IP Security

Session 8

LEARNING OBJECTIVES

On completion of this session you should:

- Be familiar with Internet Protocol Security (IPSec) capabilities
- Understand IPSec architecture
- Understand Authentication Header and Encapsulating Security Payload protocols
- Be familiar with transport and tunnel modes of operation
- Appreciate the concept of security association
- Understand key management in IPSec

Contents

Reading

Prescribed readings

Reading 1: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 284-288.

Reading 2: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 295-302.

Reading 3: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 306-310.

Reading 4: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp.299-302.

Reading 5: Skim through the following for introduction to VPN
http://www.caconsultant.com/Article/VPN/introduction_to_vpn.htm
http://compnetworking.about.com/od/vpn/a/vpn_tutorial.htm.

Reading 6: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 290-295 and 302-306.

8.0 Introduction

Even though some application-specific security mechanisms (e.g., PGP, SSL etc.) have been developed, in general, TCP/IP protocol suite used for transmitting data over the Internet does not employ any security feature. Application-specific techniques are not general enough and security

services must be added to the Internet Protocol (IP) itself. IP Security (IPSec) is an effort by the IETF to define a set of protocols to provide high quality, interoperable, and cryptology-based security for IP packets. Rather than requiring each e-mail program or web browser to implement its own security mechanisms, IPsec involves a change to the underlying networking facilities that are used by each application. It also allows network managers to apply protection to network traffic without involving the end users.

8.1 Security Services by IPSec

IPSec provides the following security services at the IP layer by making use of the security protocols, cryptographic and authentication algorithms, and key exchange mechanisms [1]:

- Access control
- Connectionless integrity – guarantees that the message received is exactly the same as the message sent. It is connectionless due to IP protocol where no attempt is made to ensure that the packets are received.
- Data origin authentication - guarantees that the message was sent by the originator of the message as it appears to be.
- Replay protection - the same message is not delivered multiple times.
- Confidentiality – only the intended recipient can read the message.
- Traffic analysis protection - an eavesdropper cannot determine the communicating parties or the frequency and the volume of communications.

Reading 1:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 284-288.

8.2 IPSec Protocols

IPsec consists of the following three major protocols:

- **Authentication Header** - provides data origin authentication, data integrity, and replay protection of IP packets.
- **Encapsulating Security Payload**- in addition to providing the same services as Authentication Header, it also offers confidentiality.
- **Internet Key Exchange** - provides key-management function.

8.2.1 Authentication Header (AH)

An attacker can manipulate an IP packet which is normally unprotected. The header in IP packet is covered by the 'Header Checksum' field (see page 215 of the textbook for IPv4 header), but this is meant to protect the header from corruption. An attacker can modify the header fields and recalculate the checksum easily to avoid detection. The same is true for the data part. The TCP segment or UDP datagram can be modified and the checksum recalculated. AH provides connectionless integrity and data origin authentication protection. This protection covers the packet's data portions and those IP header fields that cannot change in an unpredictable manner (ie., partial IP header) as the packet traverses through the Internet. The IP header fields that may change include 'Time to Live', 'Fragmentation Offset' etc. Authentication covers those header fields that do not change during transmission.

AH provides its services by calculating a keyed MAC, called an integrity check value (ICV), over the IP header except the mutable fields and the entire payload data. The results of the ICV are placed in the AH header, and the header is added to the packet. The exact placement of the AH header in the datagram depends on whether it is being used in transport or tunnel mode (IPSec modes are discussed later). The concept of authentication in AH is shown below.

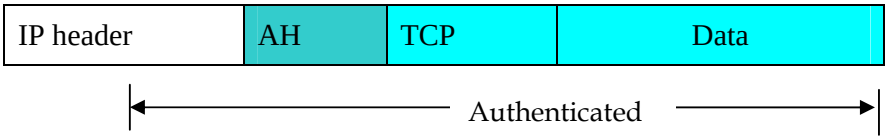


Fig. 1 AH authentication

The authentication header has the following fields:

- Next header (8 bit) – identifies the type of the immediate next header. For example, if AH is protecting a TCP segment, the next header field would contain the protocol number assigned to TCP.
- Payload length (8 bit) - length of AH itself (not the length of the data it is protecting) in 32-bit words less 2.
- Reserved (16 bits) – reserved for future use.
- Security Parameter Index (SPI - 32 bits) - identifies a security association (discussed later) which applies to the IP packet.
- Sequence number (32 bits) - a counter that monotonically increases by 1 for each AH packet with a particular security association (SA). The initial value of the counter is 1. When the maximum sequence number is reached, a new SA is negotiated. This provides anti-replay function.
- Authentication data (variable, integer multiple of 32-bit) - contains the result of the ICV (HMAC) calculation. The current specification uses MD5 and SHA-1 HMAC algorithms.

As mentioned below, placement of the AH header varies with IPSec modes and IP versions. In tunnel mode, the original IP header is encapsulated with a new IP header. Also in IPv6, extension headers like 'hop-by-hop', 'routing' and 'fragment' headers are present, which are covered by authentication header.

8.2.2 Encapsulating Security Payload (ESP)

In addition to the services provided by AH, ESP provides confidentiality. The authentication function in ESP is almost identical to that provided by AH. The difference is that ESP authentication does not protect the IP header fields, more specifically, the outer IP header fields. As mentioned earlier, tunnel mode adds an additional IP header. In this mode, ESP protects the inner IP header but not the outer while AH protects all the inner IP header and part of the outer IP header. To provide confidentiality, ESP uses encryption. The concept of ESP is shown below.

IP header	ESP header	TCP	Data	ESP trailer	ESP Auth

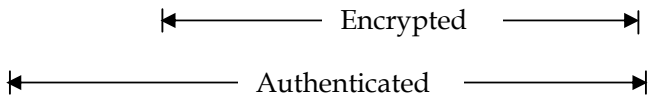


Fig. 2 ESP encryption and authentication

Here the entire block consisting of transport layer data plus the ESP trailer is encrypted and the plaintext block is replaced with the ciphertext which ensures confidentiality. In the same process as AH, authentication covers all of the ciphertext plus ESP header. The ESP trailer consists of 'Padding', 'Pad Length' and 'Next Header' fields. Padding field is added to expand the plaintext because some encryption algorithms require multiple of some number of bytes to work.

Encapsulating Security Payload packets have the following fields:

- Security parameter index (32 bits) – same as AH.
- Sequence number (32 bits) - same as AH.
- Payload data (variable) – Block cipher in CBC mode requires an initialization vector for encryption/decryption operation. Initialization Vector (IV) and ciphertext are included in this field. In reliable networks, we could send the IV in the first packet and let the receiver cache the most recent encrypted block for use with the next block's CBC operation. However, IP does not guarantee delivery of packets or their arrival in order, requiring IPsec to send IV with each packet.
- Padding (0~255 bytes) – Plaintext is padded as required for the encryption algorithm to work. It is also possible to add a random number of padding bytes to hide the length of the payload data.
- Pad length (8 bits) – indicates the number of pad bytes.
- Next Header (8 bits) – identifies the type of data contained in payload and right aligned on a 32-bit boundary.
- Authentication data (variable, integer multiple of 32-bit) - contains ICV calculated over the entire ESP packet except the authentication data field and must start on a 32-bit boundary.

The current specification supports a number of encryption algorithm, e.g., DES, triple DES, RC5, IDEA, triple IDEA, CAST, and blowfish.

Reading 2:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 295-302.

8.2.3 Internet Key Exchange (IKE)

Before two communicating parties can exchange secure communications, they need to agree on the nature of the security to be enforced. For example, they need to agree on which security headers (AH, ESP, or both) will be applied; the cryptographic algorithms to be used; the secret keys; the types of communications to be protected; the lifetime of the agreement; etc. A Security Association (SA, details in Sections 8.2 and 8.4) consists of all the information that is needed to characterize and exchange protected communications. IKE (Internet Key Exchange) is a protocol developed specifically for IPsec to enable peer-negotiation to dynamically agree on the IPsec protections that will be applied to future communications. IKE consists of: i) Oakley key determination protocols and ii) a framework called ISAKMP (Internet Security Association and Key Management Protocol). ISAKMP does not dictate any specific key exchange algorithm, Oakley is the key exchange algorithm used in the initial version of ISAKMP.

There are two phases involved in the key exchange process:

- During the first phase, a set of security related attributes is negotiated, the identities of the peers are authenticated and some keys are generated. These elements constitute a first security association, known as the ISAKMP SA. Contrary to IPsec SAs, an ISAKMP SA is bi-directional. It will be used to secure all the ISAKMP related exchanges.

- The second phase is used to negotiate the security parameters related to a SA to establish a given security mechanism (for example AH or ESP). The exchanges from this phase are protected. The ISAKMP SA can be used to negotiate several phase-2 SAs.

In IKE, the AH and ESP SAs are negotiated in the second phase. The secure channel established in phase-1 can be used to negotiate several phase-2 SAs. Recall from the previous session that Diffie-Hellman key exchange algorithm can be used to exchange a secret key between two parties. Oakley key determination protocol uses a refinement of Diffie-Hellman.

Reading 3:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 306-310.

8.3 IPSec Modes

Both AH and ESP can operate on either of the two modes – transport and tunnel. They differ mainly in two points: i) how they encapsulate data, and hence, what they protect, ii) whether they are securing communication between two hosts, or between two networks, or a network and a host. Transport mode IPsec is limited to host-to-host communications, in which each host provides its own IPsec capabilities. In this mode, the AH or ESP header is placed after the IP header as shown in the figure below.

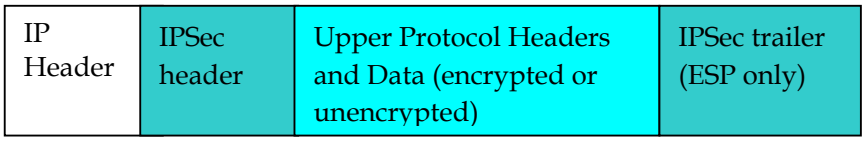
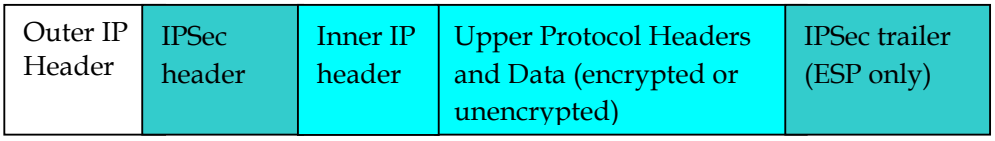


Fig. 3 Security protocol in transport mode

With tunnel mode, a security gateway, such as a firewall or router implementing IPSec, can provide protection for two networks, or a host and a network. For example, remote corporate and home networks can be connected through the tunnel-mode VPN by means of security gateways, which handle all security functions. These functions are completely transparent to the hosts on the two networks. In the case of the remote host, the gateway function is built into the remote host itself. Tunnel mode treats the entire IP packet (after addition of AH or ESP fields to the original IP packet) as payload and encapsulates it with a new outer packet. So, in a sense it is IP-in-IP. If tunnel mode ESP is used, traffic analysis protection can also be provided. Tunnel mode requires higher bandwidth than transport mode because of the extra information added to the packet. Tunnel mode packet structure is shown in the following figure.



Original IP Packet

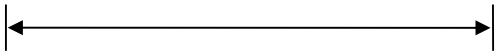


Fig. 4 Security protocol in tunnel mode

Reading 4:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 299-302.

Reading 5:
Skim through the following for introduction to VPN
http://www.caconsultant.com/Article/VPN/introduction_to_vpn.htm
http://compnetworking.about.com/od/vpn/a/vpn_tutorial.htm

6.4 Security Association

A Security Association (SA) is a set of security information relating to a given network connection or a set of connections to establish a one-way relationship between the sender and receiver. An SA is unidirectional. Therefore, at least two SAs are needed to protect data flows in a bidirectional communication. Moreover, if both AH and ESP are used to protect data flows between peers, each peer will construct an independent SA for each protocol. An SA is uniquely identified by a triplet, which consists of the followings:

- Security Parameter Index (SPI) – a bit string generated to uniquely identify an SA and is transmitted in the AH/ESP header.
- Destination IP Address – may be an end user or a network system such as a firewall or router.
- Security Protocol Identifier – indicates whether the association is in AH or ESP.

An SA normally includes the following parameters:

- Authentication algorithm, keys and their lifetimes being used with AH.
- Encryption algorithm, keys, and their lifetimes being used with the IP ESP.

- Presence/absence and size of an initialization vector field for the encryption algorithm.

Each SA has a lifetime which can be time based or traffic based. It becomes invalid on expiration of its lifetime. Before an SA becomes invalid, IKE will negotiate to set up a new SA and subsequently the connection uses the new SA.

Reading 6:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 290-295 and 302-306.

8.5 Conclusion

Application-specific security techniques are not general enough, therefore, security services must be added to the Internet Protocol (IP) itself which has no in-built security feature. IPSec is one way to ensure secure communication on TCP/IP protocol suite. IPSec enables to achieve a number of security features including data integrity, authentication and confidentiality over IP packets.

8.6 References

[1] W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011.