International Journal of Security and Its Applications
Vol. 10, No. 6 (2016) pp.205-214
http://dx.doi.org/10.14257/ijsia.2016.10.6.20

The Research based on SSL and WPKI of Mobile E-commerce

Jijun Xing

Northwest University of Politics and Law, Xian, Shaanxi, China
Xingjijun1@aliyun.com

Abstract

The recent years have witnessed the fast growth of mobile e-commerce in the world, and this model has become the most popular one among all the e-commerce models. However, compared with the traditional e-commerce models, the mobile e-commerce is less secure as the carriers, including smart phones, PDA, or handheld computers, can hardly reach the same high level of security as personal computers. The network gap caused by different network operators also causes the network delay when the users are doing cross-platform internet browsing. To solve these problems, a new scheme to reduce network delay and improve security level has been put forward. This scheme proposes to install a "routing box" in user's home at first. When the smart equipment is to be connected to the Internet, it shall log in on the equipment to be connected to the nearest cloud server which will send the connection request and connect the user to his/her aimed website quickly. Through SSL + WPKI protocol, the user's log-in information and other forms of information can be safely transmitted. The visiting history can be stored in cache in different levels via cloud server. Therefore, when the relevant information is visited again, the user request can be sent to his/her smart equipment through the nearest cloud server, which can resolve the network gap caused by cross-platform visiting. Such a scheme has been proved effective in local area network by test.

Keywords: *Mobile E-commerce, Security, Network Gap, SSL, WPKI*

1. Introduction

In current society, the rapid development of the mobile internet has brought tremendous changes to people's life and work. When shopping, eating, travelling and working, more and more people habitually take out their mobile phones to read messages, find locations, share feelings and coordinate work with others. At the same time, millions of users nationwide surf the internet via mobile devices each day to live, work, make transactions and make friends. These new network patterns have also become the impetus for the development of the mobile internet.

The mobile internet fever is rapidly spreading to every corner of the society. At the news conference of CNNIC held on February 3rd, 2015, the 35th Statistical Report on the Development of the Internet in China was released. [1] According to this report, by the end of December, 2014, the number of mobile telephone subscribers had reached 1.286 billion, and the percentage of subscribers whose phones were connected to the internet continued to increase by 4.8 percentage points (equal to 56.72 million newly added people) than the previous year. Diagram 1 illustrates the number of Chinese mobile netizens and its percentage in the whole netizens.

ISSN: 1738-9976 IJSIA

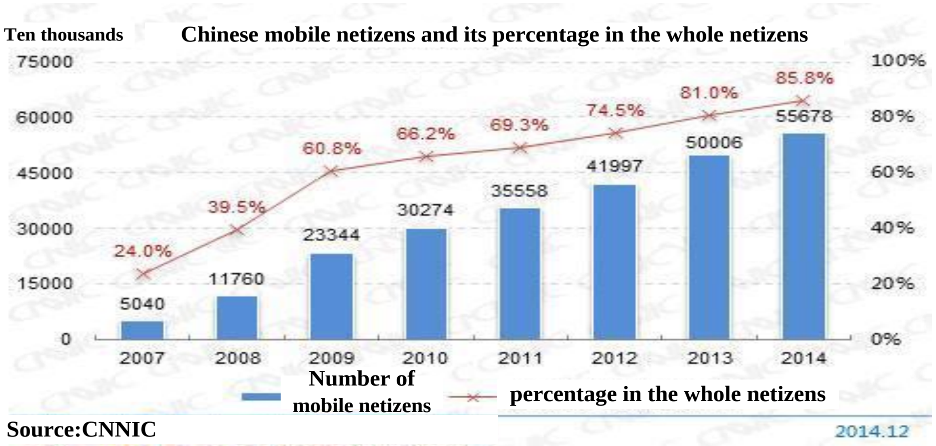

Diagram 1. Number of Chinese Mobile Netizens and its Percentage in the Whole Netizens

According to Diagram 1, since 2007, the percentage of mobile internet users has started to grow at a relatively high speed and the total number has increased in a stable rate. Meanwhile, for mobile users, they usually surf the internet to do online shopping, watch videos, search information and so on. Diagram 2 shows areas of applications of mobile internet users.

Despite the flourish of the mobile internet, problems such as internet security and low internet speed have occurred frequently. The security has always been the key factor affecting the development of mobile e-commerce. Compared with the traditional e-commerce models, the mobile e-commerce is less secure as the carriers, including smart phones, PDA, or handheld computers, can hardly reach the same high level of security as personal computers. Therefore, the personal information of mobile users (online account, password, *etc*.) accordingly cannot reach the same high level of security as personal computers. To sum up, the mobile e-commerce is less secure than the traditional one. Besides, the network gap caused by different network operators also causes the network delay when the users are doing cross-platform internet browsing, which brings trouble to most users. Diagram 2 analyzes the factors that affect the information security of internet users.

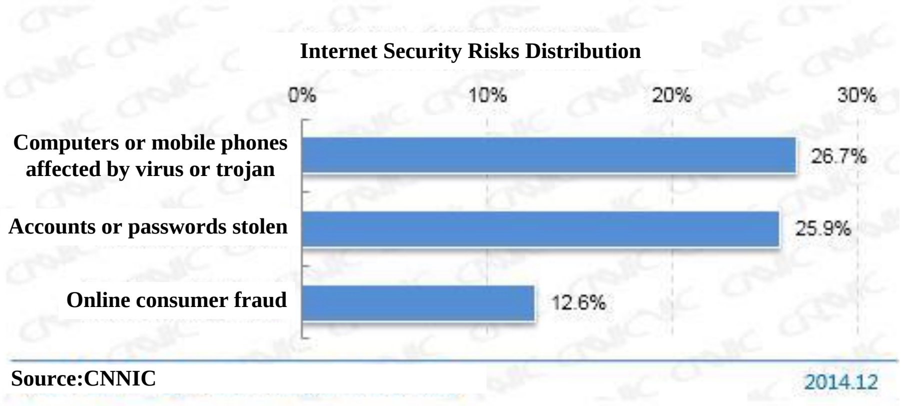

Diagram 2. Factors Affecting the Information Security of Internet Users

To solve these problems, a new scheme to reduce network delay and improve security level has been put forward. This scheme proposes to install a “routing box” in user’s home at first. When the smart equipment is to be connected to the Internet, it shall log in on the equipment to be connected to the nearest cloud server which will send the connection request and connect the user to his/her aimed website quickly. Through SSL + WPKI protocol, the user's log-in information and other forms of information can be safely transmitted. The visiting history can be stored in cache in different levels via cloud server. Therefore, when the relevant information is visited again, the user request can be sent to his/her smart equipment through the nearest cloud server, which can resolve the network gap caused by cross-platform visiting. Such a scheme has been proved effective in local area network by test.

2. Safety Technology and Protocol Analysis

2.1. SSL Protocol Analysis

SSL Protocol is also known as Secure Socket Layer Protocol. SSL VPN inherits the advantage of the consistent long-distance usage experience of IPSec VPN and the intranet, thus avoiding problems such as the inconvenient use and maintenance caused by client-side, the failure to be connected under certain internet conditions, the invasion of massive virus and worms, the failure to combine with the existing authentication server of companies and the failure to audit. [2] The advantage of SSL Protocol is that it is irrelevant to the application layer protocol. High application layer protocol (HTTP, FTP, and TELNET) can be established on the base of SSL Protocol transparently. Before the correspondence of application layer protocol, SSL Protocol has completed the negotiation of encryption algorithm and correspondence secret key and the work of server authentication. After that, data transmitted by application layer protocol will be encrypted to ensure the privacy of correspondence. [3]

SSL protocol includes two layers. The bottom layer, Record Protocol aims to block data, encrypt and decrypt, compress and uncompress, check the completeness, and pack various higher layer protocols. The higher lay, Handshake layer, consists of three paratactic protocols, namely Handshake Protocol, Change Cipher Spec Protocol and Alert Protocol. It is mainly used to produce the password parameter of session state. When SSL client starts to correspond with the server, it can negotiate the protocol version, choose password algorithm, authenticate identity and use public secret key technology to produce shared secret key. Diagram 3 illustrates the SSL Protocol stack.

<table>
<tr><th colspan="3">The application layer protocol</th></tr>
<tr><td>Handshake Protocol</td><td>Change Cipher Spec Protocol</td><td>Alert Protocol</td></tr>
<tr><td colspan="3">Record Protocol</td></tr>
<tr><td colspan="3">TCP</td></tr>
<tr><td colspan="3">IP</td></tr>
</table>

Diagram 3. SSL Protocol Stack

The main performance feature of SSL is that due to the performance reduction caused by encryption and decryption. [4] There are three encryption algorithms in SSL Protocol [5]: secret key exchange algorithm, data encryption algorithm and hashing algorithm. The key exchange algorithm adopts asymmetric secret key encryption algorithms, such as RAS or DH to communicate the secret key negotiation process between two sides; data encryption algorithm uses symmetric key encryption algorithms, such as DES, RC4, etc. In SSL protocol, these encryption algorithms combine with each other to form several cipher suites, each cipher suite corresponding to a fixed integer value. Therefore, all the cipher suites use a uniform format such as password suite

SSL_RSA_WITH_RC4_128_MD5 which represents that the secret key exchange algorithm adopts RSA, the data encryption algorithm adopts 128-bit RC4, and hashing algorithm adopts MD5.

2.2. WPKI Platform Analysis

WPKI (Wireless Public Key Infrastructure) [6] is a secret key management platform that meets certain standard. WPKI PKI is not a new PKI standard. It is an optimized and extended traditional PKI technology which has been applied to wireless environments. It uses an optimized ECC elliptic curve encryption and compressed X.509 digital certificate. [7] Meanwhile, it has a certificate management public key, which can achieve secure transmission of information through a trusted third-party organization – Authentication Center (CA) verifies the identity of user to achieve the secure transmission of information.

A complete WPKI system generally includes end-entity application, [8] PKI Portal, Authentication Center (CA), the directory server (PKI Directory), WAP gateway WTLS and other devices or protocols. WPKI structure is shown in Diagram 4 below.

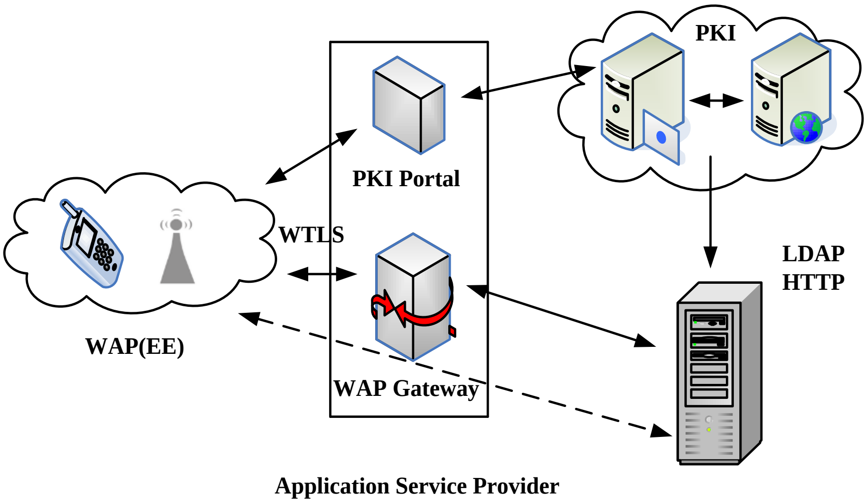

Diagram 4. WPKI Structure

In specific, end-entity application refers to mobile devices that support WAP applications, such as WAP phones, WAP-enabled PDA. It contains the SIM card and the WIM card, or the SWIM card which combines the previous two cards. PKI Portal provides users and CA with an interface to replace the function of RA (Registration Authority) in wired networks. It accepts the user's certificate signing request, confirms the user's identity, and is responsible for forwarding the needs of users to CA (Certification Authority) to present the certificate request. CA is the trust basis of WPKI, mainly responsible for generating, issuing and verifying digital certificates, and for regulating the period of validity of certificates, refreshing certificates and other management work. WAPIX needs WAP gateway to handle the protocol conversion between the client and the origin server. WAP gateway uses WAP protocol to communicate with the customer and uses standard Internet protocol to communicate with the source server. WAP2.0 standard has been greatly improved, but is still compatible with 10 standards. In WAP2.0, HTTP/1.1 can be directly used to communicate between the client and the origin server. Of course, configuring one WAP proxy can also process other work such as enhancing the function of mobile services. Directory Server is used to provide identity information of users and certificate inquiry, store signed and issued digital certificates and keep latest certificate revocation list (CRL). Users can query validation, obtain the required certificates and public keys of other users. WTLS is mainly responsible for ensuring the safety of the transport layer. It is an improved and optimized version of the traditional wired network TLS protocol.

3. Technical Proposal and Principle Analysis

3.1. Principle Analysis

Currently, 95% of the internet international exports of broadband Internet, 90% of broadband Internet accessing users and 99% of Internet content providers are concentrated in the Telecom and China Unicom, which form the situation of double monopoly. The central issue of this operator monopoly is: monopoly system of broadband accessing market, especially telecom operators do both broadband Internet service provider (ISP) and make broadband content operations (IDC) of the dilemma, leading in recent years forming a huge bandwidth gap between different operators, a direct result of Internet users, especially users of mobile Internet, access across the ISP network is very slow. The scheme needs to eliminate the ISP gap so that users will not feel the difference of the network speed. Meanwhile, for these users, the safety of their individual or company accounts can be ensured in the information transmission and the transaction process.

This scheme proposes to install a “routing box” in user’s home or office at first. This wireless router (apart from providing signal routing, it also includes a storage cell to store users’ information) uses wire mode to connect router or MODEM. The special lines will be installed in signal receiving end and sending end outdoors, and a certain number of multi-level cache servers will also be installed according to the intensity of users. Figure 6 is the schematic Diagram.

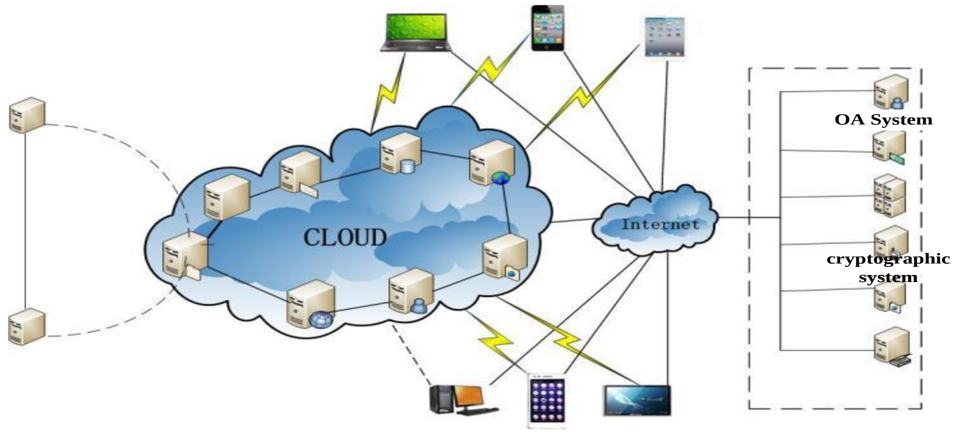

Diagram 5. Schematic Diagram of the System

For mobile users, they need to download an APP and log in the account in the first use. After the successful logging, they can download the required documents from the APP. The APP also has the service of user experience and purchase. When users need to purchase related services, they can click on the relevant interface to enter the shopping links.

Due to the layout of many servers in the cloud, once the user makes a request, the system will send the request to the node closest to the user, and then the node sends the requests to the destination. Under cross-ISP environment, since the signal transmitting end of each user is connected individually and there is no speed limit on the software or hardware, it is possible to send and receive bandwidth in the same way and eliminate network gap.

When a single node is broken, the connection will promptly migrate to other nodes to ensure the rapid recovery of the service. At the same time, because of the low coupling between nodes, when the system capacity is insufficient, adding hardware, installing software, setting up correctly and plugging the Internet cable can rapidly expand the processing power of the distributed system. Diagram 6 shows the scheme topology.

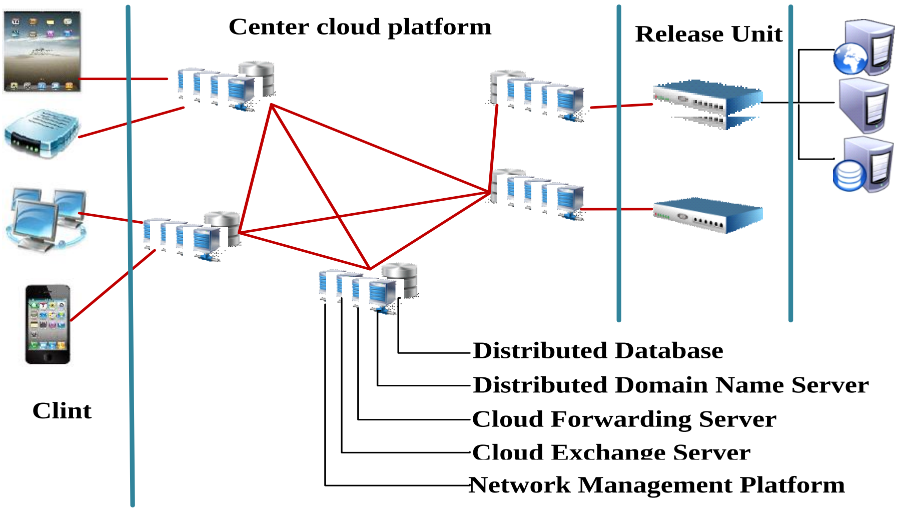

Diagram 6. Scheme Topology

3.2. Technical Proposal

1) Distributed architecture

Virtual network uses a distributed architecture, in which each node only shares the registration node information of the unit. Therefore high availability can be easily achieved. The load balancing is also achieved to respond to massive connection. When a single node is broken, the connection will promptly migrate to other nodes to ensure the rapid recovery of the service. At the same time, because of the low coupling between nodes, when the system capacity is insufficient, adding hardware, installing software, setting up correctly and plugging the Internet cable can rapidly expand the processing power of the distributed system.

2) Speed up user application

User experience can be improved by the strategy of optimizing routing in the cloud, which uses high-speed lines (special lines, fine nets, *etc*.) to accelerate the forwarding of user data and improve user experience.

3) Resolve the problem of cross-operator network interworking

Multi-line access through the cloud node can make the visit of cross-operator forwarded within the node without having to squeeze the narrow passage between operators.

4) Distributed intelligent domain name system

When users access the virtual network cloud platform, the virtual network distributed intelligence domain name system will figure out IP addresses of the nearest nodes for clients and the software will automatically find the IP address of the best connection speed according to the geographic information, operators, IP addresses and other information

5) Cloud connection service

By renting the service of virtual network cloud connection, enterprises can connect headquarters with branch offices at the network level. Compared with the special line, the cloud optimization and the reduplication in the virtual network can produce less cost and achieve better results.

6) Distributed network management platform

Cloud platform contains TR069 protocol-based network management. Through the management platform, you can know whether the device is online, the version number, the number of authorized users, CPU and configuration information such as the utilization rate of internal storage and the flow of internet access. You can also send configuration information, push the upgrade information, set alarms, etc. to multiple machines.

7) End to end security

The encrypted and signed signature key of data communication is shared by client-side and issuing units. When forwarded by the cloud platform, the encrypted data cannot be decrypted as the cloud platform does not have the key. Therefore, users do not have to worry about data being watched, stolen or collected.

4. Security Architecture

4.1 Digital Signature and Verification [9]

SSL protocol itself can authenticate the identity of users through identification exchange, digital signatures and notarization mechanism. In the verification process, the protocol checks the user's credentials to authenticate their identity by exchanging information. Authenticator checks credentials after obtaining them from the other party. Meanwhile, the data exchanged is encrypted. Only legitimate users can decrypt it and get meaningful plaintext, thus further ensuring the validity of the two communication parties. The WPKI authentication principle is based on the signature mechanism. The secure connection between the mobile terminal and the WAP gateway uses WTLS protocol, which is a secure transmission protocol from WAP protocol stack to serve the mobile e-commerce business. This can ensure the communication safety of WAP.

When mobile end users need to connect to the Internet, after they send the message m, the secret keys of the corresponding elliptic curve algorithm of the mobile terminal and application server are $(d_c, p_c)$and (d_s, p_s) respectively. In this case, the mobile terminal firstly turns m into H =Hash（m） by Hash function, and then uses the private key to sign the message. The specific process is as follows:

First, the system selects a secret key pair (k, R) based on the elliptic curve parameters $T = (p, a, b, G, n, h)$. Then it converts to the field element x_R to the integer X_R and calculates $r = X_R \bmod n$ ($r \neq 0$). Otherwise the above procedure must start over. At the same time, a random number e is generated from H in accordance with the relevant rules, then $s = k^{-1} \cdot (e + r \cdot d_m)(\bmod m)$ is calculated out ($s \neq 0$). After the said steps, digital signature $S = (r, s)$ is generated.

After getting effective legal certificates of users, the cloud server obtains the relevant elliptic curve parameters T and the public key P_M from the digital certificate, and verifies if the digital signature r and s are in the valid range [0, n-1]. If valid, it uses the above algorithms to calculate H = Hash (m), and also generates a random number e to calculate $u_1 = e \cdot s^{-1}$ (mod n), $u_2 = r \cdot s^{-1}$ (mod n) and $R = (x_R, y_R) = u_1 G + u_2 P_M$. If R is 0, the digital signature is invalid; otherwise the field element x_R will be converted to the integer X_R with the setting of $v = X_R \bmod n$. If v and r are equal, the digital signature is verified, the user information is true, and the user can request to give reply. At this point, the user information is verified.

4.2. Safe Transaction Flow

1) Users log in APP, browse relevant information and click Services they want to buy;

2) The server firstly confirms the user identity after receiving information. If the identity is verified, it forwards the subscription information to the appropriate service holders;

3) Users use their own transaction private key to sign the payment information with the signature algorithm and submit signature information and other payment messages to the trading platform;

4) After receiving customers' payment messages, the security trading platform downloads the client’s digital certificate from the CA and verifies the signature. The successful verification indicates that the payment information is indeed issued by the payer and the pay message is forwarded to the banking system;

5) The bank verifies the digital signature of the payment message and takes out payment instructions, transfer funds, and tells the secure trading platform whether the payment is successful or not, the amount of the payment and other payment results. The trading platform keeps the payment record as the receipt and the certificate for future inquiry;

6) The secure transaction platform will tell the clients the final payment results in real time.

4.3. Security Analysis

User information privacy: the communication of the wireless network uses WTLS handshake protocol. While in wired networks, the communication uses the traditional SSL cryptographic protocol. Therefore, information channels among the modules of the system are safe.

Authentication of user and service provider: certificates of parties involved in the transaction in the system are signed and issued by CA. The sender uses their private key to sign the data, and the recipient uses public key information of the certificate to verify the information. In this way, the authenticity of all transaction parties’ identity is achieved.

5. Conclusion

The scheme is mainly aimed to eliminate network gap in cross-ISP access and eliminate security risks in the process of e-commerce transactions. The main innovation is the use of Internet-based mode. Users do not need all the professional knowledge; instead, they just sign up for an account to enjoy a professional and secure remote access service. Meanwhile, the original network security equipment and project-oriented mode of operation are transformed into mode of network service. The innovation of this model will change the industry's business model and bring a new experience to users through establishing a practical platform in a free way.

The laboratory and LAN experiments proved that this scheme was feasible and produced some real data and the effect picture (Diagram 7). It can be seen that the basic network delay of across-ISP access at different times is within the allowable range.

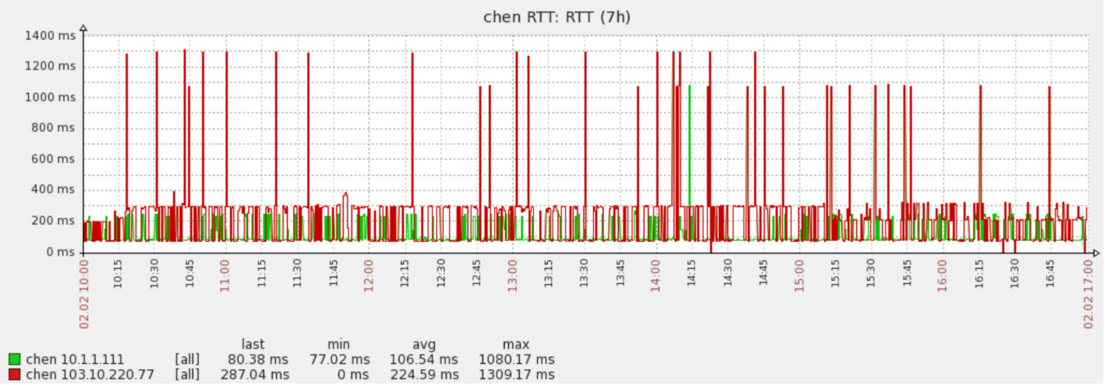

Diagram 7. The Experimental Result

References

[1] China Internet Network Information Center, Statistical Report on the Development of the Internet in China, **(2015)**, vol. 2.

[2] G. Ling and L. Weisheng, “Design and Implementation of SSL VPN”, Computer Technology and Development, **(2007)**, vol. 17, pp. 148-154.

[3] E. Rescorla, “SSL and TLS: Designing and Building Secure Systems”, Addison-Wesley Professional, 1st edition **(2000)**.

[4] Kant K., Iyer R. and Mohapatra P., “Architectural Impact of Secure Socket Layer on Internet Servers［C］”, // Proceedings of 2000 International Conference on Computer Design, Texas: IEEE Computer Society, **(2000)**, pp. 7-14.

[5] S. Zhongfa, ‘SSL-based VPN Research and Implementation’ [Master’s degree Thesis], Chongqing University, **(2007)**, vol. 1, pp. 10-15.

[6] W. Jianbing, “Security Application of PKI Digital Certificate in WEB System[J]”, Land and Resources Informatization, **(2005)**, vol. 1, pp. 40-44.

[7] S. Hung－Min, “Cryptanalysis of Aydosetal’s ECC－based wireless authentication protocol［C］”, / /Proceedings of the 2004 IEEE international conference on e－technology, e－commerce and e－commerce and e－service. [s.l.]: IEEE Computer Society, **(2004)**.

[8] H. Jingling and Z. Xiuying, “Safe Mobile Payment Research Based on WPKI Technology”, Computer Technology and Development, **(2014)**, vol. 24, pp. 156-165.

[9] T. Feng, “WPIK-based Mobile E-commerce Scheme Research”, Computer Application and Software, **(2013)**, vol. 30, pp. 61-65.

Author

Jijun Xing, Male, born in Xi’an City, Shaanxi Province in 1976, has a master’s degree in Network Security in Southwest Jiaotong University, and now works in Northwest University of Politics and Law, with major research direction being computer networks and mobile electronic commerce security.