R. Atkinson
Naval Research Laboratory

Security Architecture for the Internet Protocol

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

1. INTRODUCTION

This memo describes the security mechanisms for IP version 4 (IPv4) and IP version 6 (IPv6) and the services that they provide. Each security mechanism is specified in a separate document. This document also describes key management requirements for systems implementing those security mechanisms. This document is not an overall Security Architecture for the Internet and is instead focused on IP-layer security.

1.1 Technical Definitions

This section provides a few basic definitions that are applicable to this document. Other documents provide more definitions and background information [VK83, HA94].

Authentication
: The property of knowing that the data received is the same as the data that was sent and that the claimed sender is in fact the actual sender.

Integrity
: The property of ensuring that data is transmitted from source to destination without undetected alteration.

Confidentiality
: The property of communicating such that the intended recipients know what was being sent but unintended parties cannot determine what was sent.

Encryption
: A mechanism commonly used to provide confidentiality.

Non-repudiation
: The property of a receiver being able to prove that the sender of some data did in fact send the data even though the sender might later desire to deny ever having sent that data.

SPI
: Acronym for "Security Parameters Index". An unstructured opaque index which is used in conjunction with the Destination Address to identify a particular Security Association.

Security Association
: The set of security information relating to a given network connection or set of connections. This is described in detail below.

Traffic Analysis
: The analysis of network traffic flow for the purpose of deducing information that is useful to an adversary. Examples of such information are frequency of transmission, the identities of the conversing parties, sizes of packets, Flow Identifiers used, etc. [Sch94].

1.2 Requirements Terminology

In this document, the words that are used to define the significance of each particular requirement are usually capitalised. These words are:

- MUST

  This word or the adjective "REQUIRED" means that the item is an absolute requirement of the specification.

- SHOULD

  This word or the adjective "RECOMMENDED" means that there might exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before taking a different course.

- MAY

  This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor might choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

1.3 Typical Use

There are two specific headers that are used to provide security services in IPv4 and IPv6. These headers are the "IP Authentication Header (AH)" [Atk95a] and the "IP Encapsulating Security Payload (ESP)" [Atk95b] header. There are a number of ways in which these IP security mechanisms might be used. This section describes some of the more likely uses. These descriptions are not complete or exhaustive. Other uses can also be envisioned.

The IP Authentication Header is designed to provide integrity and authentication without confidentiality to IP datagrams. The lack of confidentiality ensures that implementations of the Authentication Header will be widely available on the Internet, even in locations where the export, import, or use of encryption to provide confidentiality is regulated. The Authentication Header supports security between two or more hosts implementing AH, between two or more gateways implementing AH, and between a host or gateway implementing AH and a set of hosts or gateways. A security gateway is a system which acts as the communications gateway between external untrusted systems and trusted hosts on their own subnetwork. It also provides security services for the trusted hosts when they communicate with the external untrusted systems. A trusted subnetwork contains hosts and routers that trust each other not to engage in active or passive attacks and trust that the underlying communications channel (e.g., an Ethernet) isn’t being attacked.

In the case where a security gateway is providing services on behalf of one or more hosts on a trusted subnet, the security gateway is responsible for establishing the security association on behalf of its trusted host and for providing security services between the security gateway and the external system(s). In this case, only the gateway need implement AH, while all of the systems behind the gateway on the trusted subnet may take advantage of AH services between the gateway and external systems.

A security gateway which receives a datagram containing a recognised sensitivity label, for example IPSO [Ken91], from a trusted host should take that label’s value into consideration when creating/selecting an Security Association for use with AH between the gateway and the external destination. In such an environment, a gateway which receives a IP packet containing the IP Encapsulating Security Payload (ESP) should add appropriate authentication, including implicit (i.e., contained in the Security Association used) or explicit label information (e.g., IPSO), for the decrypted packet that it forwards to the trusted host that is the ultimate destination. The IP Authentication Header should always be used on packets containing explicit sensitivity labels to ensure end-to-end

label integrity. In environments using security gateways, those gateways MUST perform address-based IP packet filtering on unauthenticated packets purporting to be from a system known to be using IP security.

The IP Encapsulating Security Payload (ESP) is designed to provide integrity, authentication, and confidentiality to IP datagrams [Atk95b]. The ESP supports security between two or more hosts implementing ESP, between two or more gateways implementing ESP, and between a host or gateway implementing ESP and a set of hosts and/or gateways. A security gateway is a system which acts as the communications gateway between external untrusted systems and trusted hosts on their own subnetwork and provides security services for the trusted hosts when they communicate with external untrusted systems. A trusted subnetwork contains hosts and routers that trust each other not to engage in active or passive attacks and trust that the underlying communications channel (e.g., an Ethernet) isn't being attacked. Trusted systems always should be trustworthy, but in practice they often are not trustworthy.

Gateway-to-gateway encryption is most valuable for building private virtual networks across an untrusted backbone such as the Internet. It does this by excluding outsiders. As such, it is often not a substitute for host-to-host encryption, and indeed the two can be and often should be used together.

In the case where a security gateway is providing services on behalf of one or more hosts on a trusted subnet, the security gateway is responsible for establishing the security association on behalf of its trusted host and for providing security services between the security gateway and the external system(s). In this case, only the gateway need implement ESP, while all of the systems behind the gateway on the trusted subnet may take advantage of ESP services between the gateway and external systems.

A gateway which receives a datagram containing a recognised sensitivity label from a trusted host should take that label's value into consideration when creating/selecting a Security Association for use with ESP between the gateway and the external destination. In such an environment, a gateway which receives a IP packet containing the ESP should appropriately label the decrypted packet that it forwards to the trusted host that is the ultimate destination. The IP Authentication Header should always be used on packets containing explicit sensitivity labels to ensure end-to-end label integrity.

If there are no security gateways present in the connection, then two end systems that implement ESP may also use it to encrypt only the user data (e.g., TCP or UDP) being carried between the two systems. ESP is designed to provide maximum flexibility so that users may select and use only the security that they desire and need.

Routing headers for which integrity has not been cryptographically protected SHOULD be ignored by the receiver. If this rule is not strictly adhered to, then the system will be vulnerable to various kinds of attacks, including source routing attacks [Bel89] [CB94] [CERT95].

While these documents do not specifically discuss IPv4 broadcast, these IP security mechanisms MAY be used with such packets. Key distribution and Security Association management are not trivial for broadcast applications. Also, if symmetric key algorithms are used the value of using cryptography with a broadcast packet is limited because the receiver can only know that the received packet came from one of many systems knowing the correct key to use.

1.4 Security Associations

The concept of a "Security Association" is fundamental to both the IP Encapsulating Security Payload and the IP Authentication Header. The combination of a given Security Parameter Index (SPI) and Destination Address uniquely identifies a particular "Security Association". An implementation of the Authentication Header or the Encapsulating Security Payload MUST support this concept of a Security Association. An implementation MAY also support other parameters as part of a Security Association. A Security Association normally includes the parameters listed below, but might include additional parameters as well:

- Authentication algorithm and algorithm mode being used with the IP Authentication Header [REQUIRED for AH implementations].

- Key(s) used with the authentication algorithm in use with the Authentication Header [REQUIRED for AH implementations].

- Encryption algorithm, algorithm mode, and transform being used with the IP Encapsulating Security Payload [REQUIRED for ESP implementations].

- Key(s) used with the encryption algorithm in use with the Encapsulating Security Payload [REQUIRED for ESP implementations].

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.