International Journal of Computer Sciences and Engineering Open Access
Technical Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Network Traffic Encryption by IPSec

Manoj Kumar[1*], Amit Kishor[2]

[1,2]Dept. of CSE, Subharti Institute of Technology & Engineering, Swami Vivekanand Subharti University, Meerut, U.P., India

[*]*Corresponding Author: mkd77in@gmail.com, Mobile: +919631862823*

DOI: https://doi.org/10.26438/ijcse/v7i5.912915 | Available online at: www.ijcseonline.org

Accepted: 16/May/2019, Published: 31/May/2019

Abstract- Several persons in a company use the local LAN for most of their communication & data transfer. The local LAN has several unsecured protocols & services i.e. FTP, Telnet etc. Persons who exchange highly confidential & sensitive information need a secure system on local LAN for secure communications. This paper describes the Internet Protocol Security (IPSec) & how IPSec framework can be used for secure & private communications over Internet Protocol, in local LAN environment. This paper also describes the various Protocols used in IPSec, Security Architecture of IPSec & various modes of operations in IPSec.

Keywords- Internet Protocol Security (IPSec), Internet Key Exchange (IKE), Virtual Private Network (VPN).

I. INTRODUCTION

Internet Protocol Security (IPSec) is a framework for secure & private communications over Internet Protocol. It uses cryptographic security services. It provides IP communication by authenticating and encrypting each IP packet. IPSec also includes protocols for establishing mutual authentication. IPSec supports Network- level authentication, data origin authentication, data integrity, data confidentiality and replay protection. IPSec is an end-to-end solution and operates at Network Layer of the OSI model [1-2].

The illustration as in Figure 1 shows a simple IPSec communication in a LAN environment.

The section I contains the introduction of Internet Protocol Security (IPSec), section II summarizes the related work explored in the area of IPSec, section III describes the implementation mechanism to setup secure communication system in LAN environment, section IV describes the various protocols used in IPSec, section V contains security architecture of IPSec, section VI describes the modes of operations in IPSec and section VII concludes the technical work.

II. RELATED WORK

The transmitted data needs to be protected in the network for various internet applications such as e-commerce, e-mail & on-line banking transactions etc. Most of the critical & sensitive internet applications rely on TCP/IP protocol suite for building enterprise network, which don't provide any in-built security mechanism to protect moving data.

IPSec is a Network layer security framework that can be used to build enterprise network. IPSec can provide secure

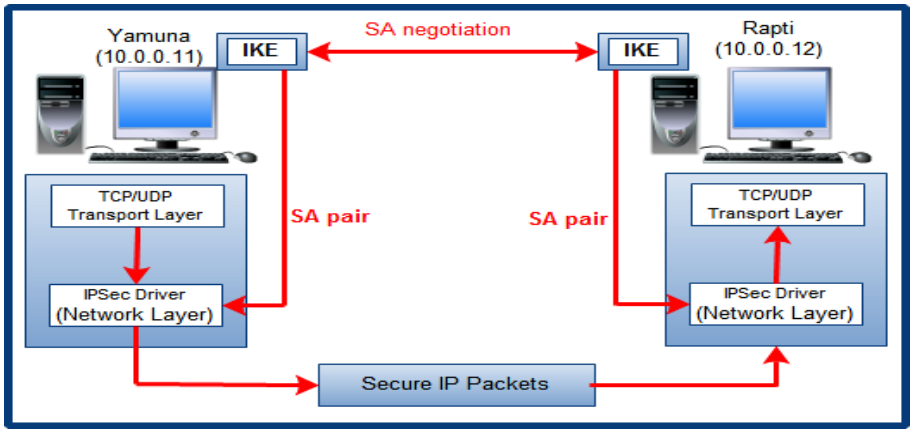

Figure 1. IPSec Communication in LAN Environment

communication over a LAN, WANs & internet.

Implementation of Virtual Private Network based on IPSec Protocol was presented by Jianwu Wu, which provides IPSec protocol implementation in Window 2003 and Cisco routers [5]. Implementation of IPSec Protocol was presented by Hitesh Dhall, which provide Host implementation and Router implementation of IPSec [6]. IPSec: Performance Analysis and Enhancements was presented by Craig A. Shue, which provides enhancing of performance of IPSec by optimizing IKE and analyzing its performance [7].

In this technical paper, we have proposed to implement a secure communication system using IPSec security framework in local LAN environment.

III. IMPLEMENTATION MECHANISM

To setup secure communication system in LAN environment, the following steps are being followed in this communication:

(i) The Source Machine (i.e. Yamuna) wants to send application IP packet to Destination Machine (i.e. Rapti).

(ii) The IPSec driver on Yamuna checks its outbound IP filter lists and determines that the packets should be secured.

(iii) The action is set to negotiate security in IPSec policy, so the IPSec driver notifies IKE to begin negotiations.

(iv) The IKE service on Yamuna completes a policy lookup, using its own IP address as the source and the IP address of Rapti as the destination. The main mode filter (of IKE) match determines the main mode settings that Yamuna proposes to Rapti. Yamuna sends first IKE message in main mode, using UDP source port 500 and destination port 500. The IKE packets receive special processing by IPSec driver to bypass filters.

(v) Rapti receives an IKE main mode message requesting secure negotiation. It uses the source IP address and the destination IP address of the UDP packet to perform a main mode policy lookup, to determine which security settings to agree to. Rapti has a main mode file that matches, and so replies to begin negotiation of the main mode SA (Security Association).

(vi) Yamuna and Rapti now negotiate options, exchange identities, verify trust in those identities (authentication), and generate a shared master key. They have now established an IKE main mode SA. Now Yamuna & Rapti would mutually trust each other.

(vii) Now Yamuna performs an IKE quick mode policy lookup, using the full filter to which the IPSec driver matched the outbound packet. Yamuna selects the quick mode security settings and proposes them to Rapti.

Rapti also performs an IKE quick mode policy lookup, using the filter description offered by Yamuna. Rapti selects the security settings required by its policy and compares them to those offered by Yamuna. Rapti accepts and completes the remainder of the IKE quick mode negotiations to create a pair of IPSec security associations.

(viii) One IPSec SA is inbound and one IPSec SA is outbound.

(ix) The IPSec driver on Yamuna uses the outbound SA to sign and encrypt the packets.

(x) The IPSec driver passes the packets to the network adapter driver.

(xi) The network adapter driver at Rapti receives the encrypted packets from the network.

(xii) The IPSec driver on Rapti uses the inbound SA keys required to validate authentication & integrity and to decrypt the packets.

(xiii) The IPSec driver converts the packets from IPSec format back to standard IP packet format. It passes the validated and decrypted IP packets to the TCP/IP driver, which passes them to the receiving application on Rapti.

IV. PROTOCOLS USED IN IPSEC

IPSec uses the following protocols to perform the various functions [8-9].

A. Internet Key Exchange (IKE)

IKE is a key exchange protocol. IKE is used to securely exchange encryption keys as part of building a tunnel. Two computers must establish a security agreement on how to exchange and protect information. IKE is used to build this security association (SA). IKE has many responsibilities i.e. it centralizes association management, reduces connection times, generates and manages shared secret keys that are used to secure information.

IKE negotiates two types of security associations. These security associations are:

(i) A main mode security association (IKE security association that is used to protect the IKE negotiation itself).

(ii) IPSec security associations (security associations that are used to protect application traffic).

B. Authentication Header (AH)

This protocol provided data origin authentication, data integrity and replay protection. It does not provide data confidentiality, means that all of the data is sent in the clear text. AH uses checksum as a message authentication code, like MD5 generates. For data origin authentication, AH includes a secret shared key that it uses for authentication. AH uses a sequence number field within the AH header for replay protection.

C. *Encapsulating Security Payload (ESP)*

ESP protocol provides data confidentiality, and also optionally provides data origin authentication, data integrity checking & replay protection. The difference between Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols is that ESP provides encryption, while both protocols provides authentication, integrity checking & replay protection. With ESP, both communicating systems use a shared key for encrypting and decrypting the data they exchange.

V. SECURITY ARCHITECTURE OF IPSEC

The various components of IPSec Security Architecture are:

A. *Encapsulating Security Payload (ESP)*

This group contains packet format and general issues related to the use of ESP for packet encryption and optionally, authentication.

B. *Authentication Header (AH)*

This group contains the packet format and general issues related to use of AH for packet authentication.

C. *Encryption Algorithm*

This group contains documents that describe various encryption algorithms used for ESP.

D. *Authentication Algorithm*

This group describes various authentication algorithms used for AH and for authentication option of ESP.

E. *Key Management*

This document describes key management schemes.

F. *Domain of Interpretation (DOI)*

This group contains values needed for other documents to relate to each other. These include identifiers for approved encryption and authentication algorithms, as well as operational parameters such as key lifetime.

The security architecture of IPSec is shown in figure 2.

VI. MODES OF OPERATIONS

There are two modes of operations in IPSec [10].

A. *Transport Mode*

In transport mode, AH and ESP protect the transport header. It protects the message passed down to IP from the transport layer. The message is processed by AH/ESP and configured security is applied. In transport mode, only the payload of the IP packet is encrypted and authenticated. The transport mode of IPSec is used only when security is desired end to end.

B. *Tunnel Mode*

In tunnel mode, the entire IP packet (data and IP header) is encrypted and/or authenticated. It is then

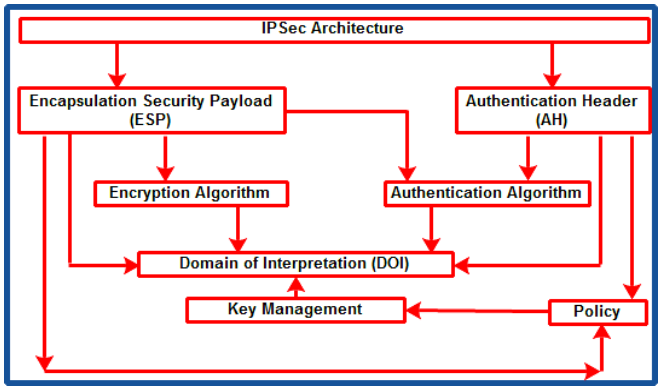

Figure 2. Security Architecture of IPSec

encapsulated into a new IP packet with a new IP header. The tunnel mode is used in cases when security is provided by a device that did not originate packets. Tunnel mode is used to create Virtual Private Networks (VPN) for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access), and host-to-host communications (e.g. private chat).

VII. CONCLUSION

Local LAN has many unsecured protocols & services. To setup secure communication system in local LAN environment, Internet Protocol Security (IPSec) framework can be used for providing secure & private communications over internet protocol.

In local LAN environment, we can encrypt network traffic by using IPSec. The IPSec uses cryptographic security services and provides IP communication by authenticating and encrypting each IP packet. The Internet Protocol Security (IPSec) uses, Internet Key Exchange (IKE) protocol for securely exchanging encryption keys as part of building a tunnel

Authentication Header (AH) protocol for data origin authentication, data integrity checking & replay protection, and Encapsulating Security Payload (ESP) protocol for data confidentiality and optionally for data

origin authentication, data integrity checking & replay protection.

IPSec operates in Transport mode and Tunnel mode. Transport mode can be used for end-to-end security. Tunnel mode can be used to create Virtual Private Network (VPN) for network-to-network communications, host-to-network communications & host-to-host communications.

On setting up a secure communication system in LAN environment, by applying IPSec policy for FTP server at Rapti and at Yamuna for FTP connection to FTP server at Rapti, by configuring IP filter list & associated filter actions. On monitoring the traffic from Yamuna to Rapti, by using Wireshark at Rapti, captured packets shows that all the packets are transmitted through ISAKMP & ESP protocols, which are used in IPSec.

REFERENCES

[1] W. Stalling, "*Cryptography and Network Security Principles & Practice"*, Pearson Publication, USA, pp. 615-650, 2011.

[2] B. A Forouzan, D. Mukhopadhyay, "*Cryptography and Network Security*", McGraw Hill Education Publication, India, pp. 487-520, 2015.

[3] A. T. Zamani, J. Ahmad, "*Adoption Ipv6: Security and Future*", International Journal of Scientific Research in Computer Sciences and Engineering, VOL.2, Issue.1, pp. 17-21, 2014.

[4] R. Ganguli, S. Roy, "*Designing a Graph Anonymization Framework for Secure Packet Transmission in the IP over Ethernet LAN"*, International Journal of Computer Sciences and Engineering, VOL.6, Issue.9, pp. 650-654, 2018.

[5] J. Wu, "*Implementation of Virtual Private Network based on IPSec Protocol*", IEEE 2009 ETP International Conference on Future Computer & Communication, Wuhan, China, pp. 138-141, 2009.

[6] H. Dhall, D. Dhall, S. Batra, P. Rani, "*Implementation of IPSec Protocol*", IEEE 2012 International Conference on Advanced Computing & Communication Technologies, Rohtak, India, pp. 176-181, 2012.

[7] C. A. Shue, M. Gupta, S. A. Myers, "*IPSec: Performance Analysis and Enhancements"*, IEEE 2007 International Conference on Communications, Glasgow, Scotland, pp. 1527-1532, 2007.

[8] R. Perlman, C. Kaufman, "*Analysis of the IPSec Key Exchange Standard*", IEEE Computer Society 10th IEEE International Workshop on enabling Technologies-Infrastructure for collaborative enterprises, Cambridge, MA, USA, pp. 150-156, 2001.

[9] K. Kedarnath, "*IPSEC: Internet Protocol Security*", International Journal of Scientific Research in Network Security and Communication, VOL.1, Issue.3, pp. 1-8, 2013.

[10] R. A. A. Al-faluji, "*Internet Protocol Security for Secure Communication: Fundamentals, Services and Application*", International Journal of Computer Engineering & Information Technology, VOL.9, Issue.9, pp. 186-191, 2017.

Authors Profile

Manoj Kumar pursued Bachelor of Engineering in Computer Science & Engineering, from M.M.M. Engineeing College, Gorakhpur University, Gorakhpur, India. He is currently M.Tech. Scholar and pursuing M.Tech. in Cyber Security, from department of Computer Science Engineering & I.T., Subharti Institute of Technology & Engineering, Swami Vivekanand Subharti University, Meerut, India. His area of work/experience focuses on Networking and Information Security.

Amit Kishor is working as Assistant Professor , in the department of Computer Science Engineering & I.T., Subharti Institute of Technology & Engineering, Swami Vivekanand Subharti University, Meerut, India. Currently he is pursuing Ph.D. in Computer Engineering from department of Computer Science & I.T., Sam Higginbottom University of Agriculture, Technology and Sciences, Allahabad.

