International Journal of u- and e- Service, Science and Technology
Vol.8, No.4 (2015), pp.17-26
http://dx.doi.org/10.14257/ijunesst.2015.8.4.03

VPN Gateway Research in Wireless Network Based on SSL Technology

Xingkui Wang[1] and Xinguang Peng[2]

[1]*College of Computer Science and Technology,Taiyuan University of Technology,Taiyuan, China*
wxk0301@163.com
College of Computer Science and Technology,Taiyuan University of Technology,Taiyuan, China
wxk0301@163.com[1], sxgrant@126.com[2]

Abstract

Security is an important issue in the design and deployment of wireless networks. Existing equipment is mainly used in security technology include SSID, MAC address Filtering, WEP and 802.11x etc. There exists certain safety defects in design and not well protect the security of the wireless network. This paper puts forward a VPN technology was applied to the deployment scheme in wireless networks, which design a set of VPN gateway using SSL technology in Linux environment, so as to solve the current security issues in accessing resources within the network through wireless network.

Keywords: *Secure Sockets Layer (SSL), Virtual Private Network (VPN), wireless network, gateway, encryption*

1. Introduction

Nowadays numerous enterprises and schools have their own VPN networks for wired network access and identity authentication. VPN in wired network is comparatively mature technically and for commercial use. But researches and application targeted at wireless VPN are much less. Since wireless media of communication is usually exposed to air and is space-reliant signal transmission. It is more likely to be intercepted of important information once hackers break into compared with wired network. Therefore the safety issue of wireless network is of remarked significance. This thesis conducts a research on realizing safe wireless network use SSL VPN.

2. Wireless Network Security Solution at Present

At present, approaches for solving wireless network security concentrate on access control and date encryption. Access control secures sensitive data only permits authorized user in, and data encryption ensures that data transmitted is only received and comprehended by expected users. Regular technologies for wireless network security are specified as follows:

(1) Service Set Identifier (SSID) Match. Wireless clients must set up an identical SSID to wireless AP for access; if it is different from the certain AP SSID, then Internet surfing throughout this service area will be denied by the AP: set a hidden AP and SSID area division and access control for data encryption, notwithstanding SSID is usually a simple password.

(2) Physical address (MAC) filtering. Manually maintained a set of legal MAC address list of wireless client network card, in order to realize physical address filtering. Shortcomings: the efficiency rest in this approach will be reduced as the terminal number

ISSN: 2005-4246 IJUNESST

increases. Illegal users are also accessible to legal MAC address lists via network intercept, and they can take over legal MAC addresses for illegal access.

(3) Wired equivalent protection (WEP). In IEEE802.il, it is WEP defined for encrypting wireless transmitted data. RC4 algorithm is the core for WEP. Shortcomings: fixed secret key, limited initial vectors and algorithm strength.

(4) Port access control technology (IEEE802.1X).When wireless workstation (STA) relates with wireless access point (AP), the accessibility of AP service depends on identification result of 802.1X. [2] If the identification passes, AP will open the logical port for STA, or otherwise user network access will be denied. Shortcomings: IEEE802.1X provides wireless client for identification with RADIUS server, rather than the identification between client and wireless access point (AP). User identification data applied is only a user name and password, which features great hazards in storage, use and identification information transmission.

Therefore for highly demanding or large-sized wireless network, VPN scheme is a better choice. Since in large-sized networks, workstation maintenance, secret key for AP WEP encryption, MAC address list in AP are tough risks for management. For wireless network, the VPN based resolution is an ideal substitute for WEP mechanism and MAC address filtering mechanism.

3. SSL Protocol Realizes VPN

Virtual Private Network (VPN for short) utilizes a public network (*e.g.* Internet) to build up a network only for private use. Traditional VPN is a network security system based on IP safeguard construction, and the network layer-based IPSec VPN is a typical example. Its primary shortcomings include: it requires VPN far-end service groups to open several ports; the client-side must implement complicated and tedious configurations and specific maintenance management; IPSec VPN is unable to cross equipments compatible with NAT. A SSL/TLS protocol based VPN structure (SSL VPN) relying on Web Server rises in response to the extensive use of HTTPS. It features “no client-side” compared with traditional VPN for better use in the wireless network.

2.1. SSL Communication Process

SSL security protocol is actually a group of protocols consisting of SSL handshake protocol, SSL cryptograph modification protocol, SSL alert protocol and SSL record protocol, which is situated in TCP/IP protocol model residing network layer and the application layer, which realizes reliable end-to-end security service in use of TCP. SSL protocol has already completed encryption algorithm, communication secret key negotiation and server authentication prior to the application layer communication. After that, all data transmitted by the application layer protocol is encrypted. SSL handshake duration will be shortened by taking advantage of the mutually established effective SSL dialogue for access. Detailed process is specified as follows:

(1) SSL client end sends greeting massages for the client to SSL server. The dialogue ID is a established one.

(2) SSL server will check if there is a designated dialogue by the client after receiving the greeting message from the SSL client end. If it do not exists, SSL will establish access totally via the handshake protocol; if it exists, SSL server end will response an identical ID to that from the greeting message from the client end, and ensure that the negotiated encryption parameter at the server end is the same as the elected encryption parameter in the original dialogue.

(3) SSL server end will then send a message of encryption standard change to the SSL client end and close up the message with the handshake server end. SSL client will send a message of encryption standard change to the SSL client end and close up the message with the handshake server end upon reception.

2.2. Algorithm Implementation

SSLVPN security is based on SSL protocol, and therefore SSL protocol implementation is a key factor. The article adopts existing database OpenSSL, which is free of charge, and greatly simplifies implementation of the entire system. First of all, use function SSL libraiy_init() to initialize OpenSSL, utilizes SSL_load_error_strings() for initializing error messages. One SSL dialogue access requires a SSL environment, the process briefings are as follows:

(1)Establish the protocol for access this dialogue: SSL_METHOD* SSLv23_server_method(void).

(2)Apply an SSL dialogue environment CTX: the OpenSSL function for applying an SSL environment is SSLK _CTX* SSL_CTX_new（SSL_METHOD*). This function returns to the current SSL access environment. Then set up the verification mode for SSL handshake phases and load the certificate.

void SSL_CTX — set_verify (SSL _CTX，int, int*(int, X509_STORE_CTX*))*

void SSL_CTX _ load _ verify _ locations (SSL _CTX , constchar*，constchar*)*

*int SSL_CTX _use_ certificate_ file(SSL _CTX * ctx, constchar int type)*

*int SSL_CTX _use_PrivateKey _ file(SSL _CTX * ctx, constchar *f ile, int type)*

After loading the certificate and document, conduct identification to determine the consistence between the private key and certificate: BOOISSL_CTX_check_private_key (SSL_CTX*).

(3)Bind SSL and the connected socket: SSL*SSL_new (SSL_CTX*) this function applies a SSL socket, then conduct binding via function int SSL_set_fd(SSL*) for socket read-write.

(4) Initiate SSL handshake movements in use of the function: int SSL_connect(SSL*)

(5) After the handshake validates, communication is initiated. Use SSL read and SSL write for SSL socket instead of traditional ones, the function is:

*int SSL_read (SSL * ss,l char* bu，fint num)*

*int SSL_write (SSL * ss，l char* bu,fint num)*

For VPN gateway server, please use SSL accept instead of the traditional accept call, the function is:

*int SSL_accept(SSL * ssl).*

(6) When the communication is over, please release the SSL resource applied formerly in use of the following function:

*int SSL_shutdown(SSL * ssl)*	open SSL socket
void SSL_free (ssl)	release SSL socket
void SSL_CTX_free(ctx)	release SSL environment

3. Construction of SSL VPN Gateway in the Wireless Network

3.1. General Design of VPN Gateway

The most fundamental SSLVPN is composed of two parts specified as the client server and SSLVPN gateway. The client server uses SSL technology to send an encryption access request to the SSL VPN gateway. The gateway will transmit the decoded message to Web servers of the enterprise, thus forming an encryption tunnel on the Internet between one client end to the SSLVPN gateway, as shown in Figure 1. The core part of the SSLVPN gateway is composed of various independent functional servers, including the LDAP server in charge of preservation of public certificate and security key. As the LDAP client-end, the SSLVPN checks user information on the LDAP server to test whether the user identity is legal or not. The RADIUS server is responsible for accessing control strategies correlated to authentication. As the RADIUS client end, the SSLVPN gateway server functions in testing legality of user identity by interactive authentication with RADIUS server. AD is a certificate authentication server.

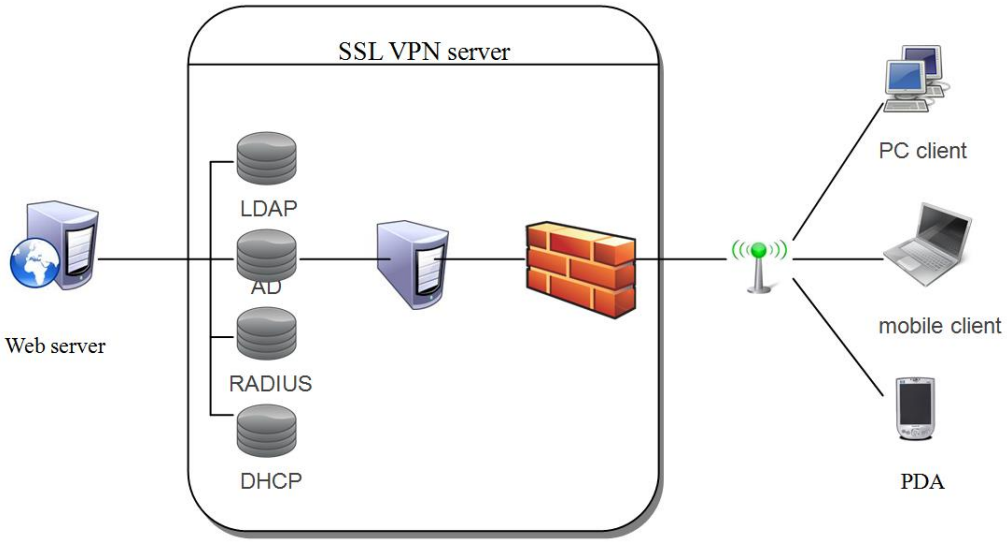

Figure 1. Whole Construction of Wireless SSL VPN Gateway

In Figure 1, the VPN gateway server and other servers are located in different mainframes in the intranet. VPN gateway server serves as a security agent in the intranet. Since it shares the same location in the intranet with other servers of various kinds, data transmission between them can be proclaimed in writing. The client end and VPN gateway server are located in different networks, and a secure channel must be built up between the two by using SSL for data encryption communication.

3.2 Logical Structure

3.2.1. Logical Design: The entire VPN system is composed of SSL gateway, Web server and AP. Among them, the SSL gateway is the most important, which ensures communication security, or confidentiality, message integrity and endpoint authentication. The SSL gateway consists of primary components including processing module, user authentication module, tunneling protocol module and secret key management protocol etc. The logic structure is specified in Figure 2 attached below.

3.2.2. Primary System Modules: Demand processing module: this module is a daemon process for resident memory in charge of SSL connects and fixed server ends monitoring. User authentication module: it adopts public key certificate authentication based on ECC elliptical curve code system. The entire identity authentication module consists of the client end, AP and the certificate server. Amid them, the certificate server includes CA, RA and CRL database and LDAP database. The certificate server undertakes the role of a server, which preserves the digital certificate ratified by CA on the client end and the authentication server. When the user connects AP, he must first be approved by the authentication server for allowing him to access AP if a legal certificate is owned as the results suggest. The secret key management module is part of the CA system. Functions contained in the secret key management module are: secret key generation, secret key update, secret key backup, secret key recovery, secret key destroy and filing processing etc. Access control module: the system administer conducts access control on intranet resources by setting up listed resource documents based on content access control.

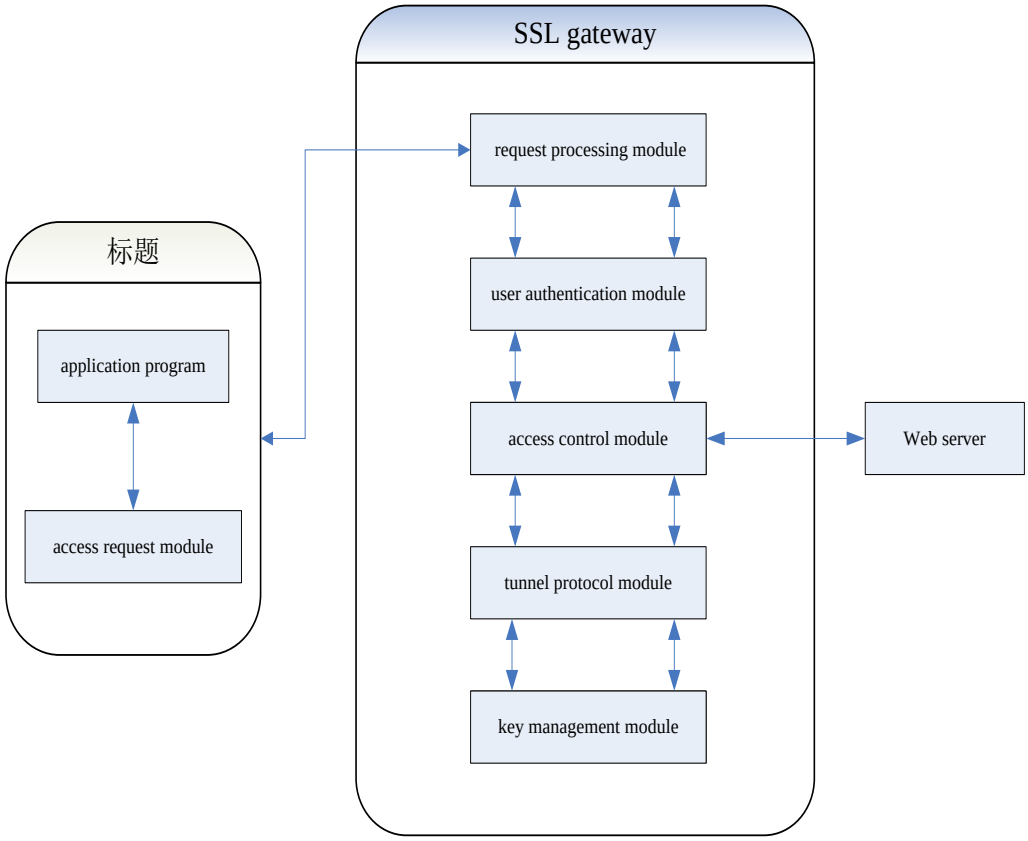

Figure 2. SSL VPN System Logic Structure

4. SSL VPN Gateway Applied in Wireless Campus Network

The SSL VPN based typical application raised in this thesis is wireless campus network. Libraries of institutes of higher education purchase enormous external resources, which are specified as remote electronic data and printed publications. These resources are not preserved on the library server, but stored in content provider server. Once the library pays for use, the content provider judges whether the applying user is authorized according to the user IP. A wide range of students and teachers can realize secure access to library resources via wireless campus network through SSLVPN.

4.1. Application System Design

The school can deploy an SSL gateway device at the back of firewall provided no change occur in the exiting wireless network. The internal resource server groups can be connected in parallel with the SSL gateway to the exchanger at the back of firewall, which will not cause communication bottlenecks and single point of failure to the system and maintain the stability of the former system to the utmost. The entire system is composed of the SSL gateway, internal servers and AP, which is illustrated in figure 3.

The article uses OPEN VPN to set up campus network VPN system. It is a type of open source software compatible with various means of identity authentication, including advanced share of private key, third party certificate and user name/password combination. It uses a number of OPEN SSL encryption libraries and SSL V3/TLSV1 and is also compatible with various VPN access schemes like remote access, 802.11 and Wifi etc.

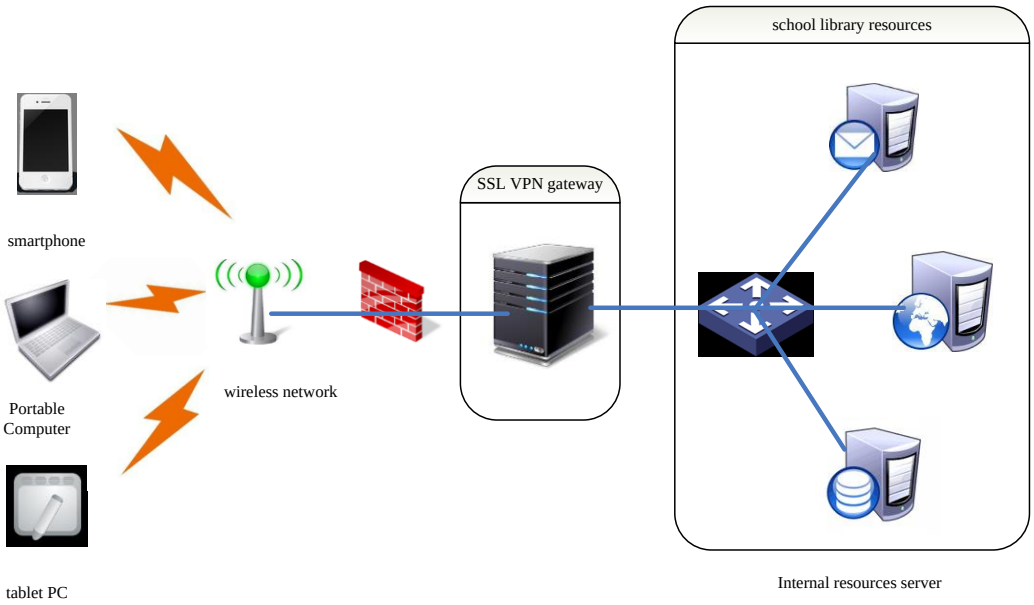

Figure 3. SSL Application System

4.2 Wireless User Authentication Design

4.2.1. Authentication Process: Division of VPN service limits of authority. Conduct security verification on the user environment according to the figure 4 workflow before establishing SSL handshake, and provide corresponding access permits to limits of authority in compliance with the security degree. Detailed process is explained as follows:

(1)Conduct verification on user password and token. SSL connect denied and dialogue closed if either is incorrect; and the process proceeds if both of them are correct;

(2)Conduct security verification on client environment. If the environment is dependable, it will provide a highly authorized service to the user.

(3)If the environment is not reliable, it will request the user to download security monitor and document removal program from the SSL VPN application gateway, confining the client to inferior authorization for access;

(4)If the client computer does not allow downloading and program installation, the system will force close the cashed function on the insecure endpoint and order the user not to buffering download the displayed content, confining the user to inferior authorization for access the server;

(5)Conduct SSL handshake with the client in consistence with the regulatory limits of authorization, and execute examination of encryption algorithm strength on the client computer. If the encryption algorithm strength is lower than the minimum security level preset in the gateway, the connect request will be denied;

(6)Implement SSL handshake and establish connect, providing corresponding SSLVPN access service to the client.

4.2.2. Authentication Implementation: In Linux system, the SSL VPN server uses OpenSSL database function to realize its function: provide SSL encryption/decryption, build up SSL data channel and realize point-to-point secure communication with the client end and the VPN server. Design ideologies stated below can realize user authentication on the SSL VPN server.

(1)Use Apache Server to manage a user access list. This list signifies specific servers accessible to each member and concrete port they need to pass through. This access list be gained by sending a webpage order request in the form of GET url + getserver. List.action +cookie.Url contained in the form stands for the server address; getserver.list.action

means an order for list acquiring; cookie is provided by HTTP protocol to ensure the Web vibration and security. The basic data structure is:

typedef struct { char username[32]； CListlist[size];}

*UserAccessList， * PuserAccessList;*

typedef struct { char m_ip[40] ； char m_netm ask[40]; int32 m_port; char Protocol[10] ； }

*CList， * PList;*

A document form is allowable for storage and management. When a user applies for the list, all lists contained in the C user Access List will be returned to VPN Server.

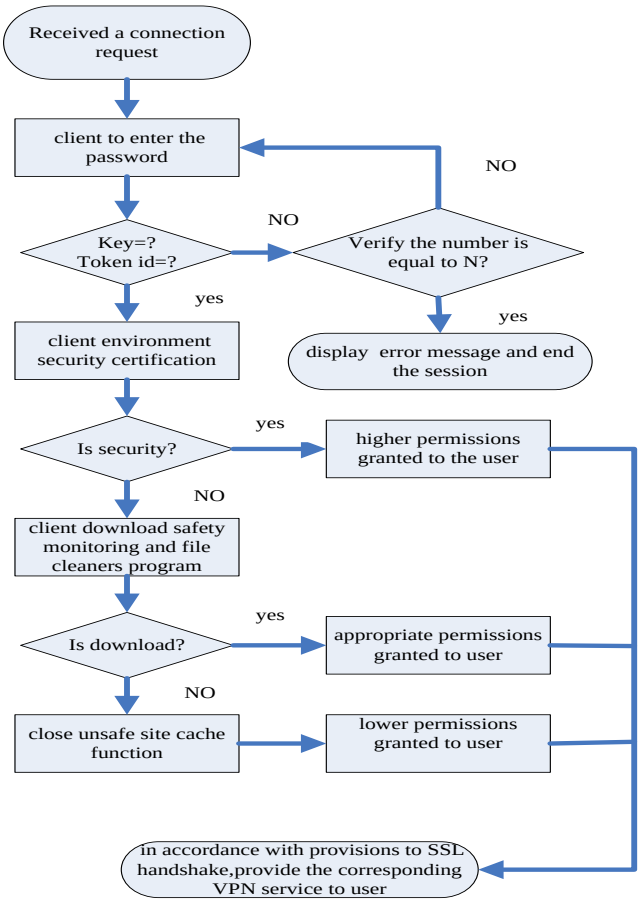

Figure 4. Client Security Certification Process

(2)The client and the SSL VPN server will execute private handshake to testify whether the client is authorized to access the real server. The establishment of private handshake is conducted after the client end gains the list from the server and a link request is sent in use of personal data format. The header format of private handshake requires some changes, and a mar can be added to the head like my head. The entire head is myhead GET url+getserver.List.action + cookie. This head is unidentifiable for the server intended to be accessed, since it is private communication data with SSL VPN. After the SSL VPN server beheads the “my head” mark attached to the request asking for the list, it will transmit to the Apache server and generates a Flag mark. The Apache server will skip over step (1) and return a server list the user is permitted to. The Flag mark means that the client end has already established private handshake with SSL VPN. The SSL VPN server will send the Flag and list to the client end. An Auth-List for user authentication will be maintained on the SSL VPN server.

4.3 System Working Process

The basic workflow in the entire VPN system is specified as follows:

(1) Users connected with campus wireless network connect the SSLVPN server via HTTPS, and the gateway will conduct user authentication (currently it is user certificate authentication). Resources lists are returned to users according to their limits of authorization.

(2) Send a request to the processing module for reception of the data packet, and sent the decrypted data to the access control module.

(3) The tunnel protocol module is responsible for end-to-end tunnel establishment.

(4) The access control module determines whether the user can access the intranet resources according to the preset access control strategies.

4.4 Security Analysis

It is evident by observing figure 3 that, the SSL VPN raised in the article is required to be installed at the back of firewall, and users required to register by the intranet for authorized external access can be moved on SSLVPN. In terms of firewall, the 443 port should be open up for public network users, which can remarkably reduce the chance for the entire network to be attacked by the public network. SSL protocol tunnel established in the application layer functions in virus and worm prevention, and all accesses are transmitted by the SSL VPN gateway to avoid threats posed by direct access to the network layer. Additionally, since the SSLVPN also serves as a server agent, all installed client ends can be protected from virus or hacker attacks. Fine grit mandatory access control and log audit are also permitted.

5. Conclusion

As a new security transmission technology, SSL VPN emerges in response to the ever-increasing demand on network security. As the article mentions, SSL VPN application provides end-to-end connect in the wireless network, and data between the client end and the server is transmitted in encoded form, which ensures the security of network resources and user data. Since SSLVPN not requires client configuration, users are allowed to adopt some traditional application tools at their disposal to realize wireless network access with ease.

Acknowledgements

The authors would like to thankWang Zheng, Wang Ying, Fu Donglai, and Bian jing for their insightful comments and suggestions. The anonymous reviewers also provided valuable feedback. This paper is supported by the Natural Science Foundation of Shanxi Province under Grant No. 2009011022-2 and Shanxi Scholarship Council of China Grant No. 2009-28.

References

[1] Q.-h. Zeng, W.-x. Xu and Q.-p. Lin, “The Construction of Library's Remote Access System Based on SSL VPN”, Information Science, vol. 10, (**2007**).
[2] Y.-K. Ou, J.-L. Zhou, T. Xia and S.-S. Yu, “Research for Virtual Service Based SSL VPN”, Journal of Chinese Computer Systems, vol. 2, no. 27, (**2006**).
[3] Z.-t. Li, J.-m. He and J. Lei, “The Threats in SSL VPN and the Solutions”, Computer Engineering & Science, vol. 8, no. 28, (**2006**).
[4] K. Zhang, B. Bei and J. Zhang, ”Construction of Remote Access System to the Digital Resources Based on SSL VPN”, Journal of Hebei University(Natural Science Edition), vol. 4, no. 33, (**2013**).
[5] S.-s. Yu, L.-j. Dong, K. Ouyang and T. Xia, “Research for STDM Based SSL VPN”, Journal of Chinese Computer Systems, vol. 7, no. 27, (**2006**).

[6] L. Guo and W.-s. Li, "Design and Implementation of SSL VPN", COMPUTER TECHNOLOGY AND DEVELOPMENT, vol. 8, no. 17, (**2008**).
[7] R. Stanton, "Securing VPNs: comparing SSL and IPsec", Computer Fraud & Security, vol. 9, (**2005**).
[8] A. Harding, "SSL Virtual Private Networks", Computers & Security, vol. 5, (**2003**).
[9] T. Rowan, "VPN technology: IPSEC vs SSL", Network Security, vol. 12, (**2007**).
[10] D. Bradbury, "A private path to security", Infosecurity, vol. 8, (**2008**).
[11] Y. Kuihe, "Implementation of Improved VPN Based on SSL"< ICEMI '07. 8th International Conference on Electronic Measurement and Instruments, (**2007**) August 16-18, Xian, Chinese.

Authors

Xingkui Wang, He born in Shanxi Province, China, in 1980. He received the B.Eng. degree in computer application and M.E. degree in network security from Taiyuan University of Technology, Taiyuan, China, in 2002 and 2005, respectively, where he is currently working towards the Ph.D. degree in information security.

In 2005, he joined Taiyuan University of Technology, where he is currently an Assistant Professor with College of Computer Science and Technology. His research interests include network security, trusted computing, virtualization technology, and study the data leak prevention.

Xinguang Peng, He received the B.Eng. degree in Department of Electronic Information and M.E. degree in computer application from Taiyuan University of Technology, Taiyuan, China, in 1979 and 1988. He received the Ph.D. degrees in computer application technology from Beijing Institute of Technology, Beijing, China, in 2004. He joined Taiyuan University of Technology, Taiyuan, China, in 1980, where he is currently a Professor leading his laboratory of network security and technology. He worked in University of Erlangen-nurnber (1993–1994), Bayern, Germany, as a visiting scholar supported by the Ministry of Education. He has authored/coauthored more than 100 journal/conference publications and 8 textbooks. His recent research efforts have been focused on network security, intrusion detection, virtualization technology and trusted computing.

论文题目	**VPN Gateway Research in Wireless Network Based on SSL Technology**		
所属主题	移动安全		
第一作者			
姓名	王星魁	职称/学位	讲师/硕士
单位	太原理工大学计算机科学与技术学院	邮编	030024
地址	山西太原市迎泽西大街79#		
电话		手机	13834645926
Email	wxk0301@163.com		

第二作者			
姓名	彭新光	职称/学位	教授/博士
单位	太原理工大学计算机科学与技术学院	邮编	030024
地址	山西太原市迎泽西大街79#		
电话	0351-6010071	手机	
Email	sxgrant@126.com		