronic commerce, the security of mobile electronic commerce is weaker. How to protect the user's legal information (account, password, etc.) from infringement is an urgent problem to be solved. In addition, at present, our country should also solve the electronic payment system, commodity distribution system and other security issues. According to the characteristics of mobile electronic commerce, we can develop portable and efficient security protocols, such as application-oriented encryption (such as electronic signature) and simplified IPSEC protocol.

WTLS certificate has the characteristics of smaller and simpler. It can not only realize the function of X. 509 certificate, but also be very suitable for handling security problems in mobile terminal. Because the WTLS certificate is a new type of certificate, it is necessary to upgrade the CA certificate to use the WTLS certificate [4]. The mobile certificate identity is usually embedded in a mobile device terminal, and then uniquely corresponds to a standard X. 509 certificate, where the user sends the mobile certificate identifier together with a certificate containing its own signature data. According to the mobile certificate submitted by the user, the other party inquires the digital certificate into the CA center to complete the authentication of the user. The use of mobile certificate identification does not require changing X. 509 certificates and requires only a very small amount of storage space, generally requiring only a few bytes.

3. Development and Security Strategy of Mobile E-Commerce

The user-oriented business needs to be improved and strengthened: in terms of current applications, mobile e-commerce applications are more focused on individual applications such as access to information, ticket booking, stock speculation, and lack of more and more attractive applications. This will undoubtedly restrict the development of mobile e-commerce. Improve the design of mobile terminals: in order to attract more people to engage in mobile e-commerce activities, it is necessary to provide convenient, reliable and multi-functional mobile devices. For example, WAP-based applications must be easier to operate than PC (like a phone); wireless devices with WAP only allow for lower cost increases.

Mobile e-commerce enables users to safely manage their personal finances on the Internet at anytime, anywhere, and to further improve the Internet banking system. Users can use their mobile terminals to check their accounts, pay bills, transfer money and receive payment notifications. Booking, booking tickets, tickets or tickets via the Internet has grown into a major business and continues to grow in size [5]. The Internet helps to check the availability of tickets and purchase and confirm tickets.

It has the characteristic of being everywhere, anytime, anywhere. The biggest characteristic of mobile e-commerce is "freedom" and "individuation". The traditional electronic commerce has made people feel the convenience and happiness brought by the network, but its limitation is that it must be connected by wire, and the mobile electronic commerce can make up for the shortcoming of the traditional electronic commerce. Allows people to check out, book tickets or shop anytime, anywhere, and experience unique business experiences.

First, multilevel dealer price increase is the main reason why the price is far from the production cost. And the model of the mobile e-commerce intelligent factory solves this problem perfectly. Consumers can communicate directly with the manufacturers, thus eliminating the steps of multi-layer dealers in the middle. Merchants will lower the price in order to obtain a more competitive price to seize the market, forming a price advantage; In this era of channel king, mastering the channels of production and sales, became the rules of the game.

Mobile e-commerce is a new development direction of e-commerce and an important part of national economy and social informatization. In recent years, the construction of mobile electronic commerce in China has made remarkable achievements in product innovation, as is shown by equation (3), where M is product operation and resource integration and so on. Mobile e-commerce business has been widely carried out, and has created enormous economic benefits. At the same time, the huge population of mobile phone users and the rapid growth of mobile phone users provide a broad market basis for the development of mobile electronic commerce.

$$M_{j,AB}^{\xi}(m,n)=\frac{2\sum_{m'\in J,n'\in K}\left|w^{\xi}(m',n')D_{j,A}^{\xi}(m+m',n+n')D_{j,B}^{\xi}(m+m',n+n')\right|}{E_{j,A}^{\xi}(m,n)+E_{j,B}^{\xi}(m,n)} \tag{3}$$

Compared with wired channel, the limitation of wireless spectrum and power makes the bandwidth smaller and the bandwidth cost higher. Meanwhile, the development of packet switching makes the channel become shared, and the delay is longer. Connection reliability is low, beyond the coverage area, the service denied access. Therefore, service providers should optimize the use of network bandwidth and increase network capacity to provide more reliable services.

Mobile MIS is to use mobile communication and mobile Internet technology to enable enterprise management information systems to directly connect decentralized customers, partners and employees through mobile communication networks to help enterprises develop their daily work more quickly and efficiently. Achieve cost savings; improve efficiency, increase revenue and other purposes of the system. At present, specific mobile MIS applications include mobile OA, mobile HR, mobile CRM, mobile SCM, and mobile ERP and so on.

At present, China's mobile phone users have reached nearly 400 million, the largest in the world. Obviously, in terms of the popularity of computers and mobile phones, mobile phones are far more popular than computers. From the perspective of consumer users, mobile phone users basically include high-end users with strong spending power, while traditional Internet users are mainly young people who lack the ability to pay. It is not difficult to see that the mobile electronic commerce with mobile phone as the carrier is superior to the traditional electronic commerce in terms of the scale of the users and the ability of the users to consume.

Compared with the traditional e-commerce, mobile e-commerce has the advantage of flexibility, and the development of services based on GPS also makes the rapid rise of mobile e-commerce, as an Internet company with physical industries, After occupying certain channels, they can provide services other than products, perfect the company's electronic commerce system, upgrade service standards, such as selecting closer logistics outlets for customers, so as to gain more profits, and at the same time accumulate more customers.

Mobile payment is an important goal of mobile e-commerce. Users can complete the necessary electronic payment service anytime and anywhere. There are a variety of mobile payment classification methods, among which the more typical classification includes: according to the amount of payment can be divided into micro payment, small payment, macro payment, according to the location of the transaction object can be divided into remote payment, face to face payment, Family payment, according to the time of payment can be divided into pre-payment, online instant payment, offline credit payment and so on.

4. Key Role of WAP and WPKI Technology in Construction of Mobile E-Commerce Security Model

The mobile environment is more open than the wired environment, which causes people to worry about the security of trading through the wireless environment, when people trade through the wireless way, Only when all users are convinced that the transaction information will not be eavesdropping and tampering, the authenticity and legitimacy of the transaction can be effectively protected, mobile e-commerce will be accepted and promoted by more people. , PKI (Public key Infrastructure (PKI () is an important security guarantee in wired network e-commerce transactions. PKI effectively solves the problems of information security, identity proof, information integrity and non-repudiation, etc. It plays an irreplaceable role in wired e-commerce transactions, and its significance in ensuring transaction security has been generally recognized.

Because WAP is based on scalable hierarchies, each layer can evolve independently of the others. This allows for the introduction of other bearer services or the use of new transport protocols without having to change other layers. WAP enables users who hold small wireless devices such as mobile phones and PDA that can browse Internet WAP takes into account the limitations of those devices and the flexibility of these users [6].

(MASP): a mobile application service provider requires some industries to send engineers or workers to the site regularly. In these industries, mobile MASP will have huge application space. MASP combines location service technology, short message service, WAP technology and Call Center technology to provide timely service for users and improve their working efficiency.

First, online marketing means are diverse, Internet companies with many years of e-commerce experience know how to please consumers; second, the accumulated years of e-commerce activities data old e-commerce companies know how to use them; third, the management of Internet companies and manufacturing is very different, so we still have deficiencies in the management of e-commerce projects. There are two solutions. First, it is looking for a more professional management team to manage our ecommerce projects. Second, train the corresponding talents from within the group, as is shown by equation (4).

$$G_N = \sum_{k=1}^{8} \left| R(k+1) - R(k) \right| = 2, R(9) = R(1) \tag{4}$$

Like Internet e-commerce, mobile electronic commerce needs four basic features (data confidentiality, data integrity, non-repudiation and authentication and authorization of the transactional parties). Due to the particularity of wireless transmission, the existing wired network security technology cannot fully meet the basic needs of mobile e-commerce.

WPKI technology mainly includes the following parts. (1) CA (CertificateAuthority) certification body. The certification body (certification center) is the core part of the PKI and the basis of trust, responsible for the issuance of certificates, (2) (RA). RA is the approval authority for digital certificate registration. RA is the extension of CA certificate issuance. RA is the interface between user and CA. It must not only accept offline certificate applications, but also provide online certificate application services. (3) Smart cards. Smart card is a kind of integrated circuit chip with storage, encryption and data processing capability embedded in plastic substrate. Smart card has strong security in access control, and its size is small, so it is difficult to crack. It has been widely used in various fields.

Mobile terminals under the WAP standard are equipped with a micro browser that works like a card set. Users can browse the various Web services provided by mobile network operators through card groups. When working, the mobile terminal user first selects a service, which will download the card group to the mobile terminal, and then the user can browse between the cards, select, arrange or input information, perform the selected work, etc. Furthermore, browsing information can be cached for later use, and card sets can be cached and bookmarked for quick retrieval. The browser also provides support for the format of electronic business cards, calendar events, online address books, and other types of content.

As a new type of electronic commerce, mobile e-commerce takes advantage of the advantages of mobile wireless network and is a useful supplement to traditional e-commerce. Although there are still many problems in the development of mobile electronic commerce, such as security and bandwidth, compared with the traditional electronic commerce, mobile electronic commerce has many advantages, which has been paid more attention to by all over the world, and the speed of development and popularization is very fast.

5. Summary

WPKI is an extension of PKI technology in mobile e-commerce. WPKI also uses certificates to manage public keys and authenticates the identity of users through the CA Authentication Center. Its goal is to realize the secure transmission of information in the wireless network environment. Currently, many security solutions (in process, technology, and organizational mode) are available to reduce the risk and vulnerability of mobile e-commerce. First, wireless e-commerce solutions require the same security controls as those used to protect wired e-commerce environments. These control methods will include firewall, content, email filtering, antivirus, user authentication, authorization, policy management, intrusion detection, enhanced platform, secure equipment management and other technologies. In addition to these control methods, other technologies are needed to provide security for all wireless e-commerce channels.

References

[1] He Ning. Multi-Perspectives Analysis of Mobile E-commerce. Science and Technology Entrepreneurship monthly. 2014:100-105.

[2] Lu Tingjie. Trend Analysis and Prospect of Mobile Commerce in China. Journal of Beijing University of posts and Telecommunications,2016:308-312.

[3] Yan Hui. Review on the Development Strategy of Mobile E-commerce. Finance and economics (middle edition). 2017.

[4] Li Na. Analysis on the Mode of Mobile E-commerce based on value chain. China science and technology information,2014.

[5] Shen Huimin. Research on the Development trend of Mobile E-commerce in China. Scientific and technological information development and economy. 2015:22-28.

[6] Mou Tonghua. Application of Mobile E-commerce in Enterprises. Enterprise economy,2012.