SSH IPSEC Express
White Paper version 2.1

August 1999

SSH Communications Security Ltd
Tekniikantie 12
FIN-02150 ESPOO
FINLAND

SSH Communications Security, Inc.
650 Castro Street, Suite 220
Mountain View, CA 94041
USA

http://www.ipsec.com/
e-mail: ipsec-sales@ipsec.com (sales), ipsec-support@ipsec.com (technical support)
Tel: +358-9-4354 3208 (Finland), +1-650-404-0160 (USA)
Fax: +358-9-4354 3206 (Finland), +1-650-404-0161 (USA)

Contents

1 Summary **5**

2 IPSEC Protocol **7**

3 AH Transformations **9**

4 ESP Transformations **11**

5 Security Associations, SAs **13**

6 ISAKMP/Oakley (IKE) **15**

6.1 IKE Modes 15

6.1.1 Main Mode 15

6.1.2 Aggressive Mode 16

6.1.3 Quick Mode 16

6.1.4 New Group Mode 16

7 What is SSH IPSEC Express? **19**

7.1 SSH IPSEC Express and ISAKMP/Oakley Functional Overview 19

7.1.1 SSH IPSEC Packet Interceptor 21

7.1.2 SSH IPSEC Engine 21

7.1.3 SSH IPSEC Policy Manager 22

7.1.4 SSH ISAKMP/Oakley 22

7.1.5 Manual Keying 23

7.1.6 Certificate Processing Tools 23

7.2 Preventing Denial of Service Attacks 24

8 Conclusions **25**

9 Related Publications **27**

10 Terms and Abbreviations **29**

Chapter 1

Summary

The open architecture of the Internet Protocol (IP) makes it a highly efficient, cost effective, and flexible communication protocol for local and global communications. It has been widely adopted not only in the global Internet, but also in the internal networks of large corporations. However, IP is vulnerable to security risks that are complicating its full use for business and other purposes involving confidential data.

To enable new types of business opportunities with IP, a number of security solutions have been developed. So far, these solutions have lacked standards that make it possible to manufacture products that interoperate - a feature that is crucial for global communications.

IPSEC is an Internet Engineering Task Force (IETF) standard for protecting IP traffic on packet level. It can protect any IP-based service or application. IPSEC has been adopted by dozens of vendors, and will be the future standard for secure communications on the Internet.

The SSH IPSEC Express toolkit is a full, portable implementation of the IPSEC protocol intended for OEMs and system integrators who want to include IPSEC functionality in their own TCP/IP products.

The SSH IPSEC Express toolkit is highly efficient and provides unrestricted, strong cryptographic security. Its modular structure enables the vendors to flexibly choose the needed components for a specific implementation. SSH Communications Security's commitment to customer support, product quality, and new innovation ensure that the SSH partners can successfully offer leading IPSEC products to their customers now and in the future.

The SSH IPSEC Express toolkit makes it easy to integrate IPSEC into the existing TCP/IP stack of a vendor's product. It is designed to be easily portable and to have clean interfaces to the surrounding operating environment to facilitate easy integration into OEM products. The SSH IPSEC Express toolkit is highly interoperable. It has been thoroughly tested against all major IPSEC implementations in the market.

Chapter 2

IPSEC Protocol

With the help of cryptography, TCP/IP communication can be made secure without limiting its flexibility. Cryptographic methods and protocols have been designed for different purposes in securing communication on the Internet. These include, for example, the SSL for HTTP traffic, the SSH for secure login, S/MIME and PGP for e-mail, and the IPSEC for packet level security.

The purpose of the IPSEC protocol suite is to provide a standard, secure way for communicating by using the TCP/IP protocol. The IPSEC protocol is a set of security extensions developed by the IETF and it provides privacy and authentication services by using modern cryptographic methods. SSH Communications Security is not only following standards, but has been actively involved in the IETF IPsec effort and has been developing those standards.

To protect the contents of an IP datagram, the data is transformed using cryptography. There are two main transformation types that form the building blocks of IPsec, the Authentication Header (AH) transformation, and the Encapsulating Security Payload (ESP) transformation. These are configured in a data structure that is called a Security Association (SA).

Chapter 3

AH Transformations

The Authentication Header (AH) provides authentication (data origin authentication, connectionless integrity, and anti-replay protection services) to a datagram. It protects all the data in the datagram from tampering as specified in the Security Association, including the fields in the header that do not change in transit. However, it does not provide confidentiality.

An IPsec AH transformation calculates or verifies a Message Authentication Code (MAC) for the datagram being handled. More specifically, in the case of an outgoing datagram, an AH transformation calculates a MAC value as specified in the relevant IPsec standard. The MAC is calculated using the appropriate security association as specified by the transformation sequence that is applied. The resulting MAC code is attached to the datagram.

AH transforms can be made in either transport or tunnel mode. Transformation in transport mode means that the original packet's IP header will be the IP header for the transformed packet and tunnel mode transformation means the that packet is appended after a new IP header as shown below in Figure 3.1 (The AH transformations). Transformation in tunnel mode is typically used in a security gateway or a VPN device while the transport mode transformation is used in host-to-host communications.

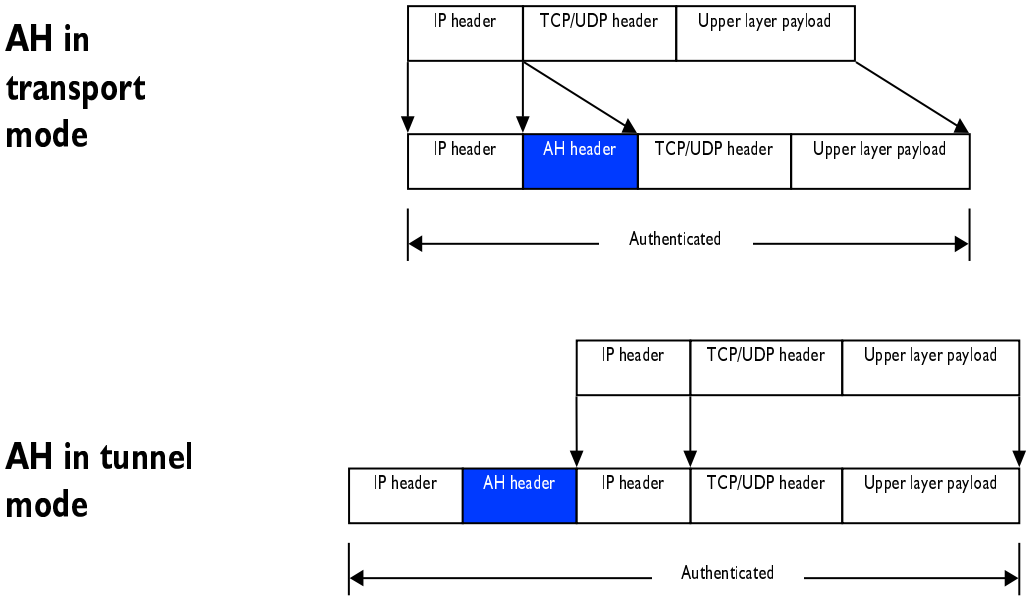


Figure 3.1: The AH transformations.

Chapter 4

ESP Transformations

The ESP header provides confidentiality, data origin authentication, connectionless integrity, anti-replay protection, and limited traffic flow confidentiality. It does this by encrypting the contents of the datagram as specified by the Security Association. The ESP transformations encrypt and decrypt portions of datagrams, optionally wrapping or unwrapping the datagram within another IP datagram. Optionally ESP transformations may perform data integrity validation and compute an Integrity Check Value (ICV) for the datagram being sent. Like AH, ESP can work in both tunnel and transport mode (see Figure 4.1 (Encapsulated Security Payload) below). In the case of a transport mode association, the upper layer payload along with any headers following the IP header are encrypted and enclosed within an ESP payload. If the transformation is a tunneling transformation, the complete IP datagram is enclosed within the ESP payload. A new IP header is generated and attached to the ESP payload. The new header will contain no IP options, independent of whether the original IP datagram had any IP options or not.

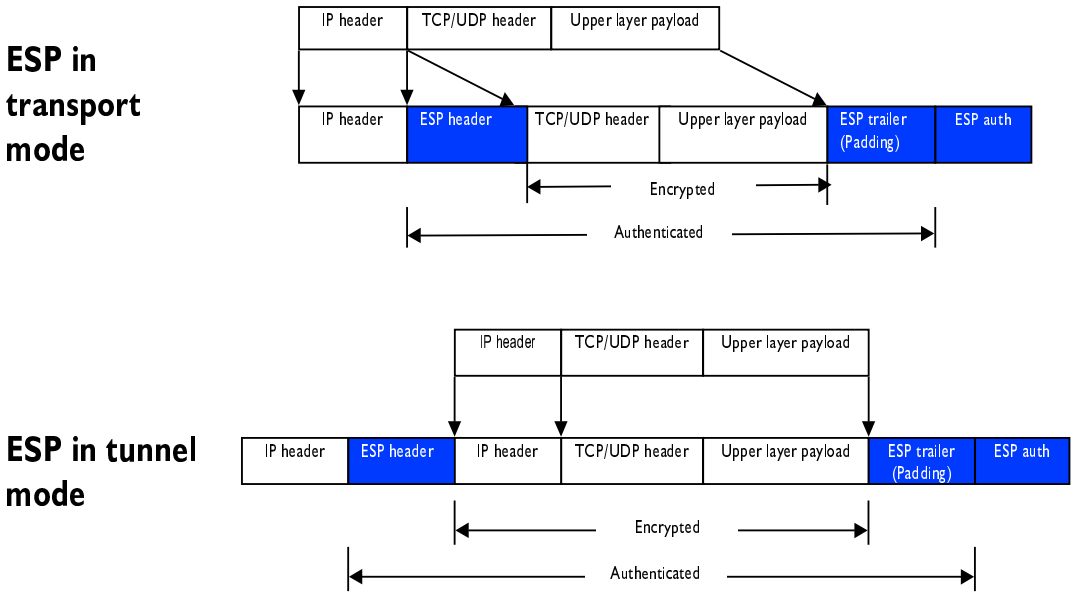


Figure 4.1: Encapsulated Security Payload.

Chapter 5

Security Associations, SAs

From the IPsec point of view, a Security Association is a data structure that describes which transformation is to be applied to a datagram, and how. The SA specifies the following parameters:

- The authentication algorithm for AH and ESP.
- The encryption algorithm for ESP.
- The encryption and authentication keys.
- Lifetime of encryption keys.
- The lifetime of the SA.
- Replay prevention sequence number and the replay bit table.

The size and contents of a Security Association are specified by the transformation. An association may be static, containing only data that is never changed by the transformation. Alternatively, it can be dynamic, containing data that is maintained by the transformation and changed whenever a datagram is handled. Serial number based replay prevention, compression are examples of transformations that need dynamic data.

An arbitrary 32-bit number called a Security Parameters Index (SPI), as well as the destination host's address and the IPsec protocol identifier, identify each SA. An SPI is assigned to a SA when the SA is negotiated. The SA can be referred to by using a SPI in AH and ESP transformations.

SA is unidirectional. They are commonly setup as bundles, because typically two SA's are required for communications. SA management is always done on bundles (setup, delete, rekey).

Chapter 6

ISAKMP/Oakley (IKE)

Before a secure session can begin, the communicating parties need to negotiate the terms for the communication. These terms are the ones that are defined in the Security Association (SA). There needs to be an automated protocol to establish the SAs to make the process feasible in a global network like the Internet. This automated protocol is the IKE. It is meant for establishing, negotiating, modifying, and deleting SAs. IKE combines the Internet Security Association and Key Management Protocol (ISAKMP) with the Oakley key exchange. ISAKMP is a framework for creating connection specific parameters that is not limited to IPsec, but currently IPsec is the only domain of interpretation for it. Oakley is the actual instantiation of the ISAKMP framework for IPsec key and SA generation.

6.1 IKE Modes

IKE works in two phases. The purpose of Phase I is to establish a secure channel for further negotiation traffic and authenticates the negotiating parties. It establishes a SA for the ISAKMP itself. Phase II negotiation is then used to establish the SA for IPsec. Though the two phase approach is more time consuming for the initial negotiation than just one phase negotiation would be, the benefits are gained as the more frequent Phase II negotiations can be performed faster after the Phase I negotiation has been made. There are two modes to establish the phase one SA: Main Mode and Aggressive Mode. They both accomplish the same thing, namely the SA. Aggressive Mode is a little faster, but it does not provide identity protection for the negotiating nodes. Quick Mode is used for establishing the Phase II SA, and as the name implies, using it is quick after Phase I negotiation has been made.

6.1.1 Main Mode

In the Main Mode, the negotiating parties use the first two messages to negotiate the security policy for the exchange. The next two messages perform a Diffie-Hellman key exchange and pass nonces to each other for signing and proving their identities. The last two messages are used to authenticate the negotiators with signatures or hashes and optional certificates.

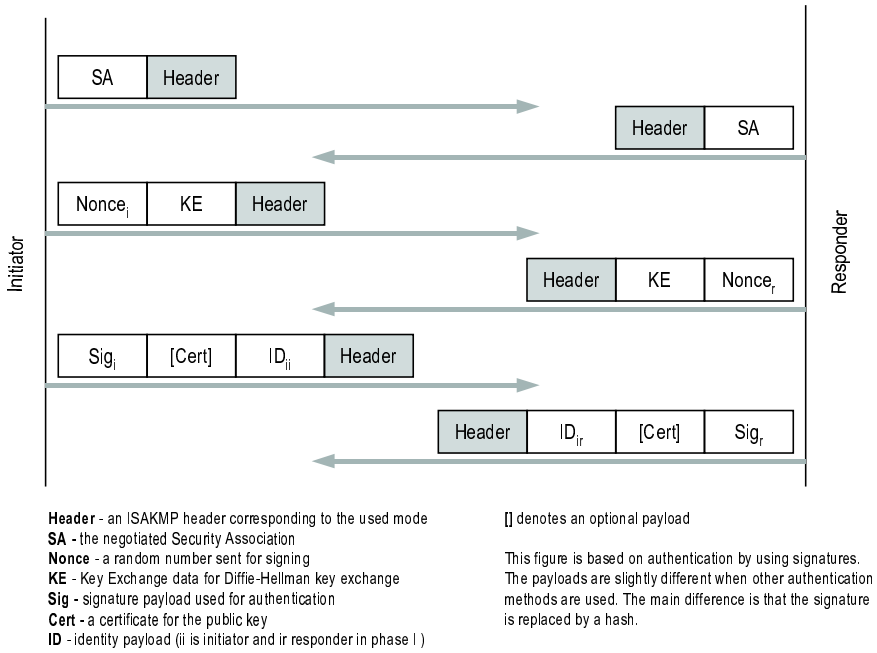


Figure 6.1: IKE Main Mode.

6.1.2 Aggressive Mode

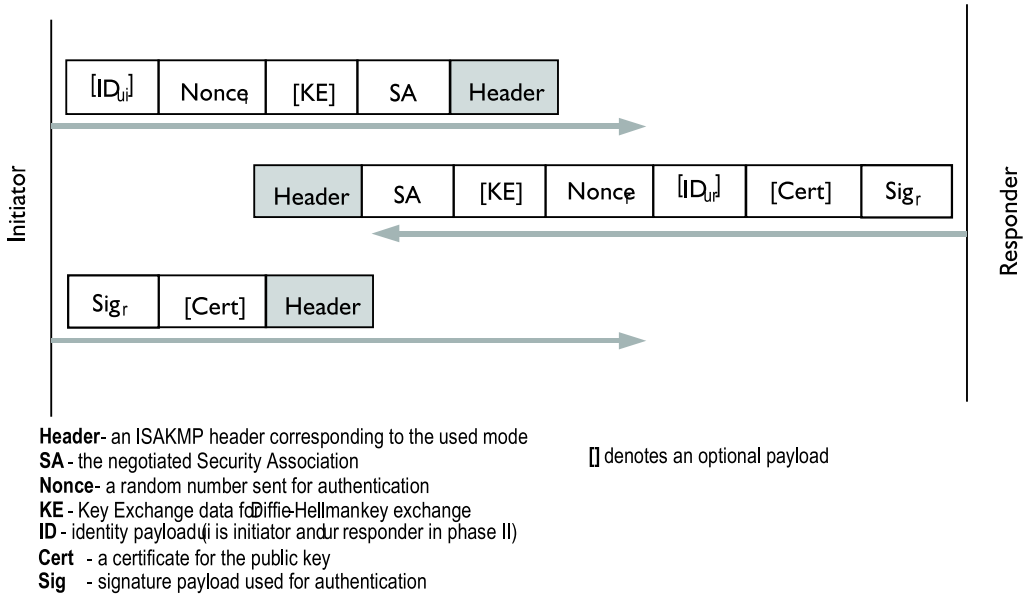
The Aggressive Mode resembles the Main Mode, but there are fewer exchanges. The first message proposes the policy, and passes data for key-exchange and the nonce for identification. The second message is a response that authenticates the responder and concludes the policy negotiation and key-exchange. The last message is used to authenticate the initiator.

6.1.3 Quick Mode

Quick mode is used to negotiate the IPsec security services and to generate new keying material. A full Diffie-Hellman key exchange may be done to provide perfect forward secrecy, though it is not mandatory. If no PFS is required, the parties just generate new key using hashes, and identify themselves by using nonces. Otherwise, the new keying material is included in the exchange.

6.1.4 New Group Mode

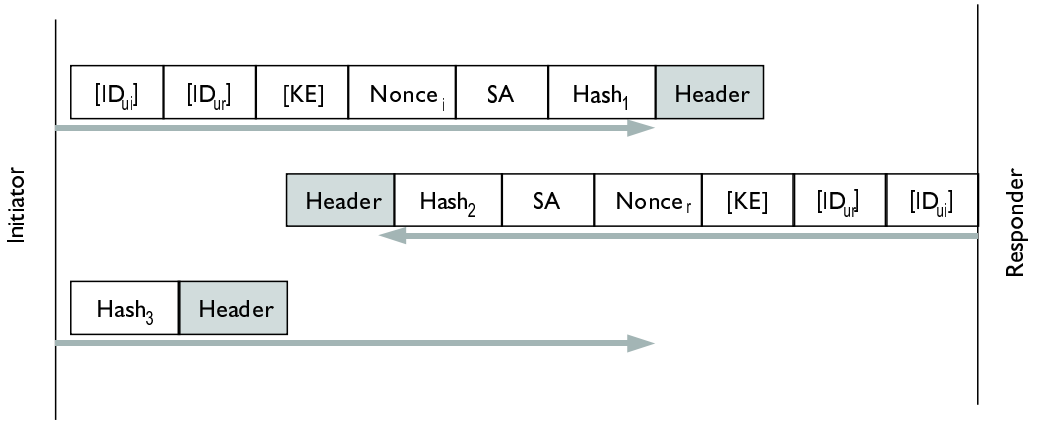
The purpose of the New Group Mode is to negotiate a new group (MODP or elliptic curve) where to do Diffie-Hellman exchange.



Header- an ISAKMP header corresponding to the used mode
SA - the negotiated Security Association
Nonce- a random number sent for authentication
KE - Key Exchange data for Diffie-Hellman key exchange
ID - identity payload (i is initiator and r responder in phase II)
Cert - a certificate for the public key
Sig - signature payload used for authentication

[] denotes an optional payload

Figure 6.2: IKE Aggressive Mode.



Header- an ISAKMP header corresponding to the used mode
SA - the negotiated Security Association
Nonce- a random number sent for authentication
KE - Key Exchange data for Diffie-Hellman key exchange
Hash - the output of a hash function over specified payload data
ID - identity payload (i is initiator and r responder in phase II)

[] denotes an optional payload

Figure 6.3: IKE Quick Mode.

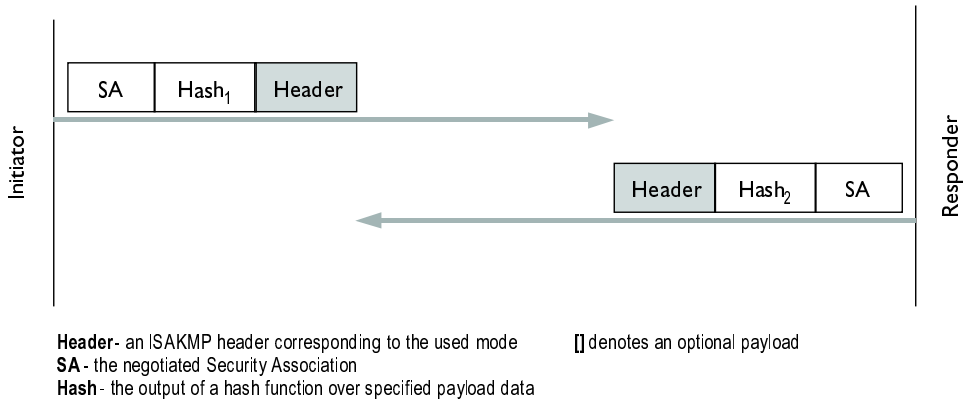


Figure 6.4: IKE New Group Mode.

Chapter 7

What is SSH IPSEC Express?

SSH IPSEC Express is a set of protocol implementations developed by SSH Communications Security Ltd. (SSH) according to the specifications set out by the Internet Engineering Task Force (IETF).

The implemented protocols include the IPsec Authentication Header (AH) and Encapsulated Security Payload (ESP) along with the standard transformations as specified by IETF. Both RFC defined old ESP and AH and new internet-draft versions of the protocols are implemented. The SSH IPSEC Express uses strong, unrestricted cryptography to provide maximum protection to confidential information.

The SSH ISAKMP/Oakley is a full implementation of the ISAKMP/Oakley protocol. It is a separate module from the SSH IPSEC Express and can be used together with SSH IPSEC Express, or as a separate key management product. It is also possible to use manual keying with the SSH IPSEC Express and adding support for more key management protocols is easy.

7.1 SSH IPSEC Express and ISAKMP/Oakley Functional Overview

The two major goals in the SSH IPSEC Express specification process are portability and architectural performance. The design reflects these contradictory goals.

The focus on portability has led to a design with a number of platform independent modules along with a number of well defined interfaces with platform specific modules and services. In order to ease source code analysis based security assurance, all security relevant functionality has been encapsulated in platform independent modules. The user is able to assure the security of the product by inspecting just one set of source code.

SSH IPSEC Express contains five basic parts, which are:

- SSH IPSEC Interceptor Module
- SSH IPSEC Packet Processing Engine

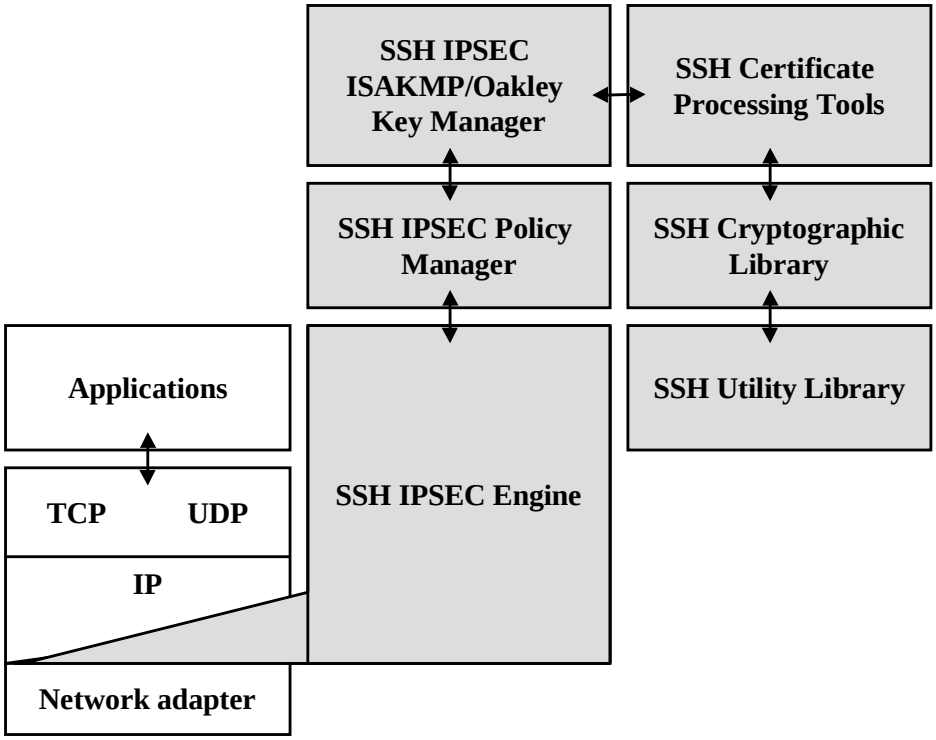


Figure 7.1: The integration of SSH IPSEC Express to the existing TCP/IP stack.

- SSH IPSEC Policy Manager
- SSH IPSEC ISAKMP/Oakley
- SSH IPSEC Certificate Processing Tools

Figure 7.1 (SSH IPSEC Express and the TCP/IP stack) shows one example on how SSH IPSEC Express interfaces with the underlying operating system. The SSH IPSEC Express can be thought as an additional protocol layer inserted between a TCP/IP implementation's IP layer and any number of network interfaces. SSH IPSEC Interceptor module represents this protocol layer. It is an operating system dependent portion of SSH IPSEC Express that passes packets from the network interfaces and the IP protocol stack to SSH IPSEC Express and back. It hides all operating system dependencies, so that the other modules can be adapted to new environments without major modifications.

The SSH IPSEC Interceptor module looks like a protocol when viewed from network adapter and like a network adapter when viewed from the upper protocol. The Interceptor module passes IP packets between operating system and the SSH IPSEC Engine.

The security transformation functionality means that security payloads are added, verified and/or removed. The payloads handled belong to the IP datagrams flowing from IP to the network interface and vice versa. The application and order of these transformations is directed by compiled interpreted byte-code, later called as filter-code. Using compiled filter code to direct how the transformations are applied is one of the novel ideas in SSH IPSEC Express, not found in other current IPsec implementations.

At a superficial level, the filter code resembles the packet filtering capabilities available in most modern TCP/IP routers. However, when combined with security transformation functionality, the expressive power greatly exceeds current router based filtering capabilities.

Above the SSH IPSEC engine is the SSH IPSEC Policy Manager, a level for policy-management. It is responsible for deciding whether or not certain connections can be established, how the corresponding parameters are set up, which certificates can be used for authentication, and what kind of limitations the parameters have. A limitation can be for example the maximum lifetime of a connection without re-keying or some algorithms that are not preferred.

The application level processes that handle key and security association negotiation form the topmost layer. These are called with the mutual name 'Key Managers'. Their task is to find appropriate key material and security association parameters based on which parties are connecting and the security policy given by the policy management and thus by the security administrator.

Key material can be pre-shared or generated on demand using the ISAKMP/Oakley protocol.

7.1.1 SSH IPSEC Packet Interceptor

The packet interceptor is an operating system dependent module. The module is injected between the IP protocol layer and any protected network interfaces at system start-up time.

The packet interceptor receives complete IP datagrams, or possibly fragmented IP packets, both from the IP protocol and network interfaces. As the packet interceptor is platform dependent, it has been designed to be as simple as possible to make porting to different platforms as easy as possible.

7.1.2 SSH IPSEC Engine

The primary purpose of the SSH IPSEC Express is to authenticate and secure communications. In practice this means performing security transformations to incoming and outgoing IP datagrams. The order and type of transformations is determined by filtering in the form of transformation sequences.

SSH IPSEC Engine performs three types of operations:

- IP packet filtering
- Security transformations
- Other transformations

In the SSH IPSEC Express framework, a security transformation may be an AH transformation, an ESP transformation, a compression transformation, or a special transformation. These are all discussed in detail below. A ”special transformation” is a term introduced for SSH IPSEC Express, it is not part of the IPsec standards track. Most special transformations handle IP options, filter packets based on their contents, or perform a network address translation (NAT).

If the size of a datagram exceeds the Maximum Transfer Unit (MTU) of the underlying network, the IPSEC Engine takes care that all necessary fragmentation will be performed.

IPSEC Engine is implemented in the operating system kernel.

Security Transformations

Security transformations are algorithmic modules that perform the ESP and AH transformations as specified in the standards. The transformation algorithms are fully re-entrant, making a later transition to parallelized architecture easier.

Special Transformations

Special transformations may be used to modify the IP header or the TCP/UDP header. They have nothing to do with AH and ESP transformations, which add or delete AH headers and ESP payloads, respectively. For example, a special transformation may be used for Network Address Translation, to redirect a certain port for all hosts within a network to a single host, e.g., a host performing a proxy key management server for all hosts within the network. As another example, a special transformation may be used to detect any IP routing options and drop any datagrams containing them.

7.1.3 SSH IPSEC Policy Manager

The purpose of the Policy Manager is to:

- Maintain the compiled filter language on behalf of the IPSEC Engine, thus keeping the actual IPSEC Engine small and fast.
- Create the filter code executed by the engine based on the SPD and SAIS.
- Communicate security association maintenance information to the IPSEC Engine (add, delete).
- Make policy decisions about acceptability of new connections based on local and remote identities.

Policy management gets requests from the IPSEC Engine and the key managers. There may also be a user interface that communicates with policy manager.

7.1.4 SSH ISAKMP/Oakley

The SSH ISAKMP/Oakley is a separate library from SSH IPSEC Express. It can be used as a part of SSH IPSEC Express or as a completely separate key management solution in conjunction with a third party IPsec Engine. The design goal has been to create an open solution that can be used with any IPsec Engine and

any CA. The structure enables easy integration to different Public Key Infrastructures (PKIs) with the help of certificate processing tools. Currently, the certificate tools support X.509v3 certificates.

The SSH ISAKMP/Oakley is a full ISAKMP/Oakley implementation that implements all the necessary phases and modes according to the latest drafts available, including support for the New Group Mode not found in many implementations. Compatibility options for older systems have also been implemented. Authentication can be done using several methods, including pre-shared keys, DSS signatures, RSA signatures, or RSA encryption.

To provide perfect forward secrecy, the SSH ISAKMP/Oakley supports Diffie-Hellman key exchange using the default 768-bit MODP or 1356-bit MODP groups. More groups over MODP can be freely negotiated.

Efficiency has been increased by, for example, supporting multiple Quick Mode SAs in one Quick Mode exchange and by supporting automatic randomizer generator during idle time to make Diffie-Hellman exponentiations faster.

7.1.5 Manual Keying

Manual keys are static cryptographic keys that have been pre-shared by security administrators. Static keys must be kept secret, as they are used for encryption and decryption as is.

In SSH IPSEC Express, manual keying is not intended for normal, every day use but mainly for testing and evaluation purposes. Using static keys makes replay prevention impossible and therefore SSH IPSEC Express will not check for replay prevention if the security association is marked as statically keyed by a key manager.

The Policy Manager implements manual keying.

7.1.6 Certificate Processing Tools

The SSH IPSEC Certificate Processing Tools enable the SSH ISAKMP/Oakley to use X.509v3 certificates. These tools make it possible to:

- Verify the X.509v3 certificates and add public keys to the public key database.
- Generate X.509v3 certificates, CRLs and ARLs.
- Generate PKCS #10 certificate requests.
- Traverse certificate chains up to a given Certificate Authority (CA).
- Check X.509 CLRs.
- Access LDAP directories for certificates and CRLs.

7.2 Preventing Denial of Service Attacks

Any host interfacing to the Internet, or any other insecure network, may become subject to Denial of Service (DoS) attacks.

The first prevention against resource exhausting DoS attacks is built into the IPsec protocol specifications. Within an incoming packet, the SPI value along with the destination address selects the security association used to decrypt or check the incoming datagram. If an adversary does not know any valid (protocol, SPI, destination address) triples, its probability to guess one is small. However, any party having a valid (protocol, SPI, destination address) triple can consume resources by sending encrypted or integrity protected packets that don't decrypt or appear to be valid.

In the SSH IPSEC Express, the input packet handling has been designed and implemented in such a way that a bad datagram is dropped as early as possible. No more resources than is necessary to determine the datagram's validity are consumed. If the datagram has a bad destination address or a bad source address, it is dropped. If the (protocol, SPI, destination address) triple is not found and security transformation is required, the datagram is dropped, and so forth.

There are also configurable limits on resource consumption such as the number of SAs and the number of SAs per host.

Chapter 8

Conclusions

IPsec is a technology that will solve many of the security problems of the current Internet. It has a wide support from all the major players in the industry. As the Internet grows, the market mandated by different organizations will demand security. The SSH IPSEC Express is a full IPsec implementation with ISAKMP/Oakley that brings the benefits of secure, interoperable communications to networking products. It supports all the latest features and standards and offers unique architectural solutions that enable easy and fast migration to a secure Internet.

Chapter 9

Related Publications

1. R. Atkinson, ”The IP Authentication Header”, RFC 1826. August 1995.
2. R. Atkinson, ”IP Encapsulating Security Payload (ESP)”, RFC 1827 Terminology
3. S. Kent, R. Atkinson, ”Security Architecture for the Internet Protocol”, Internet Draft. 1997.
4. S. Kent, R. Atkinson, ”IP Authentication Header”, Internet Draft. 1997.
5. S. Kent, R. Atkinson, ”IP Encapsulating Security Payload (ESP)”, Internet Draft. 1997.
6. C. Madson, N. Doraswamy, ”The ESP DES-CBC Cipher Algorithm With Explicit IV”, Internet Draft.1997.
7. C. Madson, R. Glenn, ”The Use of HMAC-MD5-96 within ESP and AH”, Internet Draft. 1997.
8. C. Madson, R. Glenn, ”The Use of HMAC-SHA-1-96 within ESP and AH”, Internet Draft. 1997.
9. R. Rivest, ”The MD5 Message Digest Algorithm”, RFC-1321. April 1992.
10. NIST, FIPS PUB 180-1: Secure Hash Standard. April 1995.
11. Comer, Douglas E. ”Internetworking with TCP/IP”, Vol 1. 3rd ed. New Jersey, Prentice Hall. 1995.
12. Denning, Dorothy E. R. ”Cryptography and Data Security”, Addison Wesley. 1983.
13. Halsall, Fred. ”Data Communications, Computer Networks and Open Systems”, 4th ed, Wokingham, Addison-Wesley. 1995.
14. Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A..” Handbook of Applied Cryptography”, New York, CRC Press. 1997.
15. Schneier, Bruce. ”Applied Cryptography - Protocols, Algorithms and Source Code in C”, 2nd ed. New York, John Wiley & Sons. 1996
16. Stevens, Richard W. ”TCP/IP Illustrated”, volume 1. Reading, Massachusetts. Addison Wesley. 1996

Chapter 10

Terms and Abbreviations

This section provides definitions for several key terms that are used in this document. Other documents provide additional definitions and background information relevant to this technology. Included in this glossary are generic security service and security mechanism terms, plus some SSH IPSEC Express-specific terms.

Access control A security measure that prevents unauthorized use of resources. In the IPSEC context, the resources to which access is being controlled are usually the computing cycles of a host, the data stored in it, the network behind a security gateway, or the bandwidth on that network.

Authentication Header (AH) An upper level header located between the IP header and a payload within an IP packet. Typically, an AH includes an ICV of the transfer-independent contents of the IP packet. The exact nature of the checksum depends on the transformation used. An AH is used to ensure the integrity of the whole IP packet, including both the payload and the IP header. It does not provide data confidentiality. The AH transformation is defined in RFC 2402.

Authentication The verification of the identity of a person or process. In a communications system, authentication verifies that messages come from their stated source. In relation to SSH IPSEC Express, this term is used to refer to the combination of two nominally distinct security services, data authentication and connectionless integrity.

Availability A security service that addresses the security concerns engendered by attacks on networks that deny or degrade service. For example, in the IPsec context, the use of replay prevention mechanisms in AH and ESP support availability.

BITS Bump-in-the-stack. Denotes the possible location of an IPsec implementation compared with the location of the TCP/IP stack. In a BITS implementation, IPsec is located underneath an existing implementation of an IP stack, between the native IP and the local network drivers. Source code access for the IP stack is not required in this context, making this implementation approach appropriate for use with legacy systems. This approach, when it is adopted, is usually employed in hosts.

BITW Bump-in-the-wire. Denotes the possible location of an IPsec implementation compared with the location of the TCP/IP stack. In a BITW implementation, an outboard crypto processor is used. Such im-

plementations may be designed to serve either a host or a gateway (or both). Usually the BITW device is IP addressable. When supporting a single host, it may be quite analogous to a BITS implementation, but in supporting a router or firewall, it must operate like a security gateway.

Certification Authority (CA) An entity that attests to the identity of a person or an organization. A CA can be an external company that offers certificate services or it can be an internal organization such as a corporate Management Information System (MIS) department. The chief function of the CA is to verify the identity of entities and issue digital certificates attesting to that identity.

Certificate A digital document which is used for verifying the identity of the other end of the transmission. Any type of address including domain names, IP and email addresses can be authenticated using certificates. Current SSH products use X.509 certificates.

Confidentiality A security service that protects data from unauthorized disclosure. Usually, unauthorized disclosure of application level data is the primary concern, but the disclosure of the external characteristics of communication can also be a concern in some circumstances. The traffic flow confidentiality service addresses this latter concern by concealing source and destination addresses, message length, or frequency of communication. In the IPsec context, using ESP in tunnel mode, especially at a security gateway, can provide some level of traffic flow confidentiality. See also traffic analysis.

Compression Parameter Index (CPI) A field in the IPCOMP header that denotes the algorithm to be used on payload compression. See also SPI.

Denial of Service (DoS) Denotes attacks that do not cause a security violation per se, but harm the availability of a service. For example, if an attacker sends lots of forged packets to an SSH IPSEC VPN host, they may degrade the performance of the host. One of the design goals in the SSH IPSEC architecture has been minimizing the consequences of Denial of Service attacks.

Encryption A security mechanism used for the transformation of data from an intelligible form (plaintext) into an unintelligible form (ciphertext), to provide confidentiality. The inverse transformation process is designated decryption, but encryption is often used to generically refer to both processes.

Encapsulating Security Payload (ESP) An upper level IP header that denotes that the contents of the payload are encrypted and possibly also otherwise protected. An ESP may appear after the IP header, after an ESP header or theoretically also elsewhere within an IP packet. An ESP only protects the contents of the payload, not any associated header. Therefore, it is possible, for example, to change any field in the header of the IP packet carrying an ESP without causing a security violation. The contents of the ESP header are unknown to anyone not possessing information about the transformation and SA needed to recover the protected data. An ESP may also contain integrity protection. The ESP protocol is defined in RFC 2406.

HMAC Hash Message Authentication Code. A secret key authentication algorithm. Data integrity and data origin authentication as provided by HMAC depend on the scope of the distribution of the secret key. If only the source and destination know the HMAC key, this provides both data origin authentication and data integrity for packets sent between the two parties. If the HMAC is correct, this proves that it must have been added by the source.

Integrity Check Value (ICV) Usually, an HMAC algorithm using either Message Digest 5 (MD5) or SHA-1 hash functions, but possibly also a DES-MAC or HMAC-RIPEMD algorithm. See also integrity.

Internet Key Exchange daemon (IKEd) The Internet Key Exchange daemon is an architectural component of SSH IPSEC Express responsible for negotiating and setting up SAs. The SSH IPSEC Express policy management is also combined IKEd, that makes policy decisions according to the rules set up by security administration.

Integrity A security service that ensures that data modifications are detectable. Integrity services need to match application requirements. IPsec supports two forms of integrity: connectionless integrity and replay prevention. This is in contrast to connection-oriented integrity, which imposes more stringent sequencing requirements on traffic to be able to detect lost or re-ordered messages, for example. Although authentication and integrity services are often cited separately, in practice they are intimately connected and almost always offered together.

Message Authentication Code (MAC) A mechanism that provides message integrity by using a secret key cryptographic function.

Packet filtering A method for determining how passing IP packets should be handled. Packet filtering is applied to all IP packets passing the IPSEC Engine. Packet filtering may modify the IP packet, pass it intact, or even drop it.

Security Parameters Index (SPI) An arbitrary value used in combination with a destination address and a security protocol to uniquely identify an SA. The SPI is carried in AH and ESP protocols to enable the receiving system to select the SA under which a received IP packet will be processed. An SPI has only local significance as it is defined by the creator of the SA, which is usually the receiver of the IP packet carrying the SPI. Thus an SPI is generally viewed as an opaque bit string. However, the creator of an SA may choose to interpret the bits in an SPI to facilitate local processing. This term is defined in RFC 2401.

Traffic analysis The analysis of network traffic flow for the purpose of deducing information that is useful to an adversary. For example, frequency of transmission, the identities of the conversing parties, sizes of IP packets, and flow identifiers.

Transformation A particular type of change applied to an IP packet. For example, ESP encryption, AH integrity service, and payload compression are transformation types. An SA supplies the keys and other association-specific data to a transformation. The IPSEC transformations are defined in RFC 2401, RFC 2402, RFC 2403, RFC 2404, RFC 2406, and RFC 2405.

Transformation sequence A set of transformations applied to an IP packet one after another. For example an outgoing IP packet can be protected first with and ESP to ensure data confidentiality and higher level data integrity, and then with an AH to protect the integrity of the IP header carrying the IP packet. In this case, the transformation sequence consists of an ESP transformation followed by an AH transformation. SSH IPSEC supports also other types of transformations, and therefore transformation sequences may occasionally be rather long, even 5 or 6 steps. However, typically most transformation sequences consist of just one or two steps. This is discussed in RFC 2401.

Trusted subnetwork A subnetwork of hosts and routers that can trust each other not to engage in active or passive attacks. It is also assumed that the underlying communications channel such as a LAN or CAN is not being attacked by any other means.

