International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.2, Issue No.12, pp : 1168-1172 1 Dec. 2013

A Critical Review of Security Mechanisms in Virtual Private Networks

Raj Jirapure, Sanket Jirapure
Department of Electronics,University of York,York YO10 5DD, UK
raj.jirapures@outlook.com,sanket.jirapure@gmail.com

Abstract— ***This paper discusses about the security mechanisms employed by VPN for the purpose of authentication and confidentiality of the network data, with mainly focusing on how these technologies are used, how they provides the protection, and how the potential threats can be used against them. The security mechanisms of VPN are reviewed and analysed in this paper. Security mechanisms as SSL/TLS, IPSEC, etc. which provides encryption and authentication, security between gateways, respectively were summarized.***

In this paper we presented some reviews regarding the use, protection, and potential threats used against VPN security technologies and then discussed according to the requirements of these technologies in the VPN. Finally, we presented some conclusions.

Keywords— ***AH, authentication, confidentiality, encryption, ESP, DoS, HMAC, IKE, IPSEC, SSL/TLS.***

I. INTRODUCTION

Nowadays security is an essential part of any private or peer to peer network in order to protect their networks data from the intruders of the network. For this purpose Virtual Private Network (VPN) is accepted as the firm security solution for the communication over the unsecured IP network. Security services and a tunnel are the two basic components of the VPN. By definition VPN is used to create a private and secured network across the untrusted medium which allows communicating the people over the globe through the public network. The different encryption techniques are used by VPN for the prevention of datagrams and interception through the unsecured public network. It provides three different connectivity models as extranet, intranet, and remote-access which connects different companies, offices, and users respectively [1].

The relation between VPN and security plays a vital role over the globe. Commonly, people would like to share their personal information through the internet with avoiding the man in middle attacks between their communication processes. As IPSEC deals with the Authentication Header (AH) and Encapsulation Security Payload (ESP) in order to provide a security in unsecured IP network. These protocols uses various cryptographic techniques and then data packets are encrypted and transferred over the network. SSL/TLS deals with Hash Message Authentication Code (HMAC) for authentication of network data and Pseudo-Random Function for the generation of keys to provide the protection over the unsecured network.

The paper is arranged as follows. In section II, how the security mechanisms/VPN technologies are used in VPN is reviewed and discussed. In section III, how the level of protection/security provided by the security mechanisms is investigated and discussed. In section IV, how the external threats are used against the security mechanisms is reviewed and discussed. In section V, security mechanisms are analysed. Finally, some conclusions are drawn.

II. USE OF SECURITY MECHANISMS IN VPN

Essentially, the use of security mechanisms in VPN can be done through two secure modes as tunnel mode and transport mode. In these two modes different protocols are used to provide the client to client or site to site security while data is being transfer through the VPN.

Furthermore, these security modes are categorized on the basis of security mechanisms used in VPN.

A. Use of IPSEC security mechanism

There are two secured ways in IPSEC for the data protection as Authentication Header (AH) and Encapsulation Security Payload (ESP), which can be used in either transport or tunnel mode. Garfinkel et al. [2] said that AH is being used to provide a shield of authenticity and integrity of the data which creates Hash Message Authentication Code (HMAC) for each and every transferred packet. There are not many cases where data integrity must take place in the network and due to this AH is not often used. The assurance of the data confidentiality could get through ESP, which is used to encrypt the data packets and also used to secure data integrity but unfortunately ESP is not able to secure the whole data packet in the network as like AH as shown in Fig. 1, [3]. In the calculation of HMAC, ESP does not includes the IP address and thus this does not allows IP spoofing because data authentication takes place at the initialization of the tunnel.

Moreover, Tanenbaum [4] reviews that selecting between AH and ESP, the administrator can transfer data over the network using transport or tunnel mode. The transport mode does not change the original IP header and keep continues to access the IP address and its options as shown in Fig. 2, [3]. The tunnel mode encapsulates the entire packet which includes the IP header and encrypts the original IP address by adding new IP header in front of the packet as shown in Fig. 3, [5] and Fig. 4, [5]. The IP header and data could be observed after decryption of a packet.

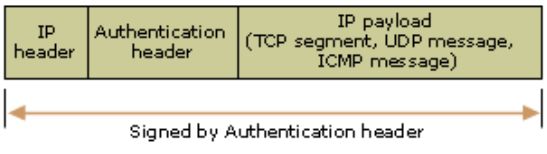

Fig. 1. AH packet authentication

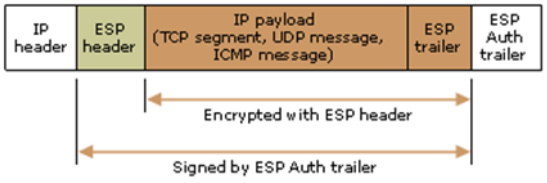

Fig. 2. ESP packet encryption

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.2, Issue No.12, pp : 1168-1172 1 Dec. 2013

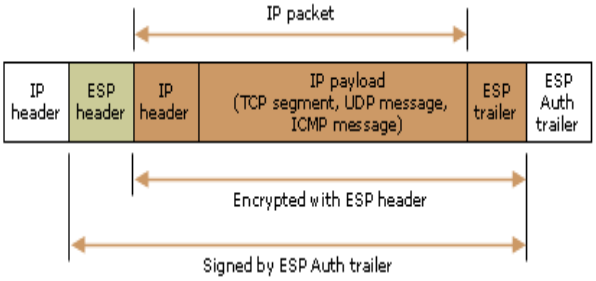

Fig. 3. AH packet authentication in tunnel mode

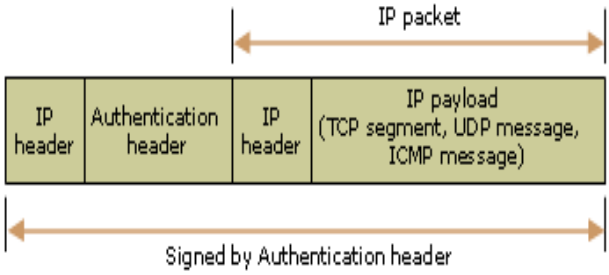

Fig. 4. ESP packet encryption in tunnel mode

B. Use of SSL/TLS security mechanism

As Dierks et al. [6] mentioned that SSL/TLS uses HMAC for authentication of network data and Pseudo-Random Function (PRF) for the generation of keys. There are two layers used by SSL/TLS protocol as record layer and the record layer protocols as handshake, alert, change, cipher spec, and application data shown in Fig. 5, [7].

TLS handshake protocol handles the algorithms used for the authentication and encryption of the data and also manages individual symmetric session keys. TLS uses four keys as encryption key, decryption key, authenticating sent packets, and authenticating arriving packets. Generally, TLS uses certificates for the data authentication, but also having a kind support to the RSA keys. Users can observe the one way authentication while browsing on the web, because server authenticates itself with the SSL certificate.

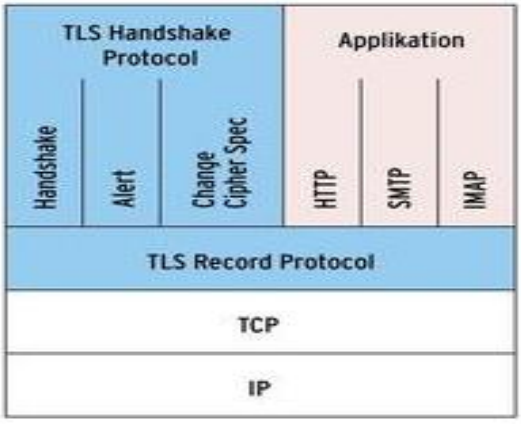

Fig. 5. TLS handshake protocol

III. SECURITY PROVIDED BY VPN TECHNOLOGIES

The level of protection gained in VPN by providing encryption to the tunnels between the authenticated sources and destinations of the network. To get a high level of protection, some cryptographic techniques are used to alter the data into other form which will provides the protection as integrity from the intruders of the network. Protection level of VPN is organized on the basis of security mechanisms.

A. IPSEC protection level in VPN

The cryptographic techniques of AH and ESP protocols based on symmetric keying. According to Harkins and Carrel [8], the Internet Key Exchange (IKE) protocol dynamically negotiates the symmetric keys at the initial establishment of the VPN connection. IKE also provides authentication to the endpoints of the VPN tunnel and negotiates the Service Associations (SA) which keeps the track of the configuration of VPN connection as shown in Fig. 6.

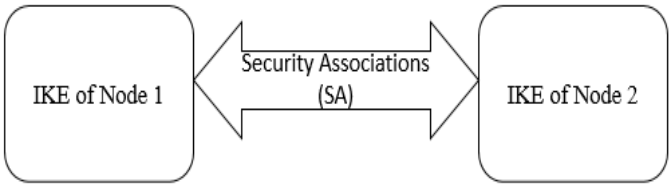

Fig. 6. Security Association (SA)

The IKE protocol passes through two phases while establishing the connection as phase 1 (Main mode) and phase 2 (Quick Mode). In main mode the node partners exchanges four messages to get the symmetric key ID (SKEYID). Using SKEYID three keys are extracted as authentication key, encryption key, and the key which is used with Quick mode. Then two encrypted messages can authenticate the VPN nodes with RSA keys or with pre-shared keys (PSK) as a digital signature. Then same secret passwords are exchanged on both the ends of the connection. The PSKs in main mode deals with only static IP addresses because they are bound to the endpoints of the tunnel and not only used for the data authentication. Garfinkel et al. [9] reviews that when authenticating with certificates, keys are continuously called by the method as Diffie Hellman Key Exchange.

PSKs can also be used to deals with the dynamic IP addresses which will come in Aggressive mode instead of Main mode. In this mode three messages are sent in which PSKs are attached as a Peer-IDs. Domain name or an email address could be act as a Peer-ID. Due to this, each node partner in the VPN connection can be easily recognized the exact PSK. Harkins and Carrel [8], recommends that in theoretical individual keys can be operated by mobile clients as making the use of multiple PSKs.

Schneier [10] mentioned that the negotiation of the symmetric keys begins in phase 2 (Quick mode) after the establishment of the secured connection from phase 1. After the negotiation of the keys, the Ipsec tunnel connection is established and data packets are sent over the network.

B. SSL/TLS protection level in VPN

The SSL/TLS protocol is used to provide protection as the confidentiality of the network data using encryption and also provides the data integrity which is used against the tampering of the actual data. SSL/TLS ensures these methods between the client and the VPN gateway. SSL/TLS protocols is also used between the VPN gateway and web host on the secured network for various applications which requires the data

encryption and integrity protection even they are present on the secured network [11].

Eastlake and Jones [13], comments that the change cipher spec protocol informs to the network node partners to protect all the data packets with the negotiated security context through cryptographic techniques like AES-CBS with 256 bit and SHA1. SSL/TLS is used to support more than above 30 protective contexts in enormous combinational ways. If anything is missing in the process then all nodes communicates with each other through alert protocol.

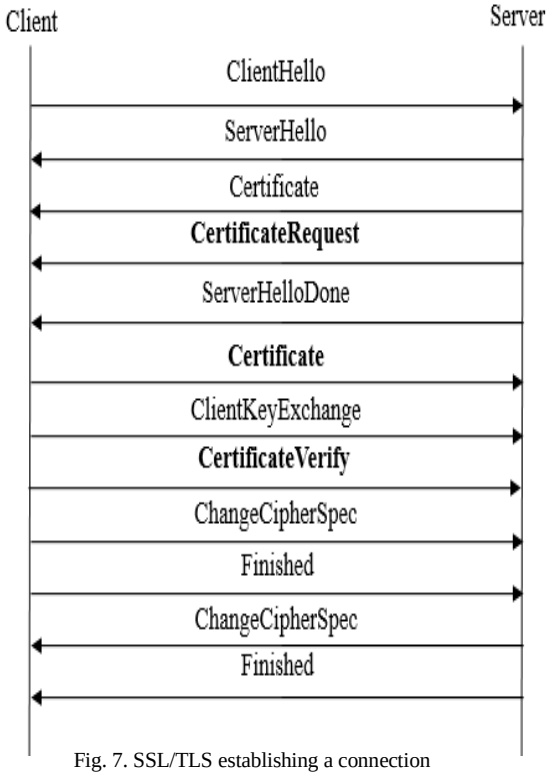

Fig. 7. SSL/TLS establishing a connection

The establishment of SSL/TLS connection uses 12 messages, which are transferred between two server packets and two client packets as shown in Fig. 7, [12]. After establishing the tunnel the TLS record compresses and starts encrypting the network data packets present on the Application Data Layer and send it further to the Layer 4 of the OSI model.

IV. POTENTIAL THREATS USED AGAINST VPN TECHNOLOGIES

There are various types of potential threats that can be used against VPN technologies (Ipsec, ssl/tls, etc.) as intrusion and Denial of Service (DoS). These potential threats are responsible to perform the Man in the Middle Attacks. As Shirey and R. [14] commented that MITM attack refers to a form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data in order to masquerade as one or more of the entities involved in a communication association. The act of bypassing the security is called intrusion which affects the integrity, confidentiality, and the availability of the data. The intruders are used to send packets over the trusted VPN network by which they can intrude the data packets over the network.

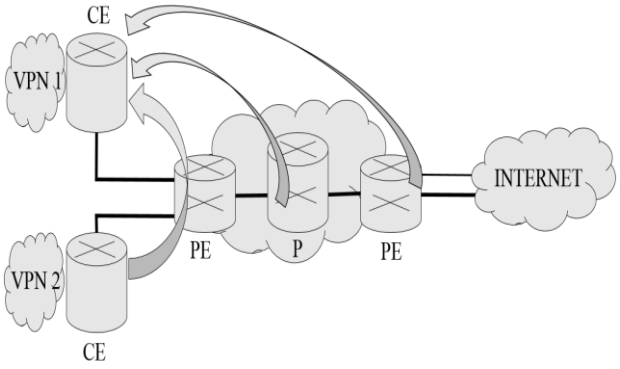

Fig. 8. Intrusion vectors in VPN

Here in this scenario as shown in Fig. 8, [15], two types of routers are used as Client Edge (CE) router which is used to connect to the client site through the service provider and Provider Edge (PE) router which is used to connect to the CE router over the local access link. It also consists of two separate VPN as present in two trusted separate networks which are connected to the IP layer. Here, there is a possibility of the Service Provider engineer could insert some malicious external sites on the trusted VPN networks which tends to the serious threat attacks on the network because the malicious external site will be the part of the trusted VPN and then also have the rights to intrude the data packets.

DoS attacks are considered to be the serious attacks. According to the view of Merike Kaco [16], DoS attacks may be directed at critical components in the VPN path, such as a VPN concentrator that could potentially terminates hundreds of VPN connections. These threats are used to transfer large amount of data into small chunks of messages or continuous packets.

There are two types of methods in DoS attacks as Protocol based attacks and Infrastructure based attacks. Ping of death, black holes, teardrop, TCP SYN flood are the protocol based attacks by which intruder can make use of the weakness in the trusted network protocols and its services in order to intrude the data packets.

Infrastructure based attacks are used to intrude at any point of the trusted network as on CE router or Core router of the network by which there is an increase in jitter, delays, packet loss and also affect hard on the packet delivery ratio. These types of threats can easily intrude due to the decentralized internet infrastructure which causes a serious impact on the operations of the network.

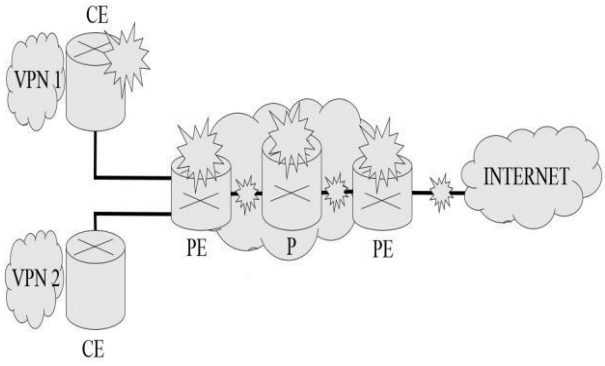

Fig. 9. DoS attack points against VPN

Here the DoS attack points against VPN are shown in the Fig. 9, [15]. In this scenario, the DoS threat model is different from the Intrusion threat model, where the trusted VPN site might receive a malicious DoS attacks on its own network routers but this also impacts very serious on the users of the trusted VPN network indirectly. For instance, PE router is affected by the DoS attacks which also affect the VPN network to which PE router is connected, even though there is no direct DoS attack on the VPN. Due to this, the performance of the trusted VPN networks slows down and which it leads to the increase in the DoS attacks.

V. ANALYSIS OF SECURITY MECHANISMS

Previous sections regarding the security mechanisms of the VPN in this review paper are analyzed. As a part of the protection in IPSEC VPN, we mentioned in the Section III that after the setup of the IPSEC parameters by IKE protocol, the encryption keys among the partner nodes get exchanged with the help of RSA keys and PSKs. Then the negotiation of these keys takes place after establishment of connection between node partners and can ready to send the data packets between each other. We consider that there is a need of a node partner authentication after the Main mode by inserting the valid login and password for each node partner in a trusted VPN network. As R. Barbieri et al. [17] proposed that Extended Authentication XAUTH as an enhancement for an authentication which is secured by IKE in main mode that needs a shared key or a certificate.

Intrusion threat can be used against trusted VPN networks which effects on the data packets of the network, confidentiality, and integrity of the packets. Intrusion attack is just a type of a malware attacks over the network which is used to send to any CE router through the data packets and then tampering of the data can be done on a CE router. The simplest way we think that these malwares must be identified on the network and then there is a need to block those data packets in which these types of malwares are present. Operating Systems firewall could perform this action in order to get protection or the other way that there is a need of anti-virus firewall protection which is used to resists these types of malwares.

DoS attacks are the most malicious attacks for the VPN to handle. As we described in section IV, DoS attacks are used to get affected only on the PE router of the network through these routers they are able to access the trusted VPNs and then able to attack on each user which is connected to that trusted VPN network. For instance, if we got the initial point of the attack then IP address can easily traced and may be possible to block the data packets. Secondly, we think to make the use of packet tracer which allows to pass the data packets through the trusted VPN networks and if any unwanted packet is being passed then it may be dropped or blocked manually. This might be a good to secure the VPN. If the DoS attacks are takes place only on the PE routers then instead of the packet tracer, a packet filter is more affordable. This packet filter might be possible to use on each node of the network but more efficient in the cost if we used it on the routers of the network. Packet filter is used to filter all the packets randomly with unrouting the IPs. Due to this it allows the packets to pass by the trusted VPN only if the packets having the registration with the VPN and else the unwanted packets might be blocked by the routers.

VI. CONCLUSION

In this paper, we presented a review by different authors on the security mechanisms of the Virtual Private Network (VPN). Moreover, we defined and explained how these security mechanisms used in the VPN using

Authentication Header (AH), Encapsulation Security Payload (ESP) protocols, TLS Handshake protocols, and TLS Record protocols. Then the protection level of the security mechanisms are reviewed and discussed using Internet Key Exchange (IKE) protocol used for the authentication and encryption of the node partners in the VPN. We analyzed that more authentication is needed for the encryption keys after main mode and before quick mode by using a valid user id and password which is secured by a shared key or a certificate. Then various potential threats can be used against the VPN technologies are reviewed and discussed using Intrusion and Denial of Services (DoS) attacks. We analyzed on the basis of the security, there are weaknesses on both of these attacks and provided a solution to recover from those attacks.

Finally, we reviewed all the security mechanisms in VPN including their use, protection level, and the potential threats used against them successfully.

REFERENCES

i. A. W. B. Diab, S. Tohme, and C. Bassil, "VPN Analysis and New Perspective for Securing Voice over VPN Network", presented at the Fourth International Conference Networking and Services, 2008, pp. 73-78.

ii. S. Garfinkel, G. Spafford and A. Schwartz, "Practical Unix & Internet Security", Sebastopol, California, O'Reilly Media, pp. 191, 2003.

iii. Microsoft Corp. (2005, Jan. 21). Transport Mode. [Online]. Available:http://technet.microsoft.com/en-us/library/cc739674(v=WS.10).aspx

iv. A. S. Tanenbaum, "Computer Networks", New Jersey, Prentice Hall, 2003, pp. 773.

v. Microsoft Corp. (2005, Jan. 21). Tunnel Mode. [Online]. Available: http://technet.microsoft.com/en-us/library/cc737154(v=ws.10).aspx

vi. T. Dierks, et al. "The TLS Protocol", Sterling, USA, Internet Engineering Task Force, 1999.

vii. A. Leitner. (2002). Transport Sicherung. Linux Magazine. [Online].Available http://www.linux- magazine.de/Ausgaben/2002/04/Transport-Sicherung

viii. D. Harkins, and D. Carrel, "The Internet Key Exchange", Sterling, USA, Internet Engineering Task Force, 1998.

ix. S. Garfinkel, G. Spafford, and A. Schwartz, "Practical Unix & Internet Security", Sebastopol, California, O'Reilly Media, 2003, pp. 182.

x. B. Schneier, "Secrets and Lies", New York, Wiley Computer Publishing, 2000, pp. 86.

xi. S. Frankel, P. Hoffman, A. Orebaugh, and R. Park, "Guide to SSL VPNs", Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology U.S. Department of Commerce, MD 20899-8930, 2008, pp. 3-6.

xii. Cisco Systems, Inc. (2002). Implementing Adjacencies. [Online]. Available: http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/sbc_adj.html

xiii. D. Eastlake, and P. Jones, "US Secure Hash Algorithm 1". Sterling, USA, Internet Engineering Task Force, 2001.

xiv. R. Shirey, "Internet Security Glossary", Request for Comments 2828, May 2000

xv. ETutorials.org. Threats against a VPN. [Online]. Available: http://etutorials.org/Networking/MPLS+VPN+security/part+I+MPLS+VPN+and+Security+Fundamentals/Chapter+2.+A+Threat+Model+for+MPLS+VPNs/Threats+Against+a+VPN/

xvi. M. Kacou, "Designing Network Security", Cisco System, Inc. Vol. 2, 2004, pp. 277.

xvii. R. Barbieri, D. Bruschi, and E. Rosti. "Voice over IPSec: Analysis and Solutions". 18th Annual Computer Security Applications Conference San Diego California, Dec2002.