Internet Protocol Security (IPSec) Mechanisms

Hani Alshamrani

Abstract— The paper describes how to provide a set of security services for traffic at the IP layer, in both the IPv4 and IPv6 environments. IP-Sec is a set of protocols operating at the OSI architecture model Network Layer three by extending the IP packet header to support secure exchange of packets. This provides the ability to encrypt any higher level messaging. IPSec includes two protocols, AH and ESP, which provide security for IP packets. The AH provides authentication, integrity and replay protection. The ESP provides authentication, integrity, replay protection and confidentiality. Authentication and integrity can be used with or without confidentiality and vice-versa. These protocols need certain parameters in order to establish each connection. The parameters are collected in an entity called security association or SA. When two nodes have established matching SAs, sent and received packets can take advantage of the security services.

Index Terms— AH, Domain of Implementation, ESP, IKE, Internet Protocol, Key Management, OSI architecture.

1 Introduction

The paper specifies the base architecture for Internet Protocol Security (IPSec) as shown in Figure 1, compliant systems [1]. It describes how to provide a set of security services for traffic at the IP layer, in both the IPv4 [9] and IPv6 [8] environments. IPSec is a set of protocols operating at the OSI architecture model Network Layer by extending the IP packet header to support secure exchange of packets. This provides the ability to encrypt any higher level messaging. Figure 1 defines how the various components of IPSec interact.

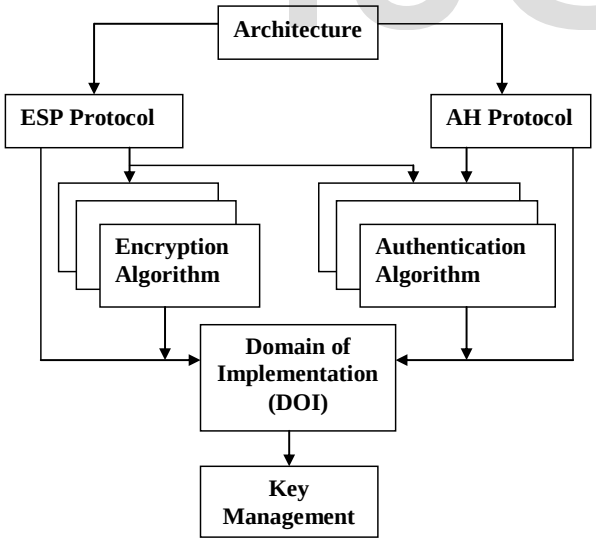


Figure 1 - IPSec roadmap

IPSec supports two security services: Authentication Header (AH) and Encapsulating Security Payload (ESP). The former provides authentication of the sender and the latter provides both authentication of the sender and encryption of the data.

IPSec supports two encryption modes: Transport and Tunnel. The Transport mode encrypts just the upper layer headers and data payload of each packet. The more secure Tunnel mode encrypts the IP header, upper layer headers, and data payload.

In order for IPSec to function properly, the sender and receiver must share a public key. This is done through a protocol known as Internet Key Exchange version 2 (IKEv2) [7]. The protocol allows the receiver to get a public key and authenticate the sender.

A fundamental construct in IPSec is the Security Association (SA), which establishes a basic connection with security services. An SA is specified at a minimum with a 32-bit Security Parameter Index (SPI).

IPSec has been deployed widely to implement Virtual Private Networks (VPNs). As such, segmented links may be securely networked with IP using encrypted tunnels. Since the routers perform the encryption/decryption, the secure applications need no local cryptographic support.

2 Authentication Header (AH)

The AH service is used to provide data integrity, data source authentication, and replay protection capability. The entire packet is authenticated. The authentication header format is shown in Figure 2 below:

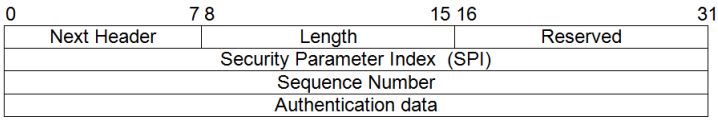


Figure 2 - Authentication Header

The Next Header is an 8-bit field that specifies the type of data contained in the payload. The Length field specifies header size in 32-bit words, minus two, and the reserved field is set to zero. The Security Parameter Index is a 32-bit number that provides the SA related to this packet. The Sequence Number keeps track of the number of packets incrementing by one for each packet. The Authentication Data is a variable length field

International Journal of Scientific & Engineering Research Volume 5, Issue [illegible]
ISSN 2229-5518

that contains the Integrity Check Value (ICV). The field size must be a multiple of 32-bits and may contain padding as needed. The sender authentication header works by calculating the ICV based on the payload, portion of the IP header, a secret authentication key, and a hash function. The receiver performs the same calculation, and if the two values match, integrity is verified. In addition, the source address provides authentication, and the sequence number replay protection.

3 Encapsulating Security Payload (ESP)

The ESP service is used to provide data confidentiality, data integrity, data source authentication and anti-play capability. The data and inner headers are encrypted and the entire packet is authenticated, with the exception of the external IP header. The ESP header is shown in Figure 3 below:

The Security Parameter Index is a 32-bit number that associates the inbound SA with this packet. The sequence number is incremented by one for each packet in the SA. The Initialization Vector is provided if needed by the encryption algorithm. The Padding field can vary in length from 0 to 255 bytes. The Authentication data contains the integrity check vector for the header and payload. Encryption is applied first then authentication takes place. The ESP does basically what the AH does except that it does not authenticate the outer IP header. In addition, it encrypts the payload using a secret key. Hence, only those who know the key can read the data, thus providing confidentiality.

4 IPSec Modes

There are three basic IPSec modes the transport, the tunnel, and the nested. The transport mode is used to protect the payload of the packet only. The authentication or encryption and connection endpoints are the same. The tunnel mode is used to protect the entire packet, which includes the header. The authentication or encryption and connection endpoints may or may not be the same. The nested mode is a combination of two or more tunnel modes. Normally a host can use transport or tunnel mode and a router can use only tunnel mode.

0	31
Security Parameter Index (SPI)	
Sequence Number	
Initialization Vector	
Protected Data	
Padding	
Padding Length	Next header
Authentication Data	

Figure 3 - Encapsulating Security Payload

4.1 Transport Mode

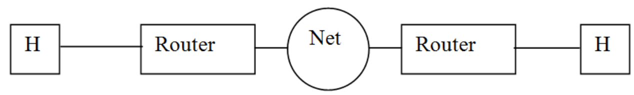
In the transport mode of operation, the TCP and Application layer data are authenticated or encrypted between two hosts. Hence the connection and security endpoints are identical.
Figure 4 illustrates the transport mode format using the ESP header.

IP Header	ESP Header	TCP (Encrypted)	Data (Encrypted)

Figure 4 - Transport Mode Format

4.2 Tunnel Mode

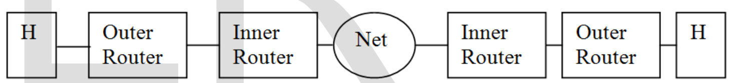
In the tunnel mode of operation, the IP, TCP, and Application layer data are encapsulated and authenticated or encrypted between two routers. A host is connected to each router that sends or receives the authenticated or decrypted packet. The security and connection endpoints are different. Figure 5 below illustrates the tunnel mode format using the ESP header.



Router IP Header	ESP Header	IP Header (Encrypted)	TCP (Encrypted)	Data (Encrypted)

Figure 5 - Tunnel Mode Format

Figure 6 illustrates a tunnel mode established between two hosts connected to two outer routers in a nested configuration for confidentiality. A second tunnel mode is established between the two inner routers for integrity. As such the security and connection endpoints are different.



In Router IP Header	AH	Out Router IP Header	ESP	IP Header (Encrypted)	TCP (Encrypted)	Data (Encrypted)

Figure 6 - Nested Configuration

5 Internet Key Exchange (IKE)

The IKE Protocol makes it possible for two nodes to negotiate a secure connection by creating a SA. The SA set of parameters is only for one direction of data flow and for only one protocol. During the negotiation, the IPSec protocols are agreed upon, the hash function, authentication key, encryption algorithm, and encryption key data are exchanged, and the duration of security association is set.

The IKE protocol consists of two phases. During phase one, a security association is established in order to protect the messages during the phase two exchanges. During phase two, an IPSec SA is established.

6 Conclusion

IPSec includes two protocols, AH and ESP, which provide security for IP packets. The AH provides authentication, integrity and replay protection. The ESP provides authentication,

International Journal of Scientific & Engineering Research Volume 5, Issue 5, May-2014
ISSN 2229-5518

integrity, replay protection and confidentiality. Authentication and integrity can be used with or without confidentiality and vice-versa. These protocols need certain parameters in order to establish each connection. The parameters are collected in an entity called security association or SA. When two nodes have established matching SAs, sent and received packets can take advantage of the security services.

In the transport mode, the initial IP header is used to deliver the packets to the endpoints. In the tunnel mode, the IP header provides the address of the router, while the endpoint addresses are encrypted along with the payload. The transport mode of operation, IPSec supports AH alone or ESP alone. Similarly, the tunnel mode IPSec supports AH alone or ESP alone. Typical applications are end-to-end security, VPN support, nested tunnels, and remote access.

REFERENCES

[1] RFC 4301 - Security Architecture for the Internet Protocol

[2] RFC 4302 - IP Authentication Header (AH); RFC 4305, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)

[3] RFC 2403 - The Use of HMAC-MD5-96 within ESP and AH

[4] RFC 2404 - The Use of HMAC-SHA-1-96 within ESP and AH

[5] RFC 2405 - The ESP DES-CBC Cipher Algorithm with Explicit IV

[6] RFC 4303 - IP Encapsulating Security Payload (ESP); RFC 4305, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)

[7] RFC 4306 - Internet Key Exchange (IKEv2) Protocol

[8] RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification

[9] RFC 791 - Internet Protocol version 4 (IPv4); RFC 2474, Definition of the Differentiated Services Field (DS Field); RFC 3168. The Addition of Explicit Congestion Notification (ECN) to IP; RFC 3260, New Terminology and Clarifications for Diffserv

[10] RFC 793 - Transmission Control Protocol (TCP); RFC 3168. The Addition of Explicit Congestion Notification (ECN) to IP