A Critical Review of Technologies Enabling VPN and Secure Remote Access

Lu Wang [1, a], Yanhong Wang [2]

[1]Nari Group, Nanjing, 210000, China

[2]State Grid Nanjing Electric Power Company, Nanjing, 210000, China

[a]Wl881208@gmail.com

Abstract

In the recent years, VPN technologies are wildly implemented in the Internet. VPN is a virtual private network that offers a secure transmission mechanism for data and IP information through networks. It provides the security feature of private network, but without the expense of a physically dedicated network. In order to accomplish secure remote accesses via a VPN, many secure mechanisms and technologies are implemented in a VPN. Typically, IP security (IPSec) that provides protections for IP-level data via encrypting or authenticating all traffic at the network layer are most widely used for a VPN. Also, TLS is able to provide remote accesses VPN capability via launching a browser to establish a VPN connection. In this paper, we address security issues and challenges associated with IPSec and TLS VPN.

Keywords

Virtual Private Network (VPN), Transport Layer Security, IP Security (IPSec).

1. Introduction

The increase development of network technology as long as the increase of remote accesses to the private networks resources and services results in the need for efficiently authenticating and securing exchanges of remote accesses. Typically, the VPN has been designed to address this issue using a public network to transform data between two remote terminals [1]. A VPN offers a secure transmission mechanism for data and IP information between networks. Since a VPN service can be implemented in a exist network, such as Internet, this is less expensive than building a dedicated private network between branch offices or organizations. In addition to this, VPNs provide flexible solutions for securing communications between users and organization's servers, no matter where the users are located. To accomplish these secure remote accesses, it is significantly important for VPNs to implement strong security mechanism enabling two endpoints to be mutually authenticated and to share a secret key protecting their information exchange. There are numerous security technologies that have been widely implemented within VPNs, in particular IP security (IPsec) and TLS. IPsec and TLS are the de facto standards for allowing mutual authentication as well as secret keys exchange.

IPsec is a collection of protocols that offers security service at the IP layer by allowing a system to select required protocols, determine the algorithms to use for the services, and put in place any cryptographic keys required to provide the request services [2]. In general, IPsec provides the IP-level security with peer entity authentication, data confidentiality and key management. The authentication mechanism ensures that all received data are not altered during transmission, and the data are really transmitted from the initial source. The data confidentiality requires transmitted message to be encrypted so that the third party cannot eavesdrop the message. The key management refers to the secure exchange of keys. There are two major protocol components that specify the actual cryptography processing applied to data. One is Authentication Header (AH), which is an extension header to provide message authentication. It provides integrity protection, data origin authentication and anti-replay services for packets through the application of MAC algorithm and the inclusion of sequence numbers in packets [3]. The other one that contains an encapsulating header and trailer to offer encryption and combined encryption and authentication is called encapsulating security payload (ESP). Basically, ESP provides similar services to AH, additionally it provides confidentiality and traffic flow confidentiality services via symmetric key. Security socket layer (SSL) is cryptographic protocol that was designed and implemented by Netscape Corporation. The successor of SSL is transport layer security (TLS) and it is built into major web browsers, such as Microsoft Explorer and Netscape. Therefore, a VPN solution with TLS/SSL can be used via a web browser communication. It also can be used in other application. However TLS/SSLVPN mainly runs an application inside a web browser. TLS is typical client/server protocol, it starts a connection via a TLS handshake including negotiation between end nodes for algorithm support, key exchange and authentication and symmetric encryption and data exchange [4]. Table 1 shows the relative location of security facilities in TCP/IP model.

Table 1 TCP model with TLS/SSL, IPsec in TCP/IP protocol stack

Application Layer(HTTP,FTP,SMTP)---SSH
Transport Layer---TLS/SSL
Network Layer---IPsec
Data Link Layer
Physical Layer

In the next sections, we would introduce how these technologies are deployed in a VPN service. It mainly contains which layer security they provide for VPNs. Meanwhile some feasible risks of these technologies are still discussed.

2. Background and literature survey

2.1 A brief description to VPNS

VPN is a virtual private network that offers a secure transmission mechanism for data and IP information through networks. Since a VPN service can be implemented in a exist network, such as Internet, this is less expensive than building a dedicated private network between branch offices or organizations. In addition to this, VPNs provide flexible solutions for securing communications between users and organization’s servers, no matter where the users are located. VPNs are able to establish a secure communication by using both symmetric and asymmetric cryptography. Asymmetric cryptography applies separate keys for encryption and decryption, while symmetric cryptography use the same key for both encryption and decryption. Because of this, asymmetric cryptography is usually used to authenticate the identities of both parties. Meanwhile, symmetric cryptography is used for protecting actual data [5]. Although VPNS are able to reduce network risks, they cannot completely eliminate risks from networks.

2.2 IPsec overview

IPsec provides the capability to secure communication through LAN, public and private WAN, and through the Internet. There are three IPsec-based VPN architectures that can be implemented by different requirements. Gateway to gateway architecture is deployed by creating a VPN gateway onto each network and building a VPN connection between the two gateways, As shown in Fig.1.

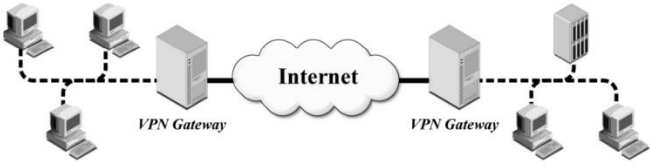

Fig.2 Gateway to Gateway scenario [5]

Another scenario that is used for secure remote access is host to gateway architecture. Typically, the organisation deploys a VPN gateway on its network, remote access users attempting to entry this organisation server is required to build a VPN connection between their local hosts and the organisation's VPN gateway. The remote user's hosts have been configured to act as the VPN clients before establishing VPN connection. When users attempt to build a VPN connection, they are asked to authenticate before the connection can be built. The least implemented VPN method is host to host architecture, which is typically used for special purpose including a system administrator performing management of a remote server [5]. The IPsec usage might be similar among these architectures. Firstly, non-secure IP traffic is conducted on separate LANs. When the traffic is out of bound across a private or public WAN, IPsec mechanism would be implemented, the operation deploys in network devices, such as routers and firewalls. From LAN to WAN, the IPsec device encrypts and compresses all traffic, while the IPsec device decrypts and decompresses all traffic going out from WAN.

Authentication header (AH) and encapsulating security payload (ESP) used by IPsec are to provide security services at the IP layer. Both AH and ESP supports tunnel and transport mode. In tunnel mode, cryptographic protection is provided for entire IP packets. Generally, a whole packet with security filed is acted as the payload of an outer IP packet using a new IP header. Since the original message is encapsulated, no intermediate routers can examine the inner IP header. In tunnel mode, IPsec processing is usually performed at security gateways. ESP in tunnel mode encrypts entire inner IP packet, AH authenticates entire inner IP packet. In contrast, ESP in transport mode encrypts and optionally select authenticates IP payload but not included IP header. AH authenticates IP payload and selected part of IP header. Thus transport mode provides protection primarily for the payload of an IP packet. The header of original packet is preserved meanwhile some security fields are added, and then the payload plus some header fields undergo cryptographic processing...The cryptographic services provided by AH can also be greatly deployed by ESP. Meanwhile ESP provides confidentiality service that AH cannot [3]. Some IPsec implementation is not supported any more [5], and according to RFC 4301 [6], supporting for AH has been downgraded. Based this views, AH might be no longer a required part of IPsec implementation, thus in this paper only ESP will be introduced.

2.3 ESP in IPsec

In tunnel model, ESP can provide encryption and integrity protection for an encapsulated packet. For this mode, the ESP header is prefixed to the packet and then the packet with the ESP trailer is encrypted. It is a good idea to counter traffic analysis. In order to avoid intermediate routers to process ESP encapsulated data, the whole block contained ESP header, cipher-text and authentication data is encapsulated so that this kind of message is only for routing not for traffic analysis. Figure 2 shows the operation of ESP in tunnel mode. Firstly, data going to IP layer is allocated an inner IP packet with a destination address. This packet is prefixed by an ESP header, and the packet and ESP trailer are encrypted. Now the new packet has had a new IP header. Next, the new packet is routed to the destination firewall. During delivering, the intermediate routers cannot process the ciphertext. And then the destination firewall processes the incoming IP header, it decrypts the remainder of the packet to recover the plaintext inner IP packet via the SPI in the ESP [7].

Each ESP header consists of two fields. One is security parameters index (SPI), which is used to identify a security association. The other one is sequence number, which is a monotonically increasing counter value and provides an anti-replay function. The next part of the packet is the payload. It contains the encrypted payload data and unencrypted initialization vector (IV). The third part of the packet is the ESP trailer, which includes padding, padding length and next header. To some extent, adding extra padding is able to hide actual data length so that improving partial traffic-flow confidentiality. Figure 3 shows ESP packet fields.

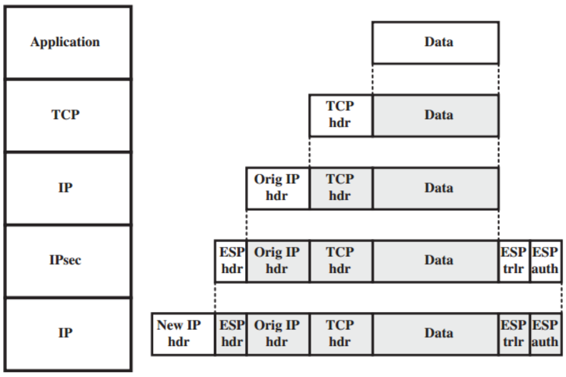

Fig.3 Implementation of ESP in tunnel mode [2]

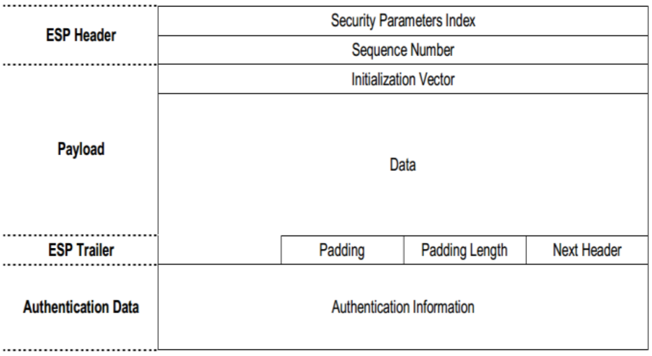

Fig.4 ESP Packet Fields [5]

2.4 Internet key exchange (IKE) in IPsec

The purpose of the IKE is to allow devices to exchange information that is required for secure communication. It implements by allowing security association (SA) to be negotiated, created and managed through a series of ISAKMP [8]. SA is a one way logical connection that affords security to carried data. By default, the key management protocol for IPsec is referred to ISAKMP/Oakeley. The ISAKMP framework is used to provide specific protocol supports including negotiating the SAs. It contains cryptographic keys used for encoding authentication information and performing payload encryption [9]. In fact, ISAMP does not have a dedicated specific key exchange algorithm. Instead, it contains a collection of message types that can use a series of key exchange information. Therefore, the protocol ISAKMP cannot work alone, it might be associated with part of the Oakley that is the specific key exchange algorithm mandated for use with the ISAKMP.

2.5 TLS/SSL VPNS

TLS/SSL is a set of Internet data security protocols that has been widely used for identifying authentication and data transmission between a Web browser and the server. The TLS/SSL can be divided into two layers: SSL handshake protocol, SSL change cipher spec protocol, SSL alert protocol and SSL record protocol [10]. SSL record protocol based on reliable transport protocol is used to provide basic function to high level protocols. SSL handshake protocol is built on SSL recording protocol that allows the client and server to authenticate each other and to negotiate an encryption and MAC algorithm. The SSL protocol format is shown in Figure 4.

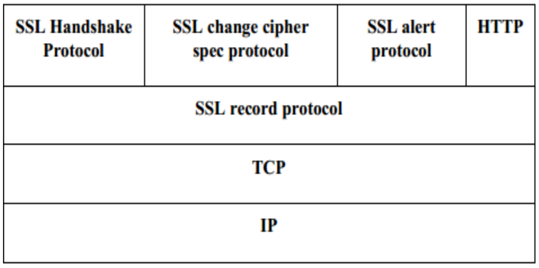

Fig.5 Structure of SSL [10]

The SSL VPN might be accessed from any location, as long as the location has connectivity to the Internet and the user has a web client running particular SSL VPN. All traffic is encrypted during routing to destination gateway. The SSL VPN gateway is the endpoint for the secure connection and provides various services [11]. During an SSL session, three kinds of security can be negotiated by the client and server. Firstly, the client and server need to negotiate the version of SSL as different SSL VPNs use different versions of SSL protocols. After that, cryptographic functions are required to be negotiated. SSL VPNs provides four significant services: confidentiality, integrity, signature and key establishment. Generally, SSL uses cipher suites to define the set of cryptographic functions. Also, the client and the server need to use the same cipher suite. At the last, when a web browser attempts to connect to an SSL VPN, the browser needs to ensure that the server is trusted. To accomplish this, SSL uses certification signed by trusted entities to authenticate the server to the web user.

3. Analysis of IPsec VPNs AND SSL VPNs

3.1 Threads to SSL VPNs

In SSL VPNs, the major security mechanism is referred to authentication and encryption. In terms of authentication, SSL-VPN users installed in public place to login remote network might be hacked by monitor keyboard input software to get username and password. Also hackers can examine the machine memory, cache and browser cooker to look for left information by users. Another thread of SSL VPN is digital certification. SSL enables users to determine whether the server certification is available. However, the user unexpectedly accepted the certification from the hacker, which would result in the “man in the middle” attack, the user thinks of the hacker as a trusted server. In terms of encryption, it is well known that the longer the key, the encryption algorithm might be more complex. SSL usually uses 40 bit or 128 bit RC4 encryption algorithm with shorter key and lower complexity, thus its security is relatively low [10]. Additionally, since SSL VPNs can start a connection from any Internet-based resource, it improves this type of service that the user forgot to close the session when his/her computer is establishing connection to an organisation’s internal network resulting in unauthorized personnel attacking this organisation’s internal network. Besides, SSL VPNs might be more vulnerable to keystroke loggers as public computer that might not meet the organization’s security policies would be involved. Furthermore, during the session period, critical information might be left on a remote computer if the computer is not appropriately protected. This is significantly important when a remote user is shared with the public

3.2 Threads to IPsec VPNs

Although IPsec VPNs can greatly reduce networking risks, they cannot eliminate all risks for network communication. One possible problem is the strength of the implementation. While the encryption algorithm is getting increasing security, absolutely trusted algorithm might be not existed so that flaws in an encryption algorithm could enable hackers to decrypt intercepted traffic. Also, random number generators could not produce enough random values leading to additional attack possibilities.

Specifically, the main drawback of IPsec VPNs is provides entry to the entire subnet under the organisation’s network. This means that if the remote client is infected with virus, the virus might spread over the entire network. When a remote client builds a tunnel with an organization, it can be a target of hackers as the remote client can be changed to a router into the organization during IPsec processing [8]. Also, the access control for IPsec VPNs could be an issue as they bases on network access controls. Since A VPN gateway is uniquely responsible for creating the VPN tunnel, the tunnel is developed the information passing through is not reviewed by any of permissions. Additionally, the IPsec VPNs usually provide encryption between gateways, but the message is not encrypted from LAN network to local gateway. Thus the hacker can listen to the sensitive information within the LAN network. It is difficult for IPsec VPNs to solve the problem of network address translation and crossing the firewall. In a large distributed system environment, the diversified regional security policy can create significant problems for end to end communication [8]. Split tunnelling also is a big issue. A remote client simultaneously exchanges network information with both the public network and the private network without first placing all traffic inside the VPN tunnel so that the hacker in public network can endanger the remote client and use it to access to the private network.

4. Conclusion

This paper focuses on VPN technologies that deploy IPsec or SSL protocols to provide VPNS service. Firstly of all, VPN security mechanism is introduced to provide secure connection. Since it is able to provide required security level and relative low cost to organizations, it has been widely accepted by organization and customers. IPsec protocol as a full-fledged VPN solution was presented in detail, especially in three aspects: authentication, encryption and key management. ESP is only represented as AH is getting less popular and ESP can provide extra security service. Two operation model: transport mode and tunnel mode was shown. Tunnel mode was primarily presented because it is more commonly used in IPsec. Nevertheless, IPsec VPN does not remove all risks from the Internet. There are some networking risks to IPsec VPNs, the paper gives a brief analysis to these risks.

Additionally, SSL VPN is an emerging technology that provides remote access capability by using SSL function that is already built into a modern web browser. This paper briefly presents SSL/TLS technologies that apply in VLNS, also security issues with SSL VPNs are addressed in this paper.

Acknowledgements

This research is supported by the Network design and security access technology research project of terminal communication access network of State, STATE GRID NANJING ELECTRIC POWER COMPANY (Grant No. J2016042).

References

[1] B. Mohamad and H. Ibrahim, “Enabling VPN and Secure Remote Access,” 1- 4244- 0495 -9/ 06/$20.00 ©2006 IEEE, 2006.

[2] S.William, “IP Security,” in NETWORK SECURITY ESSENTIALS Application and Standards Fourth Edition, Pearson education, 2011, pp. 270-274.

[3] K. G. P, “A Cryptographic Tour of the IPsec Standards”.

[4] P. Kotuliak and P. Trúchly, “Performance Comparison of IPsec and TLS,” ICETA 2011 • 9th IEEE International Conference on Emerging eLearning Technologies and Applications • October 27-28, 2011, Stará Lesná, The High Tatras, Slovakia, 2011.

[5] S. Frankel, K. Kent , R. Lewkowski, A. D. Orebaugh , R. W.Ritchey and S. R. Sharma, “Guide toIPsec VPNs-Recommendationsofthe National Institute,” NISTSpecial Publication800-77, 2005.

[6] S. Kent and K. Seo, “Security Architecture for the Internet Protocol,” RFC 4301, Dec 2005.

[7] S.William, “IP Security,” in NETWORK SECURITY ESSENTIALS Application and Standards Fourth Edition, Pearson Education, 2011, p. 281.

[8] A. O, “Analysis of problems associated with IPSec VPN Technology,” 978-1-4244 -1643 -1 /08 /$25.00 ©2008 IEEE, 2008.

[9] H. D and D. Carrel, “The Internet Key,” RFC 2409 (Proposed Standard), Nov 1998.

[10] H. MAO, L. ZHU and H. Qin , “A comparative research on SSL VPN and IPSec VPN,” 978- 1-61284-683-5/12/$31.00 ©2012 IEEE, 2012.

[11] S. Frankel, P. Hoffman, A. Orebaugh and R. Park , “Guide to SSL VPNs-Recommendations of the National Institute”.