A New Approach for the Security of VPN

Conference Paper · March 2016

DOI: 10.1145/2905055.2905219

CITATIONS
37

READS
13,701

2 authors:

Kuwar Kuldeep Veer Vikram Singh

1 PUBLICATION **37** CITATIONS

SEE PROFILE

Himanshu Gupta

Amity Institute of Information Technology

64 PUBLICATIONS **311** CITATIONS

SEE PROFILE

A NEW APPROACH FOR THE SECURITYOF VPN

Kuwar Kuldeep V V Singh
PG Student
Amity Institute of Information Technology,
Amity University Campus,
Sector-125, Noida (Uttar Pradesh), India
+91-8373923353
kulsinghdeep@gmail.com

Himanshu Gupta
Senior Faculty Member
Amity Institute of Information Technology,
Amity University Campus,
Sector-125, Noida (Uttar Pradesh), India
+91-9911987390
hgupta@amity.edu

ABSTRACT

In present days, Internet has become mainstream of the network technology for low cost communications architecture, also it brought great convenience for the organizations and businesses to support growth of their business. Since Internet is highly available in almost all the regions, it is oftenrequired by the businesses for their local presence. Thus, a secure channel within this communication network is required for the security of the confidential data traversing in the public network. Due to rapid growth ofthe digital devices and their access to the Internet caused security threats to user data. Advance measures and high technical skills adapted by the attackers, security and privacy threats has become more and more sophisticated day by day, which increases the demand foran updated and highly secure medium to secure entities and their valuable information into the Internet. There are many solutions present in the market today to choose from, out of which Virtual Private Network (VPN) is highly preferred to create a secure medium within the public Internet. It provide convenience of public network and security of private network by forming a tunnel between sender and receiver. VPN also encrypt upper level protocol information contained in its header. This paper discusses about the traditional security measures of VPN and a whole new approach for VPN security by using multi-phase encryption technique [1]. Since most user does not care about the complex underlying technologies, rather they are only concerned about the security of their data traversing in the public network. Thus, the proposed solution will only applicable for the security of user's data carried by the VPN Header. Additionally,the proposed solution will increases the complexity ofencryptionalgorithm used by VPN techniquewhich will enhances the security commitment of the user's privacy in the public communication network.

Keywords

VPN; VPN Multi-Phase Encryption Technique; Secure Tunnel; VPN Security

ICTCS '16, March 04-05, 2016, Udaipur, India © 2016 ACM. ISBN 978-1-4503-3962-9/16/03…$15.00 DOI: http://dx.doi.org/10.1145/2905055.2905219

CCS Concepts

Security and privacy → Formal Security Models

1. INTRODUCTION

VPN (Virtual Private Network) is a networking architecture which is implemented over public network to support privacy in shared public network, it emerged as a cost efficient and reliable solution in networking and telecommunication organizations. VPN are most favorable part of any IT industry because it saves the huge cost of infrastructure by using the public Internet to establish highly secure communication medium from corporate-office to remote sites and remote users.

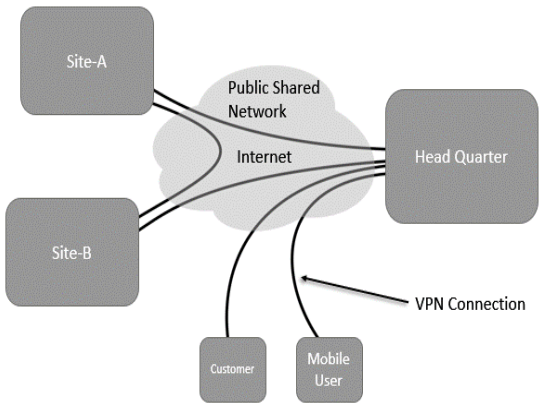

Figure 1. Typical VPN Scenario

VPN uses tunneling protocol to support its functionality. Tunneling protocol provides a secure mode of transport for the network services which elemental network does not support directly [10]. The VPN service can be looked from the perspective of different stockholders, presenting the views of the user, customer, network provider and service provider [4].

VPN establishes a logical secure channel [3] for communication between two entities over Internet by using the method of tunneling, which encapsulates the IP datagram into a tunneling protocol thus hiding the original data from intruder or hacker who are present in almost all the networks. It virtually establishes a point-to-point or multipoint link between the communicating parties in both the transmitting and receiving ends through public or shared communication network. Traditional VPN uses DES (Data Encryption Standard), AES (Advance Encryption Standard)

and Blowfish algorithm for encryption of user's data. The link in whichencrypted and encapsulated data is sent is known as VPN connection.

2. BACKGROUND AND DEVELOPMENT

Few decades ago, VPN was proposed as new concept to harness the great convenience and availability of the Internet such that it can be used as secure medium for private disposal. VPN creates a logical private network under public communication network which reduces the need of costly leased lines connections for businesses and organizations. Today VPN is being used byalmost all businesses who require to geographically expand their operation without much investing in IT infrastructure. Most vendors such as Cisco, Checkpoint and Microsoft, etc. began developing such product that provide secure channel to the business for their development needs. Early VPN development was operational in proprietary environment, the method of encryption and their supported protocols made it either a very good choice or a bad one because it can be easily compromised. Nowadays, IPsec-based VPN became an industry standard because IPsec along with its relative protocol provides adequate encryption, complexity and security to ensure that data integrity is maintained throughout the session [9].

VPN enables a computer or network-enabled device to securely send and receive data across shared or public networks as if it is directly connected to the private network, while benefiting from the functionality, usability and management policies of the public network [5]. User data may contain private information, confidential file, voice, video and most importantly financial transactions. So security of user data needs to be ensured, the commonly implemented VPN remains confined to DES (Data Encryption Standards) encryption algorithm for encryption of user data inside an encapsulated tunnel packet. DES is considered as highly complex and infeasible to decrypt without knowing the keys, it also been proved that even a supercomputer will took years to decrypt a single DES encrypted packet. But we should also consider the growth of the computer technologies and its related threat.

To further enhance the security of user's data in a VPN header, a complex algorithm is needed to prevent data tampering even in the case of compromised link. Multi-phase encryption algorithmprovides such a complex and robust mechanism to secure data inside a packet by performing encryption using different encryption algorithm in multiple level and multiple times, which is also been proven as very secure mode of encryption by using the standard encryption technique. In multi-phase encryption technique, even an outdated algorithm can be used to enhance the complexity of cipher text and overall making more secure packet.

3. ROLE OF MULTIPHASE ENCRYPTION TECHNIQUE IN VPN SECURITY

Multi-phase encryption algorithm is proven to be more secure as compare to traditional encryption techniques such as DES (Data Encryption Standard), AES (Advance Encryption Standard), and DSS (Digital Signature Algorithm). By using this approach of encryption we will ensure the confidentiality and integrityof thevaluable user's data inside an encapsulated packet of the tunnel which is used by the VPN.

The proposed technique will not interrupt any operations of the VPN and its tunneling process rather it only applies to contained user data by the tunnel encapsulated packet, by applying multiple encryption multiple times produced cipher-text is highly complex and tamperproof. When applying this technique with the user data in each packet of the session will produce a highly complex and unbreakable cipher-text, which will be very sophisticated for the intruder to break or reverse the algorithm. Therefore, users will be benefited with the enhanced security of their valuable data.

Businesses such as e-commerce, health care, legal, etc. they all can able to get the advantage of the public communication network without compromising their confidentiality and privacy. The proposed technique will offer highly complex, secure, and tamperproof solution for those clients who are more concerned about their privacy. In addition of business organizations, military operations such as in case of disaster, terrorist attack, hijack, etc. can also be benefited by the VPN and its proposed encryption technique.

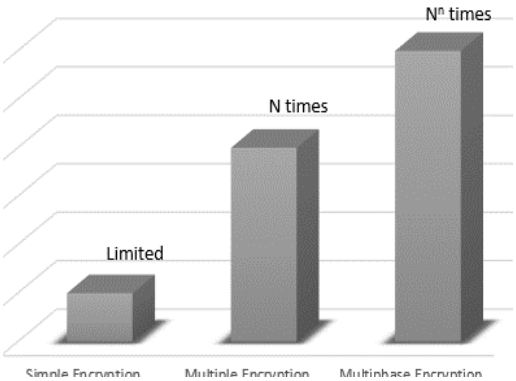

Figure 2. Complexity of Encryption Algorithm [1]

There are many encapsulation protocols which are already operational for tunneling of VPN such as PPPTP, L2TP, SSTP, each of the protocols demands certain system requirements and has their own strength and weakness as discussed below-

3.1 PPPTP

Point-to-Point Tunneling Protocol, it support multiprotocol to be encrypted and encapsulates traffic within IP packets, it uses the custom built version of the GRE (Generic Routing Encapsulation) to encapsulate frames of PPP. PPPTP uses the same authentication as PPP (Point-to-Point Protocol). Its strength depends on password strength which is used for authentication to provide security. PPTP has only the efficiency to encrypt data along 128-bit key so it does not ensures good security. However, it is generally used with multi-level of encryption and authentication.

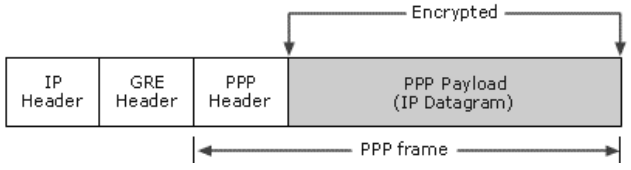

Figure 3. Encapsulated packet in PPPTP [11]

3.2 L2TP

Layer 2 Tunneling Protocol integrated the features of PPPTP with L2F (Layer 2 Forwarding) protocol, developed by CISCO Systems. Tunneling is done by using multiple levels of encapsulation that are L2TP, UDP (User Datagram Protocol), IPSec (IP Security), IP (Internet Protocol) and Data-Link, in which IPSec serves the encryption for L2TP tunnels. It does encapsulation in two layers:

Layer 1: L2TP encapsulation

PPP frame enclosed with the header of L2TP and UDP.

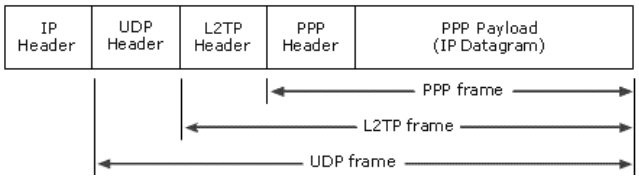

Figure 4. Encapsulated Packet in L2TP [11]

Layer 2: IPsec encapsulation

The resultant message is further enclosed with an IPsec header. IPsec is designed to specify security in between communication channel of two communication devices such as gateways, routers and firewalls. IPsec is a protocol suit developed for securing IP protocol communications by encryption and authentication of each IP packet during session. Traditional IPv4 architecture is not such designed for IPSec, while it is a built-in feature of IPv6.IPSec provides two security protocols [6]-

1. Authentication Header (AH) secures the source and destination addresses of the IP header by using a hash function with a secret key.
2. Encapsulated Security Payload (ESP) provides integrity, confidentiality and authentication and allows for encryption of payload, ensuring data integrity and data confidentiality.

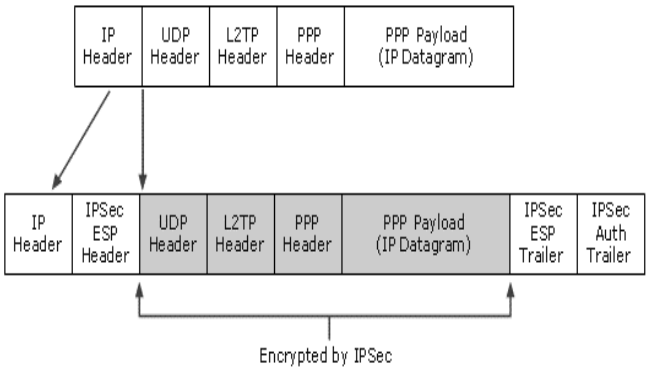

Figure 5. Complete encapsulated packet of L2TP [11]

3.3 SSTP

Secure Socket Tunneling Protocol is a latest tunneling protocol which uses HTTPS (HTTP Secured) protocol over 443 port of TCP connection to transit traffic through proxies and firewalls which might block PPTP and L2TP traffic. It facilitates mechanism to enclose PPP traffic over SSL (Secure Socket Layer) protocol which support TLS (Transport Layer Security) integrated with improvised key exchange, encryption, data confidentiality, data integrity and authentication. It was built to support remote clients, it typically does not have the capability to support site-to-site VPN tunnels. SSTP experience similar performance constraints as any other IP-over-TCP tunnel observe during session. Typically, performance is fair till sufficient excess bandwidth is present on underlying network.

Table 1. Advantages and Disadvantages of VPN Protocols [7]

	ADVANTAGES	DISADVANTAGES
PPTP	• Less network overhead. • PKI not required. • More connections of PPTP support in VPN server. • In PPTP NAT traversal, NAT compatibility is supported.	• Security and firewall problems. • Support only one tunnel at a time for each user. • No additional authentication. • Access control based upon packet filtering.
L2TP	• Support both IP and Non-IP networks. • Multiple protocol support. • More authentication protocol supported. • Simultaneous multiple support of tunnel. • In IPSec NAT traversal, NAT compatibility is supported.	• Performance issues. • Less connections of L2TP support in VPN server.
IPSec	• Flexible • Configuration is not required to user devices. • More secured data and key exchange. • Supports integrity of the transmitted data. • Compatible with variety of encryption algorithm. • Optimal for gate-to-gate VPN solutions. • Best for always-on connections. • Compatible with NAT.	• Complexity is more. • Only identifies devices. • Routing capabilities not embedded. • Only IP protocol supported. • Reduces performance of the network. • Whole network or subnet will be vulnerable.
SSL/TLS	• VPN client not required. • More secured data and key exchange. • Permits particular resource access in the network.	• Only compatible with web-based applications. • More complex firewall configuration needed. • Increases IT hours in deflecting DoS attacks.

4. OVERVIEW OF THE PROPOSED VPN SECURITY TECHNIQUE

Proposed technique of VPN encryption in which Multi-phase encryption is used for payload encryption, will only be applied to thedata inside theIP packet of the encapsulated tunnel packet. Rest all of the field will be untouched during the session. Presently, user data is encrypted with DES, AES or Blowfish algorithm to avoid data tampering or abuse. In proposed technique, user data will be encrypted using multi-phase encryption algorithm and encapsulated by traditional encapsulation method which will

enhance payload security and integrity even if the communication medium is compromised.Rest all operation of encapsulation, authentication and ESP encryption will remain same, thus no other modifications in operation is needed. This will facilitate proposed technique to be implemented in production environment without modifying the whole working of VPN tunneling. Given below figure demonstrates the typical header format of traditional VPN security and proposed VPN encryption technique.

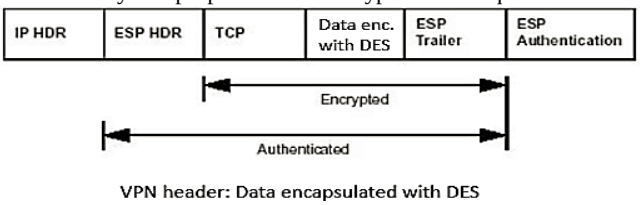

Figure 6. Standard VPN Packet

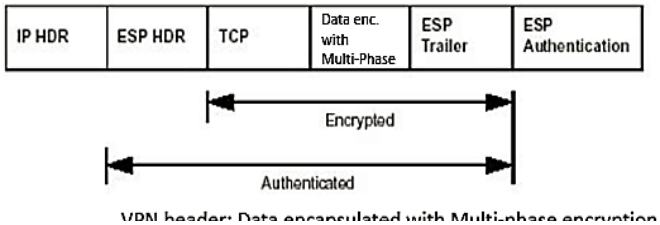

Figure 7. Proposed VPN Packet

Today's mostly VPN provider offering various mix of encryption algorithms for authentication, handshake encryption as well as data encryption inside tunnel packet to prevent active attacks. Widely adapted encryption algorithm currently used in VPN security are –

a. SHA for authentication
b. AES or Blowfish for Data encryption
c. RSA or ECC Handshake encryption

To increase speed of VPN connection users can opt out any security algorithm used in various stages of VPN tunneling. Since our proposed architecture only applies to payload inside TCP header of the tunnel packet, it can also replace the need of connection security if the speed is more desired.

CISCO has recently launched and demonstrated the use of its virtual router[8]CSR (Cloud Service Router) 1000V in the various production environment such as health sector, financial institution, military operations, cloud, etc. They have extensively used VPN connections for the purposes such as in Secure Electronic Transactions[7], confidential data transfer over the Internet, highly secure channel for sensitive information or making user isolation in a shared environment. By implementing the proposed technique in their virtual router architecture they can be benefited from a highly secure medium for user data integrity.

5. FUTURE SCOPE

Increasing demand of security will bring this concept of VPN in the front of the other solutions, as we know already VPN is widely adaptable by many business organizations a highly secure channel is demanded. We will develop an efficient algorithm to implement multi-phase encryption algorithm in VPN encryption process such that it will be properly functional in traditional VPN technologies. To further implement it in networking devices, we will design a SoC (System on Chip) based module which will help to reduce processing load from the mainstream system (routers and servers) and serve as a VPN concentrator module. Nowadays, these module are very well known and are used widely in many small and large organizations.

6. CONCLUSION

In this paper, we have proposed an implementation scenario of a very robust, complex, advance and secure method of encryption algorithm i.e. multi-phase encryption algorithm. Due to its complexity and number of operations it will be only used for payload encryption in a VPN packet. Modern emerging trends and technologiessuch as social media, file sharing apps, utility apps tracks user's data which is being recorder for enhancing app experience. These trends brings private and confidential data of the user into the public Internet which is vulnerable to theft or abuse by any attacker or intruder. Thus a more complex and secure communication medium is required to make positive use of the modern digital services developed for mankind. The advantages of the multi-phase encryption algorithm is that it addresses the problem of data theft, tampering or misuse if VPN connection is hijacked or abused. Therefore if the service is compromised, anyhow data will always remain safe and secure. Additionally, the disadvantage of this proposed method is it will require more computing resources in both ends of the communicating party. However, today's modern computer systems and devices are equipped with ample computing power to fulfill the requirements of the proposed technique.

7. ACKNOWLEDGEMENTS

The author would like to sincere and heartfelt obligation towards Dr. Himanshu Gupta, senior faculty, Amity University, Noida for his grateful guidance and kind support to publish this paper. And like to thank all the personages who have helped me in this endeavor. Without, their active guidance, help, cooperation and encouragement, I would not have made headway for the paper. At last but not least our gratitude goes to all of our friends and colleagues who directly or indirectly helped us to complete this paper.

8. REFERENCES

[1] Himanshu Gupta and Vinod Kumar Sharma, Multiphase Encryption: A New Concept in Modern Cryptography, *International Journal of Computer Theory and Engineering* vol. 5, no. 4, 2013, 638-640.

[2] Baukari N., and Ali Aljane, Security and auditing of VPN. In *sdne*, IEEE, 1996, 132.

[3] Luo, Zhiyong, et al., Research of A VPN secure networking model.*Proceedings of 2013 2nd International Conference on Measurement, Information and Control*. 2013, 567-569.

[4] OSI, "Security Audit Framework in Open Systems-Part 7", ISO/IEC CD 10181, 1993, 7.

[5] Mason, Andrew G, Cisco Secure Virtual Private Network, Cisco Press, January 4, 2002.

[6] Wafaa Bou Diab, Samir Tohme, Carole Bassi, VPN Analysis and New Perspective for Securing Voice over VPN Network, Networking and Services, Fourth International Conference, 16-21 March, 2008, 73-78.

[7] Gupta, Himanshu, and Vinod Kumar Sharma. Role of multiple encryption in secure electronic transaction. *International Journal of Network Security & Its Applications (IJNSA)* 3.6 (2011), 89-96.

[8] Wilson Talaugon, Sridhar Subramaniam, Bill Chin, Itai Aaronson,System and method for virtual router failover in a network routing system, US 7096383 B2, Aug 22, 2006.

[9] Chris Partsenidis, History of VPN: Disadvantages of early virtual privatenetwork, Search Enterprise WAN, http://searchenterprisewan.techtarget.com/tip/A-history-of-VPN-Disadvantages-of-early-virtual-private-networks.

[10] Wikipedia: The Free Encyclopaedia, Tunneling Protocol, http://en.wikipedia.org/wiki/Tunneling_protocol

[11] MicrosoftTechNet: VPN Tunneling Protocols, https://technet.microsoft.com/en-us/library/cc771298