

IP Security: A Brief Survey

Zhijun Ni, zhijunni@math.ohio-state.edu

IP Security mechanisms, such as Authentication Header (AH) and Encapsulating Security Payload (ESP) Header, are important for Internet security to ensure integrity, authentication and confidentiality for data transmission.

[Other Reports on Recent Advances in Networking](#)

[Back to Raj Jain's Home Page](#)

Table of Contents

- [Introduction](#)
 - [What is IP security?](#)
 - [How can IP Security be achieved?](#)
 - [What is a Security Association \(SA\) ?](#)
 - [IP Security Mechanisms](#)
 - [Authentication Header \(AH\)](#)
 - [AH Header Format](#)
 - [Using AH Header](#)
 - [Encapsulating Security Payload \(ESP\) Header](#)
 - [ESP Header Format](#)
 - [Using ESP Header](#)
 - [Key Management](#)
 - [Key Distribution](#)
 - [Keying Approaches for IP](#)
 - [Usage](#)
 - [Use with Firewalls](#)
 - [Use with IP Multicast](#)
 - [Use to provide QoS Protection](#)
 - [Use in Multi-level Networks](#)
 - [Reference](#)
-

Introduction

What is IP security? [[1Atk-RFC1825](#)]

IP security refers to security mechanisms implemented at the IP (Internet Protocol) Layer to ensure integrity, authentication and confidentiality of data during transmission in the open Internet environment.. The primary objective of recent work in this area, mainly by members in the IETF IP Security (IPsec) working group is to improve the

robustness of the *cryptographic* key-based security mechanisms at IP layer for users who request security.

Basic Concepts:

- *Authentication*

With certain security mechanism, two communicating parties know that the data at destination is the same as when it's initially sent (data integrity) and that the sender is not impersonated by third party.(data origin authentication).

- *Integrity*

Considered to be data integrity part of authentication (see above definition). Data is not allowed to be unmatched at source and at destination for two parties with certain security mechanism between them established.

- *Confidentiality*

With certain security mechanism (so-called encryption/decryption), data is protected during transmission from third party 's knowing the content.

- *Security Association (SA)*

An agreement between two communication parties on knowing and using certain combination of security mechanisms for data transmission between them. It's based on destination address and a certain index, called Security Parameters Index (SPI).

How can IP Security be achieved?

Currently, There are two specific headers that can be attached to IP packet to achieve security. They are the IP Authentication Header (AH) and the IP Encapsulating Security Payload (ESP) header.

If confidentiality is not required, the Authentication Header (AH) alone can provide security (in this case, connectionless data integrity and data origin authentication) to IP datagram. The implementation can be host-host, host-gateway or gateway-gateway. But only host-host implementation is encouraged. The reason is that, in the case that security gateway provides security service for the trusted hosts behind the gateway, The security attack can still arise when the trusted hosts become untrusted. In other words the security can be violated for two communicating end user if the security (without confidentiality) does not cover completely the communicating path, but instead stop at the gateway, even though SA is established. Certainly in any kind of implementation, the untrusted systems (i.e., the systems that don't have the SA established) can't have the ability to attack data authentication (always referring to both data integrity and data origin authentication) .

The IP Encapsulating Security Payload (ESP) header provides integrity, authentication, and confidentiality to IP datagrams . It can provide a mix of optional security . ESP header can be applied alone, in combination with the IP Authentication Header(AH), or in a nested way, e. g. by using Tunnel-mode. The ESP header implementation can be host-host, host-gateway, or gateway-gateway. The ESP header is inserted after the IP header and before a higher-level protocol header(Transport-mode) or the encapsulated IP header(Tunnel-mode). Gateway-to-gateway ESP implementation, using encryption/decryption , is critical for building Private Virtual Networks (PVN) across an untrusted backbone in an open environment such as the Internet.

What is a Security Association (SA) ?

Security Association (SA) is needed for both the implementation of the IP Encapsulating Security Payload(ESP) header and of the IP Authentication Header(AH). An SA consists of the Destination Address and also some parameters, so-called Security Parameters Index (SPI) and thus it's receiver-oriented. The SPI at least contains the algorithm, algorithm mode and the keys used with the algorithm. In the ESP header case, certain sizes for determining synchronization and initialization of the encryption/decryption algorithm are also needed for the SPI. In addition, the SPI contains sensitivity level of data(for example, Secret or Unclassified) for systems meant to provide multi-level security. The sending host uses the sending userid and Destination Address to select a SA (and hence SPI value). The receiving host uses SPI value and Destination Address to

distinguish the association. Hence, an AH implementation will always be able to use the SPI and the Destination Address to determine the security association and related security configuration data for all valid incoming IP packets.

An SA is normally one-way . An authenticated communication between two hosts will have two Security Parameter Indexes (SPI) for both directions. For unicast traffic, the destination system selects the SPI value. For multicast traffic, there are multiple destination systems but a single destination multicast group, so some system or person selects SPIs for that multicast group. Multiple senders to a multicast group may use a single SA (and hence SPI) for all traffic to that group. In that case, the receiver only knows that the message came from a system knowing the SA data for that multicast group. Multicast traffic may use a separate SA (and hence SPI) for each sender to the multicast group . Otherwise a receiver cannot authenticate which system sent the multicast traffic when so-called symmetric (in contrast to asymmetric) authentication algorithms are used.

[Back to Table of Contents](#)

IP Security Mechanisms

In this section we discuss the format of two IP layer security mechanism, AH Header and ESP Header and their implementation and usage.

Authentication Header (AH) [\[1Atk-RFC1825\]](#)

[The IP AH header holds authentication information for its IP datagram . It achieves this by computing a *cryptographic* authentication function over the IP datagram and using a secret authentication key in the computation. The sender computes the authentication data , i.e., the Integrity Check Value, before it sends the authenticated IP packet. Fragmentation occurs after the appending of AH Header to outgoing packets and before the stripping of AH Header for incoming packets. The receiver rematches the authentication data upon reception. Certain fields which change along the path, such as the "TTL"\(time to live\) \(IPv4: version 4\) field or "Hop Limit" \(Ipv6: version 6\) field, both decrementing on each hop, are omitted from the authentication calculation.](#)

The AH Header Format

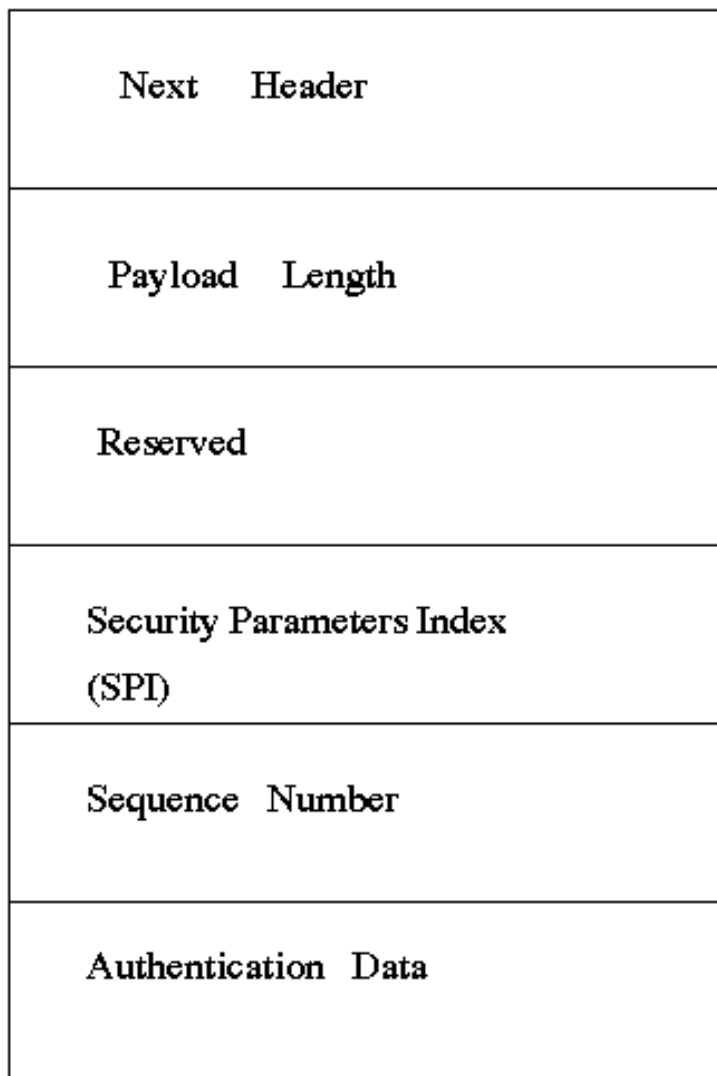


Figure 1. the Authentication Header (AH) format

- *Next Header.* An 8-bit field that identifies the type of the payload after the AH header, with value chosen from standard IP Protocol Numbers.
- *Payload Length.* An 8-bit field that specifies the length of AH header.
- *Reserved.* A 16-bit field reserved for future use. Now it's set to zero.
- *Security Parameters Index (SPI).* A 32-bit value field that identifies the Security Association (SA) for this datagram, relative to the Destination IP Address contained in the IP header.
- *Sequence Number.* A 32-bit field that contains a counter value (sequence number). Before cycle occurs, the sender and receiver have to reset the sequence number. The receiver ignores this field if anti-replay service is not requested.
- *Authentication Data.* An unfixed-length field that contains the Integrity Check Value (ICV) for this packet. It may include padding as certain algorithms require the AH header size to be a multiple of a blocksize. The ICV ignores those IP fields having a value unpredictable at reception. The ICV computation is based on authentication algorithm specified by the SA.

Using AH Header

AH Header may be used in Transport-mode or Tunnel-mode. In Transport-mode, AH header is appended before the IP header of an IP datagram and is only used for end-end implementation. The reason is that only higher-layer protocols and selected IP header fields are protected. In Transport-mode, AH header is inserted after the IP header and before an high-layer protocol (but before other Ipsec(urity) header such as ESP Header if that header is already inserted before higher-layer protocol.) For gateway security implementation, Tunnel-mode is required. In this case, AH header protects the entire inner IP packets,

including the entire IP header.

Non-repudiation, referring to being able to tell if the sender denies sending data, can be provided by some authentication algorithms (e.g., asymmetric algorithms when both sender and receiver keys are used in the authentication calculation) used with the AH Header. The default authentication algorithm is keyed MD5, which, like all symmetric algorithms, cannot provide non-repudiation by itself, because the sender's key is not used in the computation. Confidentiality protection are not provided by the AH Header.

Encapsulating Security Payload (ESP) Header

[\[1Atk-RFC1825\]](#), [\[3Ken-Atk\]](#)

The IP Encapsulating Security Payload (ESP) Header provides integrity, authentication, and confidentiality to IP datagrams . It does this by encapsulating either an entire IP datagram or only the higher-layer protocol (e.g., TCP--Transport Control Protocol) data inside the ESP, encrypting most of the ESP content, and then appending a new IP header to the now encrypted ESP Payload. This new IP header carries the protected data through the internetwork.

The ESP Header Format

Security Parameters Index (SPI)
Sequence Number
Initialization Vector
Payload Data
Padding
Padding Length
Next Header

Authentication Data

Figure 2. The Encapsulating Security Payload (ESP) Header format

- *Security Parameters Index (SPI)*. A 32-bit value field that identifies the SA for this datagram relative to the Destination Address.
- *Sequence Number*. A 32-bit field that contains a counter value (sequence number). Before a cycle arises, the counter is reset by establishing a new SA thus a new key. This field is optional depending on whether anti-replay service is required.
- *Initialization Vector*. An unfixed-length field only required by certain encryption/decryption algorithms.
- *Payload Data*. An unfixed-length field that contains data.
- *Padding*. A field for padding (margin-filling) Payload Data field if confidentiality is required, since then the block-size requirement for certain encryption/decryption algorithm has to be met.
- *Pad length*. A 8-bit field that identifies the size of the padding.
- *Next Header*. An 8-bit field that identifies the type of data contained in the Payload Data field.
- *Authentication Data*. An unfixed-length field that contains an Integrity Check Value(ICV) computed over the ESP packet (of course not including the field itself.) The mandatory-to-implement authentication algorithms, HMAC with MD5 or SHA-1, both yield a known ICV.

Using ESP Header

Like AH header, ESP header can also be implemented in Tunnel-mode, i.e., an entire IP datagram is encapsulated within the ESP header, or in Transport-mode, i.e., an higher-layer protocol (for example TCP or UDP --User Datagram Protocol) is encapsulated inside ESP and then a new IP header is appended. The encapsulating security used by ESP can impact network performance in systems establishing SA, but does not impact routers or other intermediate systems that are not in the ESP security association. Protocol processing in participating systems is more complex. Encrypting increases the communication latency.

The IP ESP Header may be used in combination with the IP AH header for requested security. The AH Header provides connectionless integrity and data origin authentication and can provide non-repudiation if used with certain authentication algorithms. The ESP header provides integrity and confidentiality and can also provide authentication if used with certain authenticating encryption algorithms. Adding the AH Header to a IP datagram before encapsulating that datagram using the ESP header can provide strong integrity, authentication, confidentiality. When the two mechanisms are combined, the positioning of the IP AH Header ensures which part of the data is being authenticated.

For communication throughout the worldwide Internet, implementations of the IP ESP header must support the use of the Data Encryption Standard (DES) in Cipher-Block Chaining (CBC) Mode (The mode is defined to be either block mode or stream mode). Cryptographic transforms for ESP which use a block-chaining algorithm and lack a strong integrity mechanism is subject to a cut-and-paste attack described by *Bellovin* and should not be used unless the Authentication Header is present with packets using that ESP transform.

[Back to Table of Contents](#)

Key Management

The key management protocol is related to AH header and ESP header only by the Security Parameters Index (SPI). It's agreed to exclude the key management mechanism from the other security mechanisms, such as AH header and ESP header. The reason is that it then allows using improved key management methods without modifying the implementations of the other

security mechanisms.

Key Distribution

Currently, most security systems are manually (by a person) configured with its own key and also with the keys of other communicating systems. Automated Key Distribution requires an Internet-standard scalable key management protocol. For Multicast Key Distribution for very large groups, new scalable techniques are needed. The use of Core-Based Trees (CBT) to provide session key management as well as multicast routing may be an approach used in the future .

Keying Approaches for IP

For host-oriented keying , users on one host share the same key on outgoing traffic destined for all users on another host. For user-oriented keying one user has one or more keys (not shared with other users on the same host) for its outbound traffic destined for another host with the SA associated..

When host-oriented keying is used and mutually untrusting users exist, it is possible for one user to determine the host-oriented key , and therefore can either read another user's (on the same host) encrypted traffic or forge traffic (impersonate). Integrity and Confidentiality can be provided by host-oriented keying when dynamic key management techniques and certain algorithms are in use. However, authentication using applications on end-systems requires that processes running applications be able to request and use their own SAs. Therefore, applications can access key distribution facilities that provide authentication.

[Back to Table of Contents](#)

Usage

[\[1A*tk*-RFC1825\]](#),

These two IP security mechanisms depends on the strength of the implemented cryptographic algorithms, the strength of the key being used, the security of the key management protocol. The security of the implementation is in part related to the security of the operating system environment . For example, if the operating system does not keep the private cryptographic keys (that is, all symmetric keys and the private asymmetric keys) confidential, then security can be defeated. Traffic analysis attack, which is not a primary concern at this time, can not be prevented by these two mechanisms.

The usage of IP AH header and IP ESP header can apply to many scenarios that we discuss now.

Use with Firewalls

Firewalls used with IP often need to parse the headers and options to determine the transport protocol (e.g., UDP or TCP) and the port number for that protocol. Firewalls can be used with the AH Header even when that firewall is not party to the SA, but a firewall not attached to the SA is normally not able to decrypt an encrypted higher-layer protocol to read the protocol or port number in needed to perform per-packet filtering or to verify that the data (e.g., source, destination, transport protocol, port number) for access control decisions is correct and authentic.

Organizations with two or more sites interconnected using commercial IP service can use a selectively encrypting firewall. If an encrypting firewall were placed between each site of a company and the commercial IP server, the firewall can provide an encrypted IP tunnel among all the company's site. Some organizations can use a fully encrypting firewall to provide a protected virtual network over commercial IP service. Different from an IP encryption device, a fully encrypting firewall provides both filtering of the decrypted incoming traffic and encrypting of outgoing traffic.

Use with IP Multicast

The Security Parameters Indexes (SPIs) in the IP security mechanisms are receiver-oriented(it at least contains the receiver's key). This is why these mechanisms are appropriate for multicasting , which has an ever-increasing capacity and performance in the Internet environment.

Use to provide QoS Protection

As QoS service becomes more frequently requested and more user-oriented, the data origin authentication has an ever-increasing importance. Authentication of packets can be provided by , e. g., AH Header. This authentication is important in packet classification within routers. The IPv6 Flow Identifier might act as a low-level Identifier. Used together, packet classification within routers becomes easy if the router is provided with the appropriate keying material. The authenticated packet classification helps ensure that each packet receives appropriate handling inside routers.

Use in Multi-level Networks

A multi-level secure network is one where a single network is used to communicate data at different sensitivity levels (e.g., Unclassified and Secret). Multi-level secure networking requires using strong Mandatory Access Controls, which ordinary users can not manipulate. The AH Header can provide security for both mandatory access control decisions in multi-level networks and discretionary access control decisions in all kinds of networks. If explicit IP sensitivity labels are used and confidentiality is not requested, the AH Header provides authentication for the entire packet, including cryptographic binding of the sensitivity level to the IP header and user data. IPv6 will normally use implicit sensitivity labels that are part of the SA but not attached with each packet during transmission. With appropriate key policies including that each key is used in a single sensitivity level, the ESP Header provides full multi-level secure networking. AH Header can also have different keys ,with the choice of key depending in part on the sensitivity level of the packet. Encryption is useful even when all of the hosts are within a protected subnet.

[Back to Table of Contents](#)

Reference

This reference collects RFC 1825 document and some internet drafts (work in progress in 1997) on the topic of IP security.

1. IETF RFC 1825, Security Architecture for Internet Protocol, R. Atkinson, Aug.,1995

This RFC provides the Internet Protocol (IP) security architecture.

<ftp://ftp.isi.edu/in-notes/rfc1825.txt>

- 2."IP Authentication Header", S. Kent, R. Atkinson, 07/22/1997.

The IP Authentication Header (AH) provides connectionless integrityand data origin authentication for IP datagrams and to provide protectionagainst replay attacks.

<ftp://ietf.org/internet-drafts/draft-ietf-ipsec-auth-header-01.txt>

- 3."IP Encapsulating Security Payload (ESP)", S. Kent, R. Atkinson,07/22/1997.

The Encapsulating Security Payload (ESP) header provides a mix of securityservices in IPv4 and IPv6, including confidentiality and integrity.

- 4."Internet Security Association and Key Management Protocol (ISAKMP)",D. Maughan, M.Schertler, M. Schneider, J. Turner, 07/29/1997.

This memo describes a protocol utilizing security concepts necessaryfor establishing Security Associations (SA) and cryptographic keys in anInternet environment.

<ftp://ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-08.txt>

5. "The OAKLEY Key Determination Protocol", H. Orman, 07/25/1997

This document describes a protocol, named OAKLEY, by which two authenticated parties can agree on secure and secret keying material.

<ftp://ietf.org/internet-drafts/draft-ietf-ipsec-oakley-02.txt>

6. "Implementation of Virtual Private Network (VPNs) with IP Security", N. Doraswamy, 03/14/1997.

This document discusses methods for implementing Virtual Private Networks (VPN) with IP Security (IPSec).

<ftp://ietf.org/internet-drafts/draft-ietf-ipsec-vpn-00.txt>

7. "IP Security Document Roadmap", R. Thayer, N. Doraswamy, R. Glenn, 07/30/1997.

The IPsec protocol suite is used to provide privacy and authentication services at the IP layer.

[Back to Table of Content](#)

IP security stands for ideally perfect security. (joke)

Last Modified August 14, 1997