Imperatives and Issues of IPSEC Based VPN

Miteshkumar Shaileshbhai Parmar, Arvind D Meniya

Abstract*— *VPN is Virtually connected networks. It is widely accepted technology for corporate world for enhancing their business. IPSEC is standard for securing packet transmission over public networks. IPSEC private network layer security and more suitable for VPN technology. In VPN network which are mainly using public network(internet) required more secure mechanism for data transmission between to node or host(Gatewayes). This article extensively and exclusively studies the issues involved in IPSEC base VPN network. and possible solution for application base protocol implementation which can be exploded as further research purpose.

Index Terms*— *Authentication Header (AH), Encapsulating Security Payload(ESP), IP Security (IPSec), Tunnel, Transport, Virtual PrivateNetworks (VPN), Quality of Service (QoS).

I. INTRODUCTION

Virtual Private Network (VPN)

VPN is stands for virtual private network. The Internet has become a popular, low-cost backbone infrastructure. the VPN concept comes in between public and private networks by offering The possibility to building almost a safe, private network over public network. VPN is the most cost-effective method to establish the point-to-point connection between remote users and corporate network. public network(s) like the internet. VPN enhance the traditional dial-up and uses the public Internet resources as a continuation of cooperate network, which minimize the expensive long-distance charge

Challenges in VPN

- Security.
- Quality of Service (QoS).
- Expandability and flexibility.
- Manageability.
- Low cost.
- Dynamic network topology
- Speed
- Frequency of updates or Network overhead
- Simulation and performance issues

IPSec is stand for Internet Protocol Security. IPSec protocol provides an end user to end user traffic with ensuring authenticity and confidentiality of data packet. IPSec supports network level data integrity, authentication and encryption and provides security within the network unlike firewalls and secure routers. IPSec is officially specified by the Internet Engineering Task Force **(IETF)** in a series of Request for Comments addressing various components and extensions, including the official capitalization style of the term. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session[1].

IPSec can be used to protect data transmission between two hosts, between a pair of security gateways (e.g. firewalls or routers). IPSec is a dual mode, end-to-end, security scheme

operating at the Internet Layer of the Internet Protocol Suite

(Fig 1)or OSI model network Layer 3. Initially VPNs relied on dial-up connections but the increasing availability and decreasing cost of broadband internet connectivity has attract companies to develop internet VPNs to provide cost effective and more flexible solution.[4]

The basic services that IPSec provides are:-

1. Access Control How should the load on the visited Web sites be minimized?
2. Connectionless integrity
3. Origin authentication
4. Rejection of replayed packet
5. Replay protection

II. IPSEC FUNDAMENTAL

This section will focus on the three primary components. The Encapsulating Security Payload (ESP), Authentication Header (AH), and Internet Key Exchange (IKE) protocols. Explaining the purpose and function of each protocol, and showing how they work together to create IPsec connections. IPsec is a collection of protocols that assist in protecting communications over IP networks[2].

1. **Authentication Header (AH)**

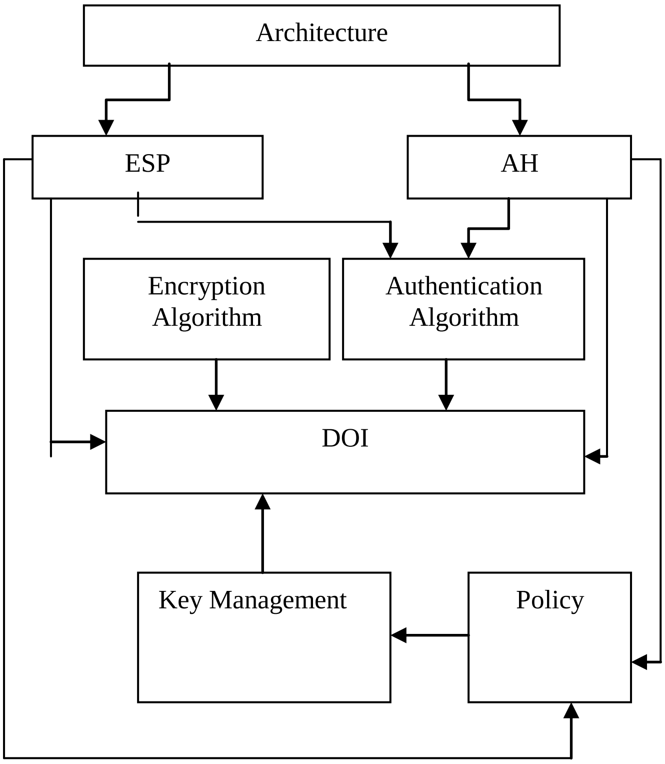
AH[3],one of the IPsec security protocols, provides integrity protection for packet headers and data, as well as user authentication. AH provides authentication for IP header as well as for upper layer protocol. AH cannot encrypt any portion of packets.

AH has two modes: transport and tunnel. In tunnel mode, AH creates a new IP header for each packet; in transport mode, AH does not create a new IP header. IPsec uses hash message authentication code (HMAC) algorithms ,which perform two keyed hashes. Examples of keyed hash algorithms are HMAC-MD5 and HMAC-SHA-1. Another common MAC algorithm is AES Cipher Block Chaining MAC (AES-XCBC-MAC-96).

Manuscript received January 10, 2013.

Miteshkumar Shaileshbhai Parmar,, PG Student at Department of Information Technology , S S Eng. College, Bhavnagar affiliated to GTU , Gujarat, India.

Prof. Arvind D Meniya, Assistant Professor at Department of Information Technology , S S Eng. College, Bhavnagar affiliated to GTU , Gujarat, India.



(Fig.1 Basic Structure of IPSec)

1.1. AH Summary

AH provides integrity protection for all packet headers and data.

Because AH includes source and destination IP addresses in its integrity protection calculations, AH is often incompatible with NAT.

AH still provides one benefit that ESP does not: integrity protection for the outermost IP header.

Next Header	Payload Length	Reserved
Security Parameters Index		
Sequence Number		
Authentication Information		

(Fig 2 AH Header)

2. Encapsulating Security Payload (ESP)

ESP[4] is the second core IPsec security protocol. In the initial version of IPsec, ESP provided only encryption for packet payload data. . Integrity protection was provided by the AH protocol if needed, In the second version of IPsec, ESP became more flexible. It can perform authentication to provide integrity protection, although not for the outermost IP header. Also, ESP.s encryption can be disabled through the Null ESP Encryption Algorithm[13].

ESP has two modes: transport and tunnel. In tunnel mode, ESP creates a new IP header for each packet. The new IP header lists the endpoints of the ESP tunnel as the source and destination of the packet.

The ESP header can also provide the following types of protections offered by AH:

2.1.1. Connectionless integrity

2.1.2. Data origin authentication

2.1.3. Replay protection

2.2. ESP Summary

In tunnel mode, ESP can provide encryption and integrity protection for an encapsulated IP packet, as well as authentication of the ESP header

In transport mode, ESP can provide encryption and integrity protection for the payload of an IP packet, as well as integrity protection for the ESP header. Transport mode is not compatible with NAT.

Security Parameters Index			
Sequence Number			
Initialization Vector			
Data			
	Padding	**Padding Length**	**Next Header**
Authentication Information			

(Fig 3 .ESP Header)

3. Internet Key Exchange (IKE)

The purpose of the Internet Key Exchange (IKE) protocol is to negotiate, create, and manage security associations(SA). That is accomplished through a two-phase protocol. Phase 1 establishes an Internet Security Association and Key Management Protocol (ISAKMP) SA which is a secure channel through which the actual IPSec SA negotiation can take place. Phase 2 negotiates a pair of one-way SAs: one for inbound and another for outbound communications [aranab]. This includes cryptographic keys that are used for encoding authentication information and performing payload encryption [5]. IKE phase 1 creates an IKE SA; IKE phase 2 creates an IPsec SA through a channel protected by the IKE SA. IKE phase 1 has two modes: main mode and aggressive mode. Main mode negotiates the establishment of the bidirectional IKE SA through three pairs of messages, while aggressive mode uses only three messages. Although aggressive mode is faster, it is also less flexible and secure. IKE phase 2 has one mode: quick mode. Quick mode uses three messages to establish a pair of unidirectional IPsec SAs. Quick mode communications are encrypted by the method specified in the IKE SA created by phase 1.

4. Quality of Service Issues

Due to resource constraint and dynamic topology of IPSec VPN, supporting QoS in VPN s is a challenging task. QoS is needed in VPN as different applications have different service requirements.

1. **Throughput**: The total bytes received by the destination node per second (Data packets and Overhead).
2. Network Address Translation (**NAT**): Connectivity can be adversely affected by Network Address Translation (NAT) or Proxy devices between the client and gateway as to require client configuration before the tunnel is established.

3. **Jitter** : It is refers to the variability of latencies for packets within a given data stream. it causes blocky video or jerky audio data.
4. **Packet Loss** : It refers to the loss or de-sequencing of data packets in a real-time data stream. It causes jerky video and broken audio.
5. **Good put** (In terms of Number of Packets)[6]: The ratio of the total number of data packets that are sent from the source to the total number of packets that is transmitted within the network to reach the destination.
6. **Good put** (In terms of Packet Size in Bytes): The ratio of the total bytes of data that are sent from the source to the total bytes that are transmitted within the network to reach the destination. Excludes protocol overhead bits as well as retransmitted data packets.
7. **Packet Delivery Ratio**: Packet Delivery Ratio in this simulation is defined as the ratio between the number of packets sent by constant bit sources (CBR) and number of packets received by CBR sinks at destination
8. **Data Dropped** : Data dropped due to unavailability of access to medium.

5. Overhead Issues

Overhead is one of the most challenging issue for IPSec base VPN network. It causes different level of QoS parameter badly affected. Overhead not only in between to end points, hosts or between VPN Gateways but also affect intermediate node like routers hub and ISP network for processing packet travel though network.

1. Number of Transactions
2. Network Load
3. Round Trip Time(RTT): It refers to computed as time interval between a data packet and an acknowledgment packet. As RTT value varies depending upon the network load dynamics, we have taken median RTT of a file transmission.[11]

6. Performance and simulation of IPSec VPN

Network simulation

Most IPsec simulative studies are based on simulation tools. The main advantage of these tools is that they provide libraries containing predefined models for most communication protocols (e.g., ns2, 802.11, Ethernet, TCP, etc.). In addition, these tools often provide graphical interfaces that can be used both during the model development phase, and during simulation runs to simplify following dynamic protocol and network behaviors. Popular network simulators used in ad hoc networks include: NS-2[8]. Wireshark OpenSwan FreeSwan software. The observed differences are not only quantitative, but also qualitative (not the same general behavior) making some past observation of IPSec base simulation studies an open issue.

While applying IPsec In VPN base network certain parameter need to consider for performance enhancement without compromise security level. Miss Ritu Malik[12] has analyze the performance of IPSec VPN with different protocol. They simulate with only AH (authentication header) then providing ESP(Encapsulating Security Payload) and both AH+ESP (authentication plus Confidentiality).

Table 1[12]

video	Average packet loss	Average packet jitter
Without IPSEC	0.9	35.44
With IPSEC AH	1.8	39.26
With IPSEC ESP	2.5	50.04
WithIPSEC AH+ESP	3.1	56.50

From table information shows different ipsec alternative used to enable VPN network secure. Different algorithm for authentication(MD5, SHA-1, SHA-256, SHA-512 and hash-based message authentication code HMAC) ,encryption (AES, RC6, RC5, TwoFish, CAST, Camellia, IDEA, DES, and DES/EDE3)and confidentiality. For bulky data transfer application like video conference ,voiP, audio video transmission between remotely located VPN ect are also require more secure transmission over public network . which is achieve by implementing IPSec at network layer without affecting upper layer protocol.

Above result found by Miss Ritu Malik as shown significant affecting QoS parameter.

Major drawback of IPSec VPN is it provide entire subnet within corporate network. if client PC becomes infected with attack it could potentially spread to the entire network.

Access control can also be an issue with IPSec VPNs since they rely on network access controls [4].configuration issue for VPN gateways and client configuration before tunneling is establish.

III. CONCLUSION

VPN is a comprehensive new network technology. IPSEC enable VPN network a standard security for corporate network. IPSec is currently the most secure VPN solution available in the market. Yes IPSEC is conflict with NAT protocol. There are some issues, the use of IPSec a cost: additional processing and increased packet size, jitter packet loss etc. the challenges of VPN is nicely solved by IPSec enable VPN by compromise certain level of overhead , performance (QoS)parameter. in order to enable both QoS and security with IPSec, a future area will consider adding some QoS parameters into the IPSec SAs.

ACKNOWLEDGMENT

I thank Prof Kalpesh Palel (LD collage of Engineerin Ahmedabad) and my guide Prof Arvind Meniya(SSEC Bhavnagar) for their valuable suggestion and reviewing this paper.

REFERENCES

1. Mr. Hitesh dhall, Ms. Dolly Dhall, Ms. Sonia Batra, Ms. Pooja Rani IMPLEMENTATION OF IPSEC PROTOCOL 2012 Second International Conference on Advanced Computing & Communication

Technologies*978-0-7695-4640-7/12*

2. RFC 2401, Security Architecture for the Internet Protocol, provides an overview of IPsec. The RFC is available for download at *http://www.ietf.org/rfc/rfc2401.txt*.
3. AH is IP protocol number 51. The AH version 2 standard is defined in RFC 2402, IP Authentication Header, available at *http://www.ietf.org/rfc/rfc2402.txt*.
4. Olalekan Adeyinka Analysis of problems associated with IPSec VPN Technology 2008 *978-1-4244-1643-1/08*
5. ESP is IP protocol number 50. The ESP version 2 standard is defined in RFC 2406, IP Encapsulating Security Payload (ESP), available at *http://www.ietf.org/rfc/rfc2406.txt*.
6. D. Harkins and D. Carrel, “The Internet Key Exchange (IKE),” RFC 2409 (Proposed Standard), Internet Engineering Task Force, Nov. 1998.
7. Ankur Lal, Dr.Sipi Dubey,Mr.Bharat Pesswani "Reliability of MANET through the Performance Evaluation of AODV, DSDV, DSR "International Journal of Advanced Research in Computer Science and Software Engineering Vol. 2, No. 5,May 2012,pp. 213-216.
8. D. Harkins and D. Carrel, “The Internet Key Exchange (IKE),” RFC 2409 (Proposed Standard), Internet Engineering Task Force, Nov. 1998.
9. The Network Simulator-ns-2, http:// www. Isi. Edu / nsnam/ns/index.html.
10. Muhammad Awais Azam, Zaka-Ul-Mustafa, Usman Tahir, S. M. Ahsan, Muhammad Adnan Naseem, Imran Rashid, Muhammad Adeel” Overhead Analysis of Security Implementation Using IPSec “
11. S. P. Meenakshi S. V. Raghavan “Impact of IPSec Overhead on Web Application Servers”
12. Ritu Malik Rupali Syal “Performance Analysis of IP Security VPN “International Journal of Computer Applications *(0975 – 8887) Volume 8– No.4, October 2010*

Books:

William Stallings, *Cryptography and Network Security,* Principles and Practices, second edition, Pearson Education

“Guide to IPsec VPNs” ()by Sheila Frankel Karen Kent Ryan Lewkowski Angela D. Orebaugh Ronald W. Ritchey Steven R. Sharma

Recommendations of the National Institute of Standards and Technology NIST Special Publication 800-77

Theses:

[13]Arnab Kundu, *AN EXTENSION OF MULTI LAYER IPSECFOR SUPPORTING DYNAMIC QOS AND SECURITY REQUIREMENTS* Supercomputer Education and Research Centre Indian Institute of Science Bangalore February 2010.

AUTHORS PROFILE

Miteshkumar Shaileshbhai Parmar : PG Student at Department of Information Technology , S S Eng. College, Bhavnagar affiliated to GTU ahmedabad.

Prof. Arvind D Meniya : Curently working as Assistant Professor in Information Technology Department of S S Eng. College, Bhavnagar affiliated to GTU ahmedabad.