Introduction to IPSEC (Internet Protocol Security)

인터넷 보안 프로토콜 IPSEC

Y.B. Choi (최영배) Internet Service Department (네트워크소프트웨어연구팀 선임연구원)
S.O. Hwang (황성운) Internet Service Department (네트워크소프트웨어연구팀 연구원)
J.S. Lee (이준석) Internet Service Department (네트워크소프트웨어연구팀 선임연구원)
K.S. Yoon (윤기송) Internet Service Department (네트워크소프트웨어연구팀 책임연구원, 팀장)
M.J. Kim (김명준) Internet Service Department (인터넷서비스연구부 책임연구원, 부장)

IPSEC (Internet Protocol Security) is a network layer security protocol that is designed to support secure TCP/IP environment over the Internet considering flexibility, scalability, and interoperability. IPSEC primarily supports security among hosts rather than users unlike the other security protocols. Recently, IPSEC is emphasized as one of the important security infrastructures in the NGI (Next Generation Internet). It also has suitable features to implement VPN (Virtual Private Network) efficiently and its application areas are expected to grow rapidly. In this paper, the basic concepts and related standard documents of IPSEC will be introduced.

I. Definitions and Concepts

The IPSEC is an open architecture and an open framework defined by the IPSEC Working Group of the IETF (Internet Engineering Task Force). It provides a scalable, long lasting base for providing network layer security [1]. The IPv4 implementations are strongly recommended to support IPSEC and IPv6 implementations are required to do so. IPSEC provides the base security functions for the Internet and furnishes flexible building blocks from which secure and robust Virtual Private Networks (VPNs) can be constructed.

The IPSEC Working Group of the IETF has been working on defining protocols to address the following major areas:

- Data Origin Authentication: The verification that each datagram was originated by the claimed sender.
- Data Integrity: The verification that the contents of the datagram were not changed in transit, either deliberately or due to random errors.
- Data Confidentiality: The concealment of the cleartext of a message, typically by using encryption.
- Replay Protection: The assurance that an attacker can not intercept a datagram and play it back at some later time.
- Automated Management of Cryptographic Keys and Security Associations: The assurance that a company's VPN policy can be conveniently and accurately implemented throughout the extended network with little or no manual configuration. These functions make it possible for a VPN's size to be scaled to whatever size a business requires.

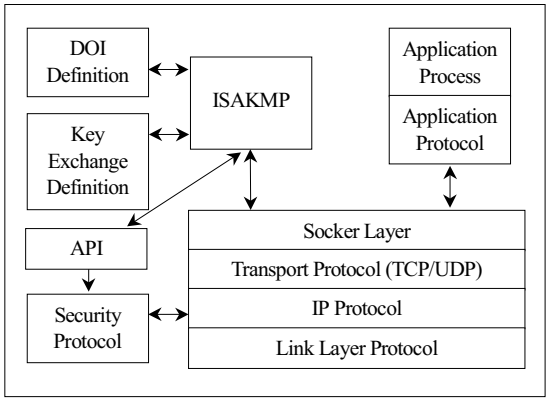

Fig. 1. Structure of IPSEC.

First, Fig. 1 shows the overall structure of IPSEC. IPSEC is a set of general-purpose protocols for protecting TCP/IP communications. In practice they work best for protecting traffic between hosts and not between users on a given host.

Next, we describe some basic terms and their concepts to understand IPSEC protocol more easily.

- Security Protocol: It consists of an entity at a single point in the network stack, performing a security service for network communication. IPSEC ESP (Encapsulating Security Payload), IPSEC AH (Authentication Header) and TLS are the examples.
- Protection Suite: A list of the security services that must be applied by various security protocols. For example, a protection suite may consist of DES encryption in IP ESP, and keyed MD5 in IP AH.
- SA (Security Association): An agreement between two peers on what and how of IPSEC protection: what types of protection to apply, how to do encryption or authentication, and which keys need to be used. A security association is uniquely identified (determined) by a triple consisting of a Security Parameter Index (SPI), an IP Destination Address, and a security protocol (AH or ESP) identifier. When a host applies IPSEC protection to an outgoing packet, it uses a security association belonging to the destination. The host applies the association's crypto method and key to the data to protect, and inserts the association's SPI in the IPSEC header. When the peer host processes the first IPSEC header in an incoming packet, the SPI is used to identify the appropriate security association. There are three kinds of SAs: AH and ESP SAs are always either oriented to-peer or from-peer and ISAKMP (Internet Security Association and Key Management Protocol) SAs are always bi-directional.
- SPI: To identify a particular SA, an application needs a peer address and a SPI. A SPI is basically a pointer to a particular SA, relative to some security protocol. A (security protocol, SPI) pair may uniquely identify an SA. Depending on the DOI, additional information (e.g., host address when the DOI is IPSEC) may be necessary to identify a SA. The DOI will also determine which SPIs (i.e., initiator's or responder's) are sent during communication.
- DOI (Domain of Interpretation): A DOI defines payload formats, exchange types, and conventions for naming security-relevant information such as security policies or cryptographic algorithms and modes. Within ISAKMP, all DOI's must be registered with the IANA (Internet Assigned Numbers Authority) in the "Assigned Numbers" RFC. The IANA Assigned Number for the Internet IP Security (IPSEC DOI) is one (1). Within the IPSEC DOI, all well-known identifiers must be registered with the IANA under the IPSEC DOI.
- Payload: ISAKMP defines several types of payloads, which are used to transfer information such as security association data, or key exchange data, in DOI-defined formats.

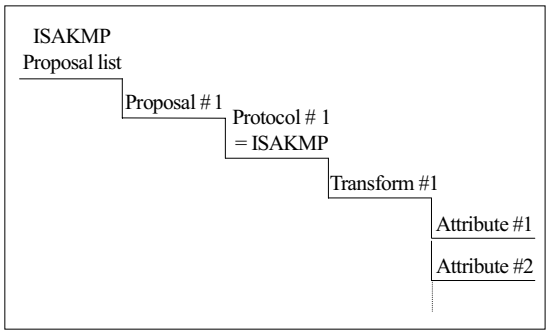

Fig. 2. Generic ISAKMP proposal diagram.

- Proposal, Transform and Attribute: When an application wants to establish a new security association with a peer, it presents one or more proposals to that peer. Each proposal contains a protection suite. A protection suite allows different protocols (AH, ESP, etc.) to be negotiated together. In the ISAKMP/Oakley framework, an application first establishes ISAKMP SAs with a peer in order to then establish AH or ESP SAs with that peer. When creating a request for an ISAKMP SA, there is only one protocol (ISAK MP of course!), so there can be only one proposal sent to the peer (see Fig. 2).

When the application is negotiating SAs for the AH and/or ESP protocols, there may be multiple proposals with different protection suites. Consequently an AH/ESP proposal list can become quite complex. For example, consider the proposal list shown in Fig. 3.

In the above proposal list, proposal 1 consists of

- The AH protocol using either MD5 (preferred) or SHA-1 and
- The ESP protocol using triple-DES

Proposal 2 consists of one protocol, ESP, using either DES (preferred) or triple-DES.

The application receiving this proposal could select one of the following protection suites:

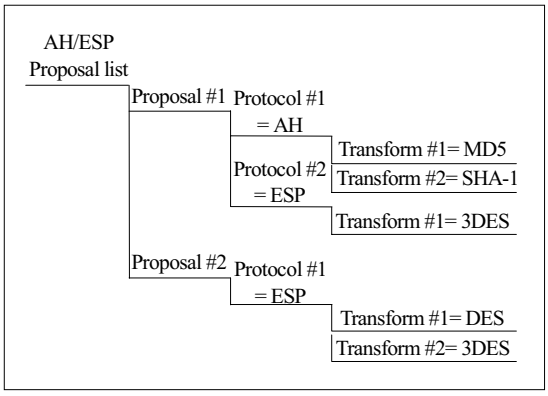

Fig. 3. AH/ESP proposal list with two proposals.

- AH using MD5 AND ESP using triple-DES (most preferred)
- AH using SHA-1 AND ESP using triple-DES
- ESP using DES
- ESP using triple-DES (least preferred)

II. Related Documents and Protocols

1. Related Protocols

This section describes the IPSEC related protocols. The major IPSEC related protocols are the IS AKMP, AH, ESP, and Oakley.

A. ISAKMP

The ISAKMP (Internet Security Association and Key Management Protocol) provides a mechanism for the automatic set-up of SAs and management of their cryptographic keys. A SA contains all the relevant information that communicating systems need in order to execute the IPSEC protocols, such as AH or ESP. ISAKMP defines a standardized framework to support negotiation of SAs, initial generation of all cryptographic keys, and subsequent refresh of these keys. Oakley [2] is the mandatory key management protocol that is required to be used within the ISAKMP framework. ISAKMP

supports automated negotiation of SAs, and automated generation and refresh of cryptographic keys. The ability to perform these functions with little or no manual configuration of machines will be a critical element as a VPN grows in size.

ISAKMP requires that all information exchanges must be both encrypted and authenticated: no one can eavesdrop on the keying material, and the keying material will be exchanged only among authenticated parties. The ISAKMP has been authenticated with explicit goals of providing protection against the following several well-known exposures:

- Denial of Service: The messages are constructed with unique 'cookies' that can be used to quickly identify and reject invalid messages without the need to execute processor-intensive cryptographic operations.
- Man-in-the-Middle: Protection is provided against the common attacks such as deletion of messages, reflecting messages back to the sender, modification of messages, replaying of old messages, and redirection of messages to unintended recipients.
- Perfect Forward Secrecy (PFS): Compromise of past keys provides no useful clues for breaking any other key, whether it occurred before or after the compromised key. Each refreshed key will be derived without any dependence on predecessor keys.

The IPSEC uses a 2-phase approach. In Phase 1, the cryptographic operations are the most processor-intensive to exchange a 'master secret' securely. In contrast, Phase 2 exchanges are less complex, since they are used only after the security protection suite negotiation in Phase 1 has been activated. A more detailed explanation is given in Appendix.

While the two-phased approach has a higher start-up cost for most simple scenarios, there are several reasons that it is beneficial for most cases. First, entities (e.g., ISAKMP servers) can amortize the cost of the first phase across several second phase negotiations. Note that Phase 1 negotiations use computationally intensive public key cryptographic operations (e.g., modular multiplication) many times, while Phase 2 negotiations use the less public key cryptographic operations, and the less computationally intensive symmetric key cryptographic operations. This allows multiple SAs to be established between peers over time without having to start over for each communication. Second, security services negotiated during the first phase provide security properties for the second phase. For example, after the first phase of negotiation, the encryption provided by the ISAKMP SA can provide identity protection, potentially allowing the use of simpler second-phase exchanges. Third, having an ISAKMP SA in place considerably reduces the cost of ISAKMP management activity — without the "trusted path" that an ISAKMP SA gives you, the entities (e.g., ISAKMP servers) would have to go through a complete re-authentication for each error notification or deletion of an SA.

B. AH

The IP AH provides connectionless (per-packet) data integrity and data origin authentication for IP datagrams, and, also offers replay protection. Data integrity is assured by the checksum generated by a message authentication code such as the Message Digest 5 (MD5). Data origin authentication is assured by providing a secret shared key in the data to be authenticated. Replay protection is assured by use of a sequence number field within the AH header. In the IPSEC all these three func tions are put together as the name 'authentication.'

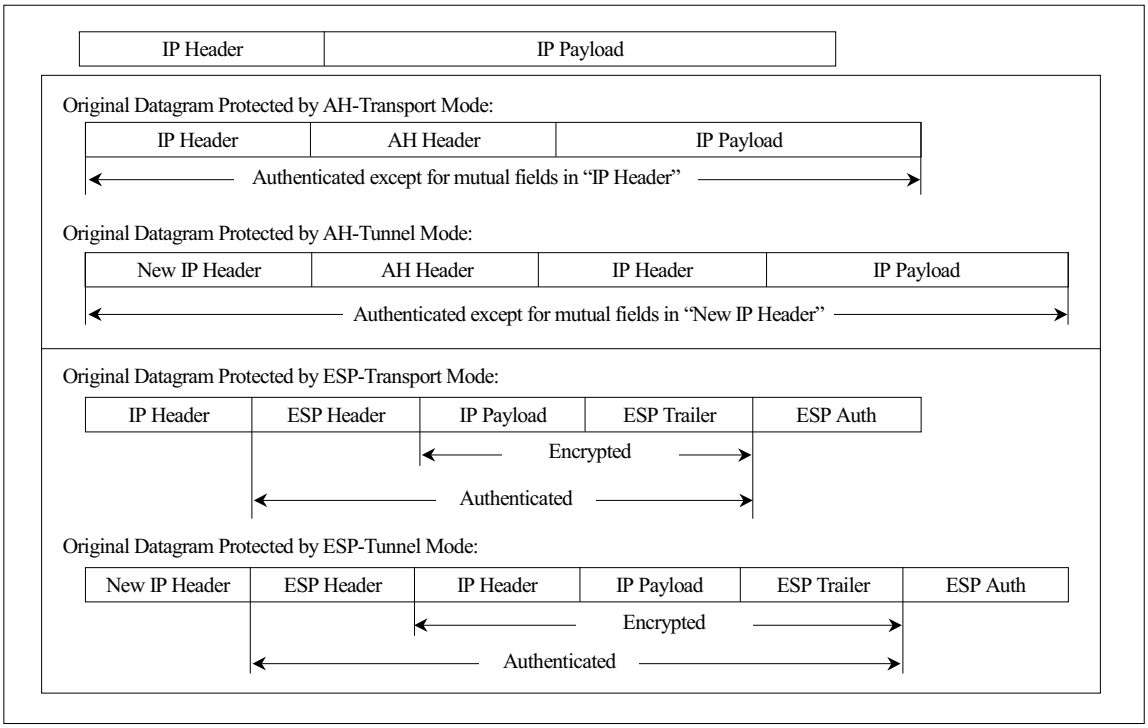

Fig. 4. AH/ESP Transport and Tunnel Mode.

The AH uses the Hashed Message Authentication Codes (HMAC) that applies a conventional key message authentication code two times continuously: first, to a secret key and the data (i.e., AH header plus IP payload), and then to a secret key and the output of the first step. Since the underlying message authentication code is MD5, the algorithm is called as HMAC-MD5. The other message authentication code that AH support is Secure Hash Algorithm (SHA): HMAC-SHA.

AH protects the entire contents of an IP datagram except for certain fields in the IP header ('mutable fields') that could normally be modified while datagram is intransit. The integrity check value is carried in the 'AH Header' field in Fig. 4.

AH can be applied in either transport mode or tunnel mode (see Fig. 4).

- Transport Mode: The entire original datagram, as well as the AH Header itself, is authenticated, and any change to any field except for the mutable fields can be detected. All information in the datagram is in cleartext form, and therefore is subject to eavesdropping while it is in transit.
- Tunnel Mode: A new IP header is generated for use as the outer IP header of the resultant datagram. The source and destination address of the new header will generally differ from those used in the original header. The entire datagram (new IP Header, AH Header, IP Header, and IP Payload) is protected by the AH protocol. Any changes to any field except the mutable fields in the tunnel mode datagram can be detected. All information in the datagram is in cleartext form, and therefore is subject to eavesdropping while it is in transit.

AH may be applied alone, combined with ESP, or even nested within another instance of itself. With these combinations, authentication can be supplied

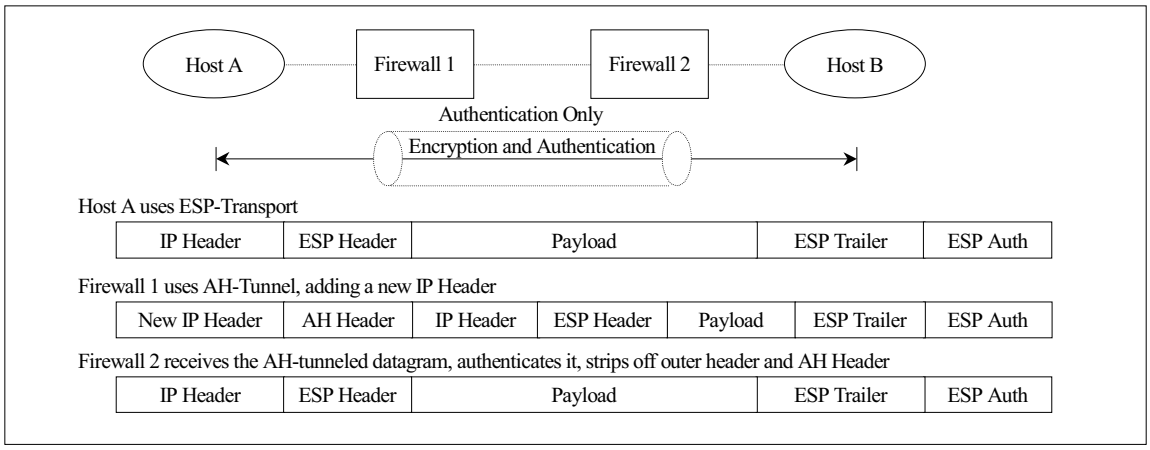

Fig. 5. Nesting of IP AH and ESP protocols.

between a pair of communication hosts, between a pair of communicating firewalls, or between a host and a firewall.

C. ESP

ESP always provides data confidentiality, and can also optionally provide data origin authentication, data integrity checking, and replay protection. ESP's encryption uses a symmetric shared key, that is, a shared key is used by both parties for encrypting and decrypting the data that is exchanged between them.

When ESP is used to provide authentication functions, it uses the same HMAC algorithms (HMAC-MD5 or HMAC-SHA) as are used by the AH protocol. But, the coverage is different as in Fig. 4 according to the mode of ESP.

ESP can be applied in transport mode or tunnel mode as in Fig. 4:

- Transport Mode: ESP's authentication functions protect only the original IP payload, but not the original IP header. The IP Header itself is neither authenticated nor encrypted, so the addressing information in the outer header is visible to an attacker while the datagram is in transit.
- Tunnel Mode: ESP's authentication functions protect the original IP Header and the IP Payload, but not the New IP header. Because the original IP Header is encrypted, its contents are not visible to an attacker while it is in transit. So, a common use of ESP tunnel mode is to hide internal address information while a datagram is 'tunneled' between two firewalls.

ESP may be applied alone, combined with AH, or even nested within another instance of itself. With these combinations, authentication can be supplied between a pair of communication hosts, between a pair of communicating firewalls, or between a host and a firewall.

D. The Use of IPSEC Transport and Tunnel Modes: AH and ESP

IPSEC's tunnel mode is an encapsulation technique modeled after RFC 2003 ('IP Encapsulation within IP'). The important points are:

- Transport mode is normally used between the end points of a connection. If secure communications were desired along all elements of a path from a client to a server, the client and the server would use IPSEC's transport mode.
- Tunnel mode is normally used between two ma-

chines when at least one of the machines is not an end point of the connection. The examples are the secure communications between two firewalls and the secure communication between a dial-up remote host and an entry gateway at its home network.

The following Fig. 5 shows the case where it is desirable to use IPSEC's transport and tunnel modes simultaneously-'nesting' or 'bundling.' Here, a path between a client and a server might pass through two firewalls (security gateways). The client and the server would use IPSEC's transport mode, while two firewalls would use IPS EC's tunnel mode. Figure 5 also shows how a composite datagram would be constructed when ESP is used between end points and AH is used between firewalls. Theoretically, encapsulation can be applied repetitively, but, practically, IPSEC protocols require support for only 2 levels of nesting.

E. Oakley

The Oakley protocol makes it possible for authenticated parties to agree on secure and secret keying material. The basic mechanism is the Diffie-Hellman key exchange algorithm. The Oakley protocol supports Perfect Forward Secrecy (PFS), compatibility with the ISAKMP protocol for managing security associations, user-defined abstract group structures for use with the Diffie-Hellman algorithm, key updates, and incorporation of keys distributed via out-of-band mechanisms [2].

2. Related Documents

This section describes IPSEC related documents. The IPSEC documents are in grouped as the architecture, AH Protocol, ESP Protocol, key management, DOI, authentication algorithm, and encryption algorithm. The following Fig. 6 shows the IPSEC Document Roadmap.

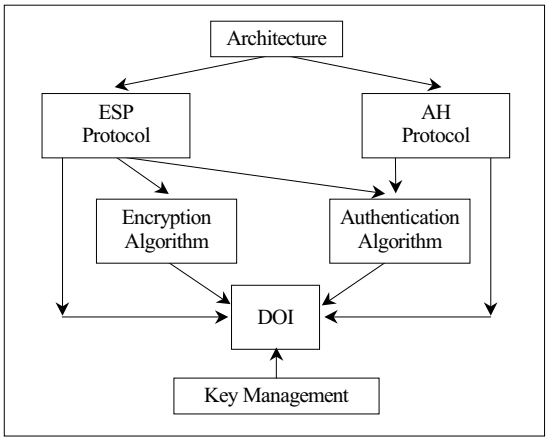

Fig. 6. IPSEC Document Roadmap.

A. Architecture

This document describes the general concepts, security requirements, definitions, and mechanisms of the IPSEC technology. The document [3] is the latest document of this type.

The document [3] specifies the base architecture for IPSEC compliant systems. The goal of the architecture is to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments. This document describes the goals of such systems, their components and how they fit together with each other and into the IP environments. It also describes the security services offered by the IPSEC protocols, and how these services can be employed in the IP environments. This document does not address all aspects of IPSEC architecture. Subsequent documents will address additional architectural details of a more advanced nature, e.g., use of IPSEC in NAT (Network Address Translation) environments and more complete support for IP multicast. The following fundamental components of the IPSEC security architecture are discussed in terms of their underlying, required functionality. Additional RFCs define

the protocols in (a), (c), and (d).

(a) Security Protocols: AH and ESP
(b) Security Associations: What they are and how they work, how they are managed, and associated processing
(c) Key Management: Manual and automatic (the Internet Key Exchange (IKE))
(d) Algorithms for authentication and encryption.

B. AH Protocol

This document describes the Authentication Header format, Authentication Header processing (Authentication Header location, authentication algorithms, inbound and outbound packet processing), Auditing, Conformance Requirements, and Security Considerations on the AH protocol of the IPSEC technology. The document [4] is the latest document of this type.

C. ESP Protocol

This document describes the ESP packet format, Encapsulating Security Protocol processing (ESP Header location, algorithms, inbound and outbound packet processing), Auditing, Conformance Requirements, and Security Considerations on the ESP protocol of the IPSEC technology. The document [ESP] is the latest document of this type.

D. Key Management

This document set is a collection of documents describing the IETF standards-track key management schemes. These documents must provide certain values such as the key length for the DOI document. Up to now, the documents [5] and the document [2] are examples.

The document [5] describes a protocol utilizing security concepts necessary for establishing SA and cryptographic keys in an Internet environment. The document [5] also explains the ISAKMP terminologies and concepts, ISAKMP Payloads, ISAKMP Exchanges, ISAKMP Payload processing, ISAKMP Security Association Attributes, and defining of a new DOI.

The document [2] describes a protocol, named OAKLEY, by which two authenticated parties can agree on secure and secret keying material. The basic mechanism is the Diffie-Hellman key exchange algorithm. This [2] explains the details on the OAKLEY such as the Protocol outline, specifying and deriving of Security Associations, ISAKMP compatibility, Security implementation, OAKLEY parsing and state machine, and Credential Payload.

E. DOI

This document is a part of the IANA (Internet Assigned Numbers Authority) Assigned Numbers mechanism and the values in the DOI document are already known. This document includes values for the other documents to relate with each other. For example, this document contains authentication algorithms, encryption algorithms, and operational parameters such as key lifetimes, etc.

The document [6] defines the Internet IP Security DOI (IPSEC DOI), which instantiates ISAKMP for use with IP when IP uses ISAKMP to negotiate security associations.

Within ISAKMP, a DOI is used to group related protocols using ISAKMP to negotiate security associations. Security protocols sharing a DOI choose security protocol and cryptographic transforms from a common namespace and share key exchange protocol identifiers. They also share a common interpretation of DOI-specific payload data content, including the Security Association and Identification payloads.

Overall, ISAKMP places the following requirements on a DOI definition:

(a) Definition of the naming scheme for DOI-specific protocol identifiers
(b) Definition of the interpretation for the Situation field
(c) Definition of the set of applicable security policies
(d) Definition of the syntax for DOI-specific SA Attributes (Phase 2)
(e) Definition of the syntax for DOI-specific payload contents
(f) Definition of additional Key Exchange types, if needed
(g) Definition of additional Notification Message types, if needed.

The remainder of this document detail the instantiation of these requirements for using the IP Security (IPSEC) protocols to provide authentication, integrity, and/or confidentiality for IP packets sent between cooperating host systems and/or firewalls.

F. Authentication Algorithm

This document set is a collection of documents describing how various authentication algorithms are used for both ESP and AH. Examples of this document are [7] and [8] documents. If these and other authentication algorithms are used for both ESP or AH, the DOI document must indicate certain values, such as algorithm type.

The document [7] describes the use of the HMAC algorithm [RFC2104] in conjunction with the MD5 algorithm [RFC1321] as an authentication mechanism within the revised IPSEC Encapsulating Security Payload [9] and the revised IPSEC Authentication Header [4]. HMAC with MD5 provides data origin authentication and integrity protection.

The document [8] describes the use of the HMAC algorithm [RFC2104] in conjunction with the SHA-1 algorithm [FIPS-180-1] as an authentication mechanism within the revised IPSEC Encapsulating Security Payload [9] and the revised IPSEC Authentication Header [4]. HMAC with SHA-1 provides data origin authentication and integrity protection.

The [7] and [8] each details algorithm and mode, keying material, interaction with the ESP Cipher Mechanism, and security considerations.

G. Encryption Algorithm

This document set is a collection of documents describing how various encryption algorithms are used for both ESP. Examples of this document are [10] and [11] documents. If these and other encryption algorithms are used for ESP, the DOI document must indicate certain values, such as encryption algorithm identifier, etc.

Notice: This document will be refined as the technical progress on the IPSEC is made.

III. Conclusion

We introduced the basic concept of IPSEC and its related terms. As IPSEC is a general architecture to support IP layer security on the Internet, it consists of several related protocols (authentication, encryption, key exchange) and documents. Here we gave an overview of them and their relationships. In particular, we tried to explain what SA is, how SAs are established between communicating peers, how IPSEC is applied in each case of AH and ESP protocol. Next, we are going to talk about VPN designs using IPSEC and their related issues.

Appendix: Key Management Process (Internet Key Exchange)

Key management protocol used in IPSEC is

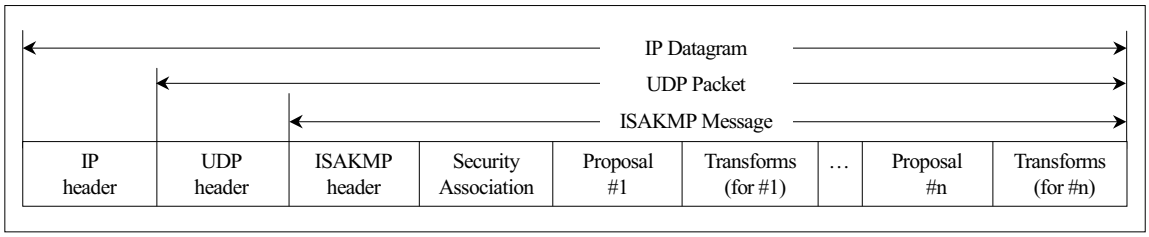

Fig. 7. ISAKMP Phase 1 SA Exchange.

composed two phases. The first phase, called ISAKMP main mode, generates a security association (called ISAKMP SA) and keys that are used for the protection of the second phase exchanges. The key management second phase is called ISAKMP quick mode. This phase generates a security association called non-ISAKMP SAs and keys that will be used to protect IP datagrams exchanged between the pair of users.

PHASE I: SETTING UP ISAKMP SA (ISAKMP/OAKLEY MAIN MODE)

The ISAKMP main mode process comprises three stages (each phase consists of two messages):

1. Cookie and SA negotiated (See Fig. 7)

- The two hosts negotiate the characteristics of the security associations (here all information is exchanged in the clear, unauthenticated form)
- Here, the cookie is a token that is derived from the host's IP address. Verification of the cookie ensures that the key management process is taking place within the appropriate session, with the correct peer. The pair of values <Cookie A, Cookie B> − which serves as an SPI for ISAKMP SA − provide a pointer to the correct algorithm and key to be used to en/decrypt the message. The two hosts negotiate the characteristics of the security associations by the initiator sending proposal, the responder agreeing on that proposal (clear, unauthenticated). The following is the parameters of SA that is contained in each proposal:
  - ISAKMP exchange type: MAIN MODE, AGGRESSIVE MODE
  - ISAKMP encryption algorithm: DES_CBC, 3DES_CBC, CAST_CBC
  - ISAKMP hash algorithm: MD5, SHA
  - ISAKMP authentication algorithm: pre-shared secret authentication, public key (RSA, DSS) signature authentication, public key encryption authentication
  - ISAKMP Diffie Hellman group description (prime number, generator): 768 bit, 1024 bit prime number
  - ISAKMP SA life time
- As we can see in Fig. 7, the above SA-related information is contained in the Security Association payload, and each proposal, transform information in each Proposal payload, Transform payload. And then ISAKMP header, UDP header, IP header is appended in the order and is sent to the peer host.

2. Diffie-Hellman Exchange (See Fig. 8)

The Diffie-Hellman Exchange stage generates the shared secret (or master secret) from which the symmetric ISAKMP keys are derived. During this stage, Diffie-Hellman public values and nonces are exchanged, contained in each Key Exchange payload, Nonce payload of Fig. 8 (clear, unauthenticated). The central property of the Diffie-Hellman

IP header	UDP header	ISAKMP header	Key Exchange	Nonce

Fig. 8. ISAKMP Phase 1 Diffie-Hellman Exchange.

algorithm is that, even if an adversary intercepts all the data exchanged during the execution of the algorithm, the shared secret still cannot be deduced.

3. Authentication Information Exchange
(See Fig. 9)

At this stage, the two hosts will exchange identity information with each other, for example, using digital signature algorithm to authenticate them. As shown in Fig. 9, the ISAKMP message will carry an Identity payload, a Signature payload, and an optional Certificate Payload. Only after both sides authenticate each other, the ISAKMP SA can be used.

IP header	UDP header	ISAKMP header	Identity	Certificate	Signature

Fig. 9. ISAKMP Phase 1 Authentication Information Exchange.

PHASE II: SETTING UP NON-ISAKMP SA (ISAKMP/OAKLEY QUICK MODE)

After having completed the ISAKMP/Oakley Phase 1 negotiation process to set up the ISAKMP SA, initiating host's next step is to initiate the ISAKMP/Oakley Phase 2 message exchanges to define the security associations and keys that will be used to protect IP datagrams exchanged between the pair of users. Since the purpose of the Phase 1 negotiations was to agree on how to protect ISAK MP messages, all ISAKMP Phase 2 payloads, but not the ISAKMP header itself, must be encrypted using the algorithm agreed to by the Phase 1 negotiations.

When Oakley Quick Mode is used in Phase 2, authentication is achieved via the use of several cryptographically-based hash functions. The input to the hash functions comes partly from Phase 1 information (i.e., keying material) and partly from information exchanged in Phase 2. Phase 2 authentication is based on certificates, but the Phase 2 process itself does not use certificates directly. Instead, it uses the keying material from Phase 1, which itself was authenticated via certificates.

Quick Mode comes in two forms:

- Without a Key Exchange attribute, Quick Mode can be used to refresh the cryptographic keys, but does not provide the property of Perfect Forward Secrecy (PFS). Enhanced security can be obtained by using the Perfect Forward Secrecy option, which prevents any association between successive session keys. This may, however, affect the key exchange performance as each exchange will take longer. Perfect Forward Secrecy means that the optional Diffie-Hellman component will be sent.
- With a Key Exchange attribute, Quick Mode can be used to refresh the cryptographic keys in a way that provides PFS. This is accomplished by including an exchange of public Diffie-Hellman values.

The ISAKMP Quick Mode process comprises three messages:

1. SA Proposal (See Fig. 10)

This message comprises the parameters of SA, proposed by the initiator, the IP address of the host or the subnet that will use this SA, and an optional Diffie-Hellman component. Here, the SPI value is randomly chosen by the initiator with the protocol (AH or ESP). The following is the parameters of SA which is contained in each proposal:

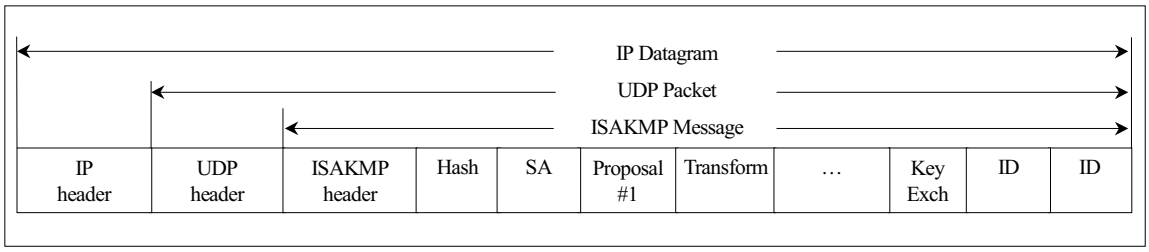

Fig. 10. ISAKMP Phase 2 SA Exchange.

- IPSEC protection mode: AH, ESP, IPCOMP
- IPSEC encapsulation mode: TUNNEL MODE, TRANSPORT MODE
- IPSEC HMAC algorithm: MD5, SHA
- IPSEC SA life time
- Diffie-Hellman component (optional)

Unlike the Phase 1 SA Exchange in Fig. 7, the Hash, Key Exch, two ID payloads are added in Fig. 10. Here Hash payload is made by hashing the following: master secret from Phase 1, Security Association, nonce, Diffie-Hellman public value from Phase 2, etc. Key Exch payload is optional and only desired when Perfect Forward Secrecy is desired. And two ID payloads are relevant if the initiator's host and the peer's host are acting as a proxy negotiator for another entity.

2. SA Response

After responder receives the above message, i.e., SA proposal and successfully authenticates it, it constructs a reply, SA response. This message comprises the parameters of the SA selected by the responder and the IP address of the host or the subnet that will use this SA. Responder's SPI does not depend in any way on the SPI that the initiator assigned to that protocol when it offered the proposal. If Diffie-Hellman is used, both sides generate a shared secret using Diffie-Hellman, like they did in the main mode. Otherwise, a new shared secret is derived from the Diffie-Hellman shared secret generated in the first phase.

At this point, initiator and responder have exchanged all the information necessary for them to derive the necessary keying material. Note that in the main mode, keys for the protection of the quick mode are generated. In the quick mode, from the shared secret generated in the main mode, two pairs of session keys are derived, one for transmitted datagrams and the other for received datagrams. Among these, one pair are for encrypting (or decrypting) session keys and another pair are authenticating (i.e., datagram integrity check) session keys. Thus, a single session between two hosts or subnets may involve four keys.

3. SA Acknowledge

This message is used to acknowledge to the responder that the initiator indeed accepted its response.

Glossary

CA	Certificate Authority
CBC	Cipher Block Chaining
DES-CBC	Data Encryption Standard-Cipher Block Chaining
DNS	Domain Name System
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
SHA	Secure Hash Algorithm
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

References

[1] *Using IPSEC to Construct Virtual Private Networks*, IBM, 1998.

[2] H. Orman, *The Oakley Key Determination Protocol*, RFC 2412, Nov. 1998.

[3] S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 2401, Nov. 1998.

[4] S. Kent and R. Atkinson, *IP Authentication Header*, RFC 2402, Nov. 1998.

[5] D. Maughan, M. Schertler, M. Schneider, and J. Turner, *Internet Security Association and Key Management Protocol (ISAKMP)*, RFC 2408, Nov. 1998.

[6] The Internet IP Security Domain of Interpretation for ISAKMP.

[7] C. Madson and R. Glenn, *The Use of HMAC-MD5-96 within ESP and AH*, RFC 2403, Nov. 1998.

[8] C. Madson and R. Glenn, *The Use of HMAC-SHA-1-96 within ESP and AH*, RFC 2404, Nov. 1998.

[9] S. Kent and R. Atkinson, *IP Encapsulating Security Payload (ESP)*, RFC 2406, Nov. 1998.

[10] C. Madson and N. Doraswamy, *The ESP DES-CBC Cipher Algorithm With Explicit IV*, RFC 2405, Nov. 1998.

[11] R. Periera and R. Adams, *The ESP CBC-Mode Cipher Algorithms*, RFC 2451, Nov. 1998.

[12] Jong-Hyeon Lee, *A Survey on IPSEC Key Management Protocols*, Computer Laboratory, University of Cambridge, United Kingdom, Dec. 1996.

[13] R. Thayer, N. Doraswamy, and R. Glenn, *IP Security Document Roadmap*, RFC 2411, Nov. 1998.

[14] Steven M. Bellovin, "Problem Areas for the IP Security Protocols," *The 6th VSENIX UNIX Security Symp*., San Jose, California, USA, July 1996.

[15] URL=http://www.ietf.org/html.charters/ipsec-charter.html.