**Chapter 9**

• RFC 1636 • “Security in the Internet Architecture” • Issued in 1994 by the Internet Architecture Board (IAB) • Identifies key areas for security mechanisms

=> Need to secure the network infrastructure from unauthorized monitoring and control of network traffic

=> Need to secure end-user-to-end-user traffic using authentication and encryption mechanisms

• IAB included authentication and encryption as necessary security features in the next generation IP (IPv6) • The IPsec specification now exists as a set of Internet standards

Text

Description automatically generated

Diagram

Description automatically generated

**Some of the benefits of IPsec:**

1. When IPsec is implemented in a firewall or a router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing

2. IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization

3. IPsec is below the transport layer (TCP, UDP) and so is transparent to applications. Hence, there is no need to change software on a user or server system when IPsec is implemented in the firewall or router

4. IPsec can be transparent to end users, hence, there is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization

5. IPsec can provide security for individual users if needed, this is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications

Text, timeline

Description automatically generated with medium confidence

Diagram

Description automatically generated

**Transport Mode:**

• Provides protection primarily for upper-layer protocols

• Examples include a TCP or UDP segment or an ICMP packet

• Typically used for end-to-end communication between two hosts

• ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header

• AH in transport mode authenticates the IP payload and selected portions of the IP header

**Tunnel Mode:**

• Provides protection to the entire IP packet

• Used when one or both ends of a security association (SA) are a security gateway

• Several hosts on networks behind firewalls may engage in secure communications without implementing IPsec

• ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header

• AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header

Table

Description automatically generated

**IPSec Architecture**

Diagram

Description automatically generated

**Security Association (SA)**

• A one-way logical connection between a sender and a receiver that affords security services to the traffic carried on it • In any IP packet, the SA is uniquely identified by the Destination Address in the IPv4 or IPv6 header and the SPI in the enclosed extension header (AH or ESP)

Three parameters uniquely identify SA

1. Security Parameters Index (SPI) • A 32-bit unsigned integer assigned to this SA and having local significance only
2. Security protocol identifier • Indicates whether the association is an AH or ESP security association
3. IP Destination Address • Address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router

**Security Association Database (SAD)**

=> Defines the parameters associated with each SA

=> Normally defined by the following parameters in a SAD entry: • Security parameter index • Sequence number counter • Sequence counter overflow • Anti-replay window • AH information • ESP information • Lifetime of this security association • IPsec protocol mode (i.e., Tunnel, transport, or wildcard). • Path MTU

**Security Policy Database (SPD)**

• The means by which IP traffic is related to specific SAs

• Contains entries, each of which defines a subset of IP traffic and points to an SA for that traffic

• In more complex environments, there may be multiple entries that potentially relate to a single SA or multiple SAs associated with a single SPD entry

• Each SPD entry is defined by a set of IP and upper-layer protocol field values called selectors

• These are used to filter outgoing traffic to map it into a particular SA

**SPD Entries**

Diagram, text

Description automatically generated

**Host SPD Example**

Table

Description automatically generated

**Processing Model for Outbound Packets**

Diagram

Description automatically generated

**Processing Model for Inbound Packets**

Diagram

Description automatically generated

**Anti-replay mechanism**

Diagram

Description automatically generated

Diagram

Description automatically generated

Graphical user interface, application

Description automatically generated

Diagram

Description automatically generated

**ESP with Authentication Option**

• In this approach, the first user applies ESP to the data to be protected and then appends the authentication data field

**Transport mode ESP:** Authentication and encryption apply to the IP payload delivered to the host, but the IP header is not protected

**Tunnel mode ESP:** • Authentication applies to the entire IP packet delivered to the outer IP destination address and authentication is performed at that destination • The entire inner IP packet is protected by the privacy mechanism for delivery to the inner IP destination

• For both cases authentication applies to the ciphertext rather than the plaintext

**Transport Adjacency**

• Another way to apply authentication after encryption is to use two bundled transport SAs, with the inner being an ESP SA and the outer being an AH SA

• In this case ESP is used without its authentication option

• Encryption is applied to the IP payload

• AH is then applied in transport mode

• Advantage of this approach is that the authentication covers more fields

• Disadvantage is the overhead of two SAs versus one SA

**Transport-Tunnel Bundle**

• The use of authentication prior to encryption might be preferable for several reasons:

• It is impossible for anyone to intercept the message and alter the authentication data without detection

• It may be desirable to store the authentication information with the message at the destination for later reference

• One approach is to use a bundle consisting of an inner AH transport SA and an outer ESP tunnel SA

• Authentication is applied to the IP payload plus the IP header

• The resulting IP packet is then processed in tunnel mode by ESP

• The result is that the entire authenticated inner packet is encrypted, and a new outer IP header is added

Diagram

Description automatically generated

**Internet Key Exchange**

• The key management portion of IPsec involves the determination and distribution of secret keys

• A typical requirement is four keys for communication between two applications

• Transmit and receive pairs for both integrity and confidentiality

The IPsec Architecture document mandates support for two types of key management:

• **Manual:** A system administrator manually configures each system with its own keys and with the keys of other communicating systems

• This is practical for small, relatively static environments

• **Automated-** Enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration

**ISAKMP/OAKLEY**

• The default automated key management protocol of IPsec

• Consists of:

• Oakley Key Determination Protocol

• A key exchange protocol based on the Diffie-Hellman algorithm but providing added security

• Generic in that it does not dictate specific formats

• Internet Security Association and Key Management Protocol (ISAKMP)

• Provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes

• Consists of a set of message types that enable the use of a variety of key exchange algorithms

**Features of IKE Key Determination**

A picture containing table

Description automatically generated

Table

Description automatically generated

Table

Description automatically generated