Design and Implementation of Mobile Security Access System (MSAS) Based on SSL VPN

Dingguo Yu
College of Information
Shaoxing University
Shaoxing, China
zjydg@163.com

Nan Chen
College of Qiangjiang
Hangzhou Normal University
Hangzhou, China
ermunan@126.com

Chengxiang Tan
Department of Computer
Tongji University
Shanghai, China
jerrytony777@gmail.com

***Abstract*—With the rapid development of mobile networks technology and popularization of mobile device, people can access Internet by mobile device and wireless connection covering the entire mobile communication network (GSM/GPRS/CDMA/3G/802.11etc) at any moment. Business system based on mobile network has been becoming hotspot. Compare with traditional business system, the security risk of business system based on mobile network is more popular and grave. However, the traditional mobile communication technology does not provide the security services such as authentication, confidentiality, and integrity etc. To solve this security problem, in this paper, we designed and implemented a mobile security access system (MSAS) using SSL VPN, CA and smart card technology. It establishes a complete authentication mechanism based on smart card and X. 509 certificates, and uses SSL VPN tunnel to protect the security of a message transmission on the Internet and mobile communication network. It will help some commercial companies and government authorities, who need confidential information transmitted over the air, such as banks providing mobile bank service, policemen exchanging data of criminals, etc, to build secure communications channel, and some secure business system based on fixed-IP network extend to mobile network.**

Keywords-Mobile Computing; Security and Protection; Virtual Private Networks (VPN); Secure Socket Layer (SSL)

I. INTRODUCTION

Mobile telecommunication handsets and networks are developing rapidly in recent years. At the middle of 2008, the worldwide number of mobile users was over 3.6 billion people [1]. Today, people can access Internet by mobile device and wireless connection covering the entire mobile communication network (GSM/GPRS/CDMA/3G/802.11etc) at any moment. The research and exploitation about mobile business system has been becoming hotspot. But some commercial companies and government authorities, who need confidential information transmits with their back-office application server over the air, such as banks providing mobile bank service, policemen exchanging data of criminals, etc.

According to the characteristic of mobile device and mobile network, the security risk of business system based on mobile network is more popular and grave, compare with traditional business system. To exploit a secure mobile business system, it is necessary to enhance its functionalities to offer the security services such as authentication, confidentiality, integrity, and non-repudiation, etc. However, such requirements are not provided by the traditional mobile network. How to ensure the security of the mobile terminal accessing and exchanging data with their back-office application server is becoming more and more important.

The critical fields of mobile security access system include mobile terminal security, wireless network security and access security. In this paper, we designed and implemented a security mobile access system (MSAS) which based on SSL VPN technology. The MSAS establishes a complete authentication mechanism based on smart card and X. 509 certificates, and use SSL VPN tunnel to protect the security of message transmission on the Internet and mobile network.

The rest of this paper is organized as follows: Section 2 introduces and reviews the background technologies. Section 3 analyses the architecture and work flow of the mobile security access system (MSAS). Section 4 introduces the result of the system implement and test. Section 5 concludes the paper.

II. BACKGROUND TECHNOLOGIES

A. SSL/TSL protocol [2][3][4][5]

The Secure Sockets Layer (SSL), a protocol originally defined by Netscape, is a commonly-used protocol for managing the security of a message transmission on the Internet. The IETF adopted the technology as a standard in 1999, naming it Transport Layer Security (TLS). However, most users still call it SSL.

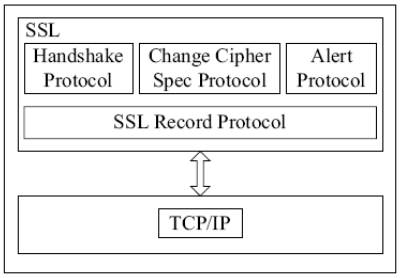

Figure 1. SSL protocol layer architecture

This research is supported by the National High Technology Research and Development Program of China (863 Program), No. 2006AA01Z438

978-0-7695-3557-9/09 $25.00 © 2009 IEEE
DOI 10.1109/ETCS.2009.559

SSL protocol provides connection security with the following basic properties: peer entity authentication, data integrity, data confidentiality, key generation and distribution and security parameter negotiation. This protocol consists of several sub-protocols, specially the Record and the Handshake protocol. Figure1 illustrates the SSL protocol layer architecture. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP [TCP]), is the SSL Record Protocol. The Record Protocol provides private and reliable connection security; it is used for encapsulation of various higher level protocols. One such encapsulated protocol, the Handshake protocol is used to allow peers to authenticate themselves, negotiate security parameters of a session for the record layer, and report error conditions to each other. Once a transport connection is authenticated and a secret shared key is established with the SSL Handshake protocol, data exchanged by application protocols can be protected with cryptographic methods by the Record layer using the keying material derived from the shared secret.

SSL defines the full handshake phase that involves the exchange of X.509 certificates and the cryptographic information to allow peers to be authenticated. This step requires several operations. First, peers must verify the integrity of certificates and should generally support certificate revocation messages. Also, the certificate should always be verified to ensure it is trusted and signed by a known Certificate Authority (CA). Finally, the client should be able to view the information about the certificate and the CA root.

One advantage of SSL is that it is application protocol independent. Higher level protocols can layer on top of the SSL Protocol transparently. The SSL standard, however, does not specify how protocols add security with SSL; the decisions on how to initiate SSL handshaking and how to interpret the authentication certificates exchanged are left up to the judgment of the designers and implementers of protocols which run on top of SSL.

B. SSL VPN

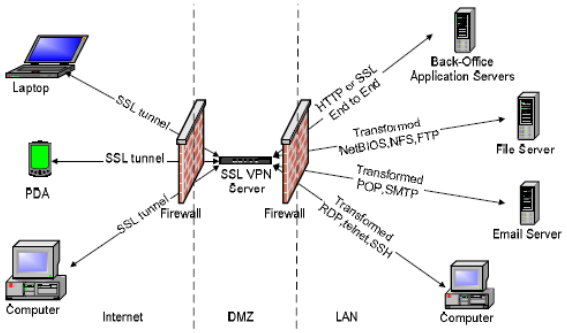

Figure 2. A typical example of SSL VPN

SSL VPN is a secure remote access solution based on SSL/STL protocol, and develops rapidly in recent years. According to the prediction of Gartner Company [6], SSL VPN market will grow more than 170% per year.

Figure 2 shows a typical example of SSL VPN structure [7][8]. When a client needs to connect to an internal application server, at first, the client should request to create a VPN connection with SSL VPN gateway, and then the VPN peers authenticate each other through their digital certificates and negotiate security parameters. After the VPN peers were authenticated, a SSL VPN tunnel will be created, connecting the client and the SSL VPN gateway. Then the SSL VPN gateway sets up a TCP connect to the internal application server on behalf of the client. Thereafter, the SSL VPN gateway relays data between the client and the internal application server, all data flows of the VPN should be encapsulated or unwrapped at the SSL VPN gateway according to SSL protocol. Inside the LAN, communication data between the SSL VPN gateway and the internal application server can be either in plain text, or protected by additional internal SSL tunnels, it's up to internal security requirement.

Compared with IPSec VPN, SSL VPN has some outstanding advantages, like easy-to deploy, fine-grained access control, etc.

III. ANALYSIS AND DESIGN OF MSAS

A. MSAS Architecture

Figure3 illustrates the architecture of the Mobile Security Access System (MSAS). The MSAS is composed of two parts: Mobile Device (MD) and Security Access System (SAS). The MD is a secure mobile terminal installed an add-on VPN Management Toolkit which developed with Java 2 Micro Edition (J2ME). It includes four main function modules: VPN connection management, certificates management, and smart card management and encryption/decryption module. The VPN connection management module implements functions as fellows: VPN connection mode setting, VPN connection dial-up, manage currently connection and close VPN connection. The SAS make up of modules as follows: VPN gateway, encryption/decryption, CA, access control, users management, network management and system log management, etc. The MD creates VPN connection with the SSL VPN gateway, and exchanges data with internal applications server follow the VPN tunnel.

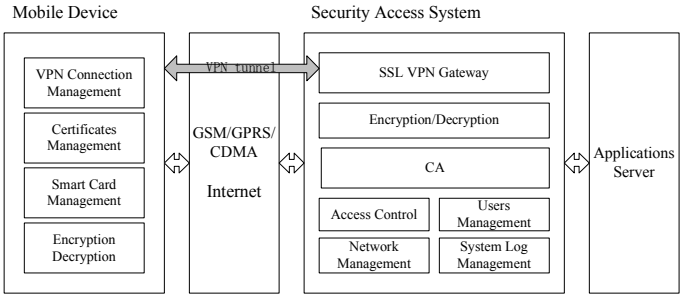

Figure3. The architecture of MSAS

B. *MSAS work flow*

The MSAS work flow as Figure4 illustrates, it is composed of 3 steps: create VPN connection, access internal application server and close VPN connection. In the create VPN connection step, the MD request to create a VPN connection with the SSL VPN gateway firstly. According to the SSL/STL protocol, the SSL VPN gateway and the MD authenticate certificate each other and negotiate the secure parameters of a session including protocol version, session ID, cipher key and encryption/decryption functions and version, etc through hello messages. After the MD was authenticated by the SSLVPN gateway, a SSL tunnel connecting the MD and the SAS will be created. In the access internal application server step, after created VPN connection, the access control management module validates the MD user's access act according to the access control strategies firstly, if truth, it locate the MD user's application request to one application server. Additionally, the application server returns the data to the SSL VPN gateway, the SSL VPN gateway encrypt the application data and sent the encrypted packet to MD.

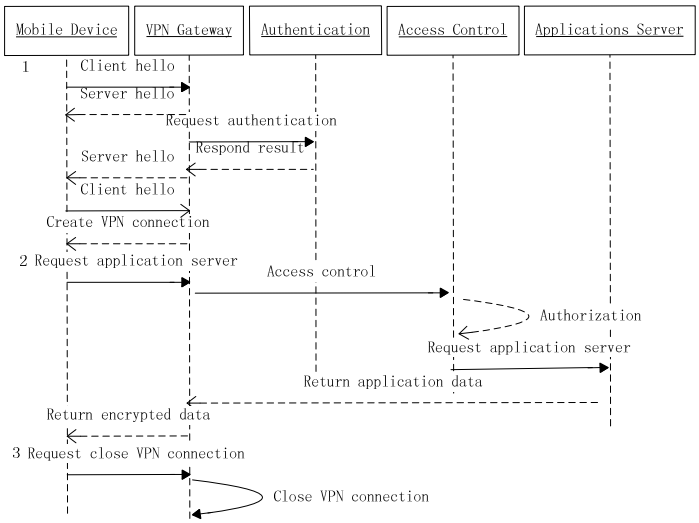

Figure 4. MSAS work flow

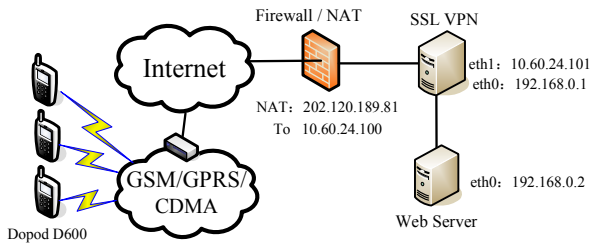

Figure 5. Test network environment

IV. IMPLEMENTATION AND TEST

The test environment makes up of three MDs (Dopod D600), one wireless access point and two servers (SSL VPN Server and Web Server), as Figure5 shows. Through GPRS, CDMA or WLAN, we test the functions, capability and security of the MSAS. Under GPRS or CDMA mobile communication network, the MD connect up GPRS or CDMA mobile communication network firstly, and create a VPN connection to SSL VPN server, then access web server through SSL VPN tunnel. Under WLAN environment, the MD access Internet through the wireless access point firstly.

Under every mobile network (GPRS, CDMA or WLAN) environment, every MD tests 20 times. Every test includes the functions of create VPN connection, examine current VPN connection, close VPN connection and access Web server and their response time. The average response time of test result as TABLE Ⅰ illustrates.

The result of security test as TABLE Ⅱ illustrates, it show the MSAS can offer the security server of information exchange between the secure mobile terminal and internal application server through mobile communication network and Internet.

TABLE Ⅰ. RESULT OF CAPABILITY TEST (S)

Network	Create VPN connection	Examine current connection	Close connection	Access Web server
GRPS	8.1	0.8	0.9	4.5
CDMA	6.5	0.6	0.8	3.8
WLAN	3.2	0.5	0.5	1.6

TABLE Ⅱ. RESULT OF SECURITY TEST

Test	Result
Smart card PIN error	Create VPN connection error
A overdue certificate	Create VPN connection error
A fabricated certificate	Create VPN connection error
Capture packet	Encrypted packet
Fabricate packet	Close VPN connection

V. CONCLUSION

In this paper, we designed and implemented a mobile security access system (MSAS) using SSL VPN, smart card and CA technology for the mobile terminal security accessing and exchanging data with back-office application servers based on fixed-IP network by wireless connection covering the entire mobile communication network. After test, this system can meet the demand of mobile security accessing on functions, capability and security, etc. It will help some commercial companies and government authorities, who need confidential information transmitted over the air, such as banks providing mobile bank service, policemen exchanging data of criminals, etc, to build secure communications channel, and some secure business system based on fixed-IP network extend to mobile network.

REFERENCES

[1] GSM World News-Statistics: http://www.gsmworld.com/news/statistics/index.shtml. Oct. 23 2008.

[2] Alan Freier and Philip Karlton, "The SSL Protocol Version 3.0 ", http://wp.netscape.com/eng/ssl3 /draft302.txt, Oct.2004.

[3] T. Dierks and C. Allen, "RFC2246: The TLS Protocol Version 1.0", http://www.ietf.org/rfc/rfc2246.txt, 1999.

[4] Yang Kuihe and Chu Xin, "Implementation of Improved VPN Based on SSL", The Eighth International Conference on Electronic Measurement and Instruments (ICEMI'2007), 2007, pp:2-15—2-19

[5] Mohamad BADRA and Pascal URIEN, "Toward SSL Integration in SIM SmartCards", Wireless Communications and Networking Conference, 2004(WCNC 2004), March.2004, pp:889 - 893

[6] Gartner Company, http://www3.gartner.com/.

[7] Jingli Zhou, Hongtao Xia, Xiaofeng Wang, and Jifeng Yu, "A New VPN Solution Based on Asymmetrical SSL Tunnels", Proceedings of the Japan-China Joint Workshop on Frontier of Computer Science and Technology (FCST'06), Nov.2006, pp.71-78

[8] Karen Heyman, "A New Virtual Private Network for Today's Mobile Word", Computer, Dec.2007, pp.17-19.