ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

AN INTRODUCTION TO IPsec (INTERNET PROTOCOL SECURITY)

By Sheila Frankel, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

In its early days, the Internet was the domain of academics and researchers. Its goal was to maximize communication, connectedness and collaboration, and to minimize barriers that would detract from the realization of those goals. By the late 1980s, it became apparent that some individuals were abusing the capabilities of the Internet and were reading or changing information they shouldn't, and even deliberately causing some Internet services to fail. Security continues to be a major concern in today's Internet. Fundamental changes to improve the security of basic Internet services have been slow in their development. In the intervening time, two types of solutions have emerged in response to the security hazards that threaten Internet traffic: localized solutions and application-specific solutions. The localized solutions are attempts by computer network administrators to isolate or fortify their particular fiefdoms, and take the form of screening routers, firewalls, defensive scanners, and the elimination of known security holes from operating systems and application programs. The application-specific solutions are applied to specific applications, such as electronic commerce or e-mail, and are agreed upon by some segment of the user population.

Over time, it became obvious that these techniques were not general enough and that security services must be added to the Internet Protocol (IP) itself. In 1992 the Internet Engineering Task Force (IETF) began such an effort called IPsec. What differentiates IPsec from other solutions? IPsec is an attempt to utilize cryptographic techniques in a more global solution to the problem of Internet security. Rather than requiring each e-mail program or web browser to implement its own security mechanisms, IPsec involves a change to the underlying networking facilities that are used by every application. It also allows network managers to apply protection to network traffic without involving the end users.

What is IPsec used for today? Figure 1 shows two typical scenarios: the "road warrior" and the Virtual Private Network (VPN). A road warrior is a busi-

Continued on page 2

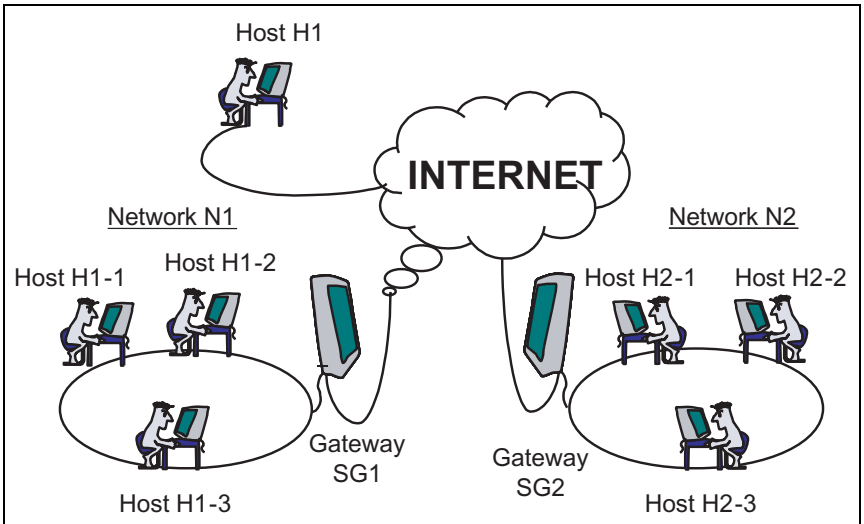


Figure 1: IPsec Usage Scenarios

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since September 1999

- *Securing Web Servers,* September 1999
- *Acquiring and Deploying Intrusion Detection Systems*, November 1999
- *Operating System Security: Adding to the Arsenal of Security Techniques,* December 1999
- *Guideline for Implementing Cryptography in the Federal Government*, February 2000
- *Security Implications of Active Content*, March 2000
- *Mitigating Emerging Hacker Threats*, June 2000
- *Identifying Critical Patches with ICAT*, July 2000
- *Security for Private Branch Exchange Systems*, August 2000
- *XML Technologies*, September 2000
- *An Overview of the Common Criteria Evaluation and Validation Scheme*, October 2000
- *A Statistical Test Suite for Random and Pseudorandom Number Generators For Cryptographic Applications*, December 2000
- *What Is This Thing Called Conformance?* January 2001

ness employee who is working at home or at another location away from their office and needs to access an office computer. IPsec can ensure that those communications are conducted in a private, tamper-proof manner. Another common use of IPsec is the creation of a VPN. If a company needs to conduct secure communications among scattered locations, a private network can be constructed by leasing or stringing private communication lines. A less expensive and more flexible alternative is a VPN that uses the Internet as the communications medium and employs IPsec to ensure that these communications are indeed private. Although the VPN's traffic crosses the public Internet, IPsec protection prevents unauthorized outsiders from reading or modifying the traffic. In Figure 1, the road warrior's host, H1, provides its own IPsec protection; networks N1 and N2 obtain their IPsec protection from the VPN connecting security gateways SG1 and SG2, respectively.

Security Protections Provided by IPsec

IPsec can provide some or all of the following types of protection.

- **Connectionless Integrity**: a guarantee that the message that is received is the exact one that was sent, and no tampering has occurred. Why "connectionless"? This is because communications at the Internet layer follow a Post Office model (as opposed to a Phone Company model). Messages are sent from the sender to the receiver, but no attempt is made to ensure that they are received in order, or that any (or all) were in fact received. That task is left to one of the upper layer protocols.
- **Data Origin Authentication**: a guarantee that the message actually was sent by the apparent originator of the message, and not by another user masquerading as the supposed message originator.
- **Replay Protection**: assurance that the same message is not delivered multiple times and that messages are not delivered grossly out of order. This capability must be implemented by the sender, and the receiver may optionally enable its use.
- **Confidentiality** or **privacy**: a guarantee that, even if the message is "read" by an observer, the contents are not understandable, except to the authorized recipient.
- **Traffic analysis protection**: an assurance that an eavesdropper cannot determine who is communicating with whom or determine the frequency and volume of communications between specific entities.

IPsec Context and Components

IPsec is a protocol that operates within the Internet Protocol (IP). IP in turn is one part of a layered suite of communication protocols known as TCP/IP. The upper layers, the transport and application layers, rely on the Internet layer protocol, IP, for the following:

- transmitting messages (generally called packets in this context) from one host to another
- routing the messages so that they arrive at the desired destination
- if the messages are too large to be transmitted by one or more of the network links encountered along the way, breaking the messages into smaller fragments and, at the other end, re-assembling the fragments to reconstruct the original message

IP accomplishes these tasks through the use of the IP header, which is inserted at the beginning of each message and contains all of the information (source and destination addresses, etc.) required for the message to traverse the Internet and arrive at its destination.

The IPsec protocols are additions to IP that enable the sending and receiving of cryptographically protected messages. This is accomplished through the use of two special IPsec headers, inserted immediately after the IP header in each message. The Encapsulating Security Protocol (ESP) Header provides privacy and protects against malicious modification, and the Authentication Header (AH) protects against malicious modification without providing privacy. The Internet Key Exchange (IKE) protocol is a mechanism that allows for secret keys and other protection-related parameters to be exchanged prior to a communication without the intervention of the user. The IPsec and IKE protocols are being developed within the IPsec working group under the umbrella of the Internet Engineering Task Force (IETF).

The Authentication Header (AH) and the Encapsulating Security Payload (ESP) Header

AH uses a keyed message authentication algorithm (MAC) to provide connectionless integrity and data origin authentication protection. This protection covers the packet's data portions, as well as certain portions of the IP header: those IP header fields that cannot change in an unpredictable manner as the packet traverses the Internet. The ESP header can also provide integrity and authentication protection through the use of a keyed MAC. In addition to, or in place of, these types of protection, the ESP header can use an encryption algorithm to provide confidentiality. The ESP's protections cover the packet's data, but not the IP header. Both AH and ESP can provide replay protection. Each header identifies the types

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our Web site is http://www.itl.nist.gov/.

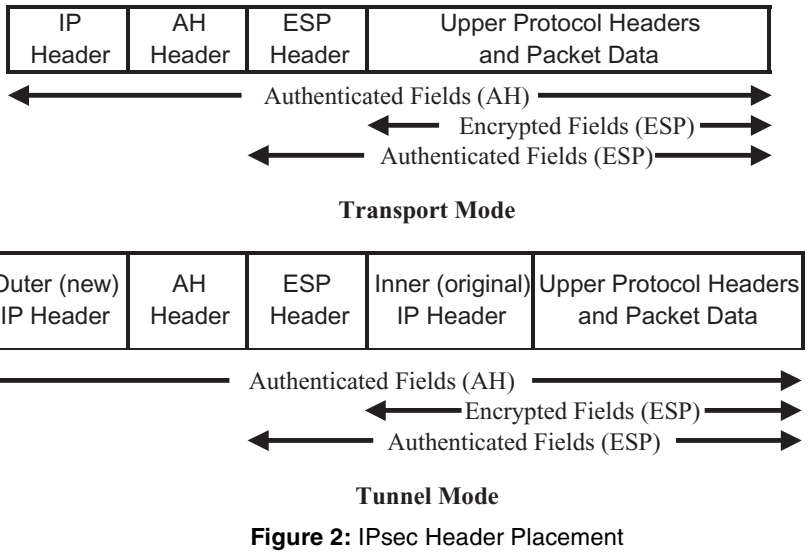


Figure 2: IPsec Header Placement

of cryptographic protection that were applied to the packet and includes other information necessary for the successful decoding of the protected packet.

If AH or ESP is added to an IP packet following the existing IP header, this is referred to as transport mode. An alternative, tunnel mode, requires the insertion of an additional IP header to the packet, but offers increased flexibility. Transport mode IPsec is limited to host-to-host communications, in which each host provides its own IPsec capabilities. With tunnel mode, a security gateway can provide IPsec protection for one or more hosts or networks located behind the gateway. If tunnel mode ESP is used, traffic analysis protection can also be provided. Tunnel mode AH and ESP protect the original IP header and the packet data; tunnel mode AH also protects portions of the new IP header. Figure 2 shows the placement of the IPsec headers within an IP packet in both transport and tunnel mode, and the portions of the packet that are protected by each header.

Since ESP can provide the same protections as AH, as well as privacy, why are two distinct security headers necessary? The answer lies in the dual realms of history and politics. A number of countries forbid the export of software that enables or incorporates encryption. The initial IPsec definition split off the undeniably exportable AH from the more problematic (in terms of exportability) ESP header. In its original form, the ESP header provided only encryption; if authentication was required, both headers had to be applied. Since an encrypted, unauthenticated packet is vulnerable to several types of modification attacks, every encrypted packet should also be authenticated, which would have required the use of both IPsec headers for each protected packet. Therefore, in the second round of IPsec development, authentication was added to the ESP Header. Initially, the new, improved ESP Header always provided encryption and, optionally, authentication. The definition of the Null ESP Encryption Algorithm allowed the ESP Header to provide authentication without encryption, thus duplicating the Authentication Header. It is true that the Authentication Header protects header fields that are not protected by the ESP Header, in particular the source and destination addresses. However, if the Internet Key Exchange (IKE) is used to negotiate the IPsec protections and the related secret keys, this serves to bind the participants' addresses to the keys, effectively authenticating these critical IP header fields. In addition, the Authentication Header processing, faced with the necessity to distinguish between mutable and non-mutable IP header fields, is more complex than that required for ESP. The Authentication Header was left intact for the original political reasons, as well as through a desire not to radically alter the IPsec protocols, which were already beginning to be implemented and used. It is possible that at some future time it may be either eliminated or converted into an optional component of IPsec.

The Cryptographic Algorithms

Since the format of Internet packets is publicly defined and well known, a packet that traverses the Internet can easily be captured and its contents can be read and/or changed. Even the checksums that are part of the Internet packet format cannot protect a packet from unauthorized alteration. These checksums were intended to guard against data corruption caused by malfunctioning devices. If the data alteration is intentional, the checksum can simply be re-computed by the attacker, and the packet will appear to be perfectly intact. How, then, can Internet packets be protected from attacks by cyber-menaces? The solution involves the use of secret codes. If the contents of a message are rendered unintelligible through the application of a secret code, then those contents are safe from prying eyes. If a message's contents are left intact, but a secret code is used to compute a value that uniquely characterizes this message, then the message's contents cannot be altered without alerting the recipient that something is amiss. Today's computer-assisted code-breakers, or cryptanalysts, are

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

capable of breaking extremely complex secret codes. Therefore, information that is impossible to guess, even with the aid of today's computing power, must form an integral part of the coded messages. This information, the secret key, must be known only to the communication's participants.

A one-way hash is an algorithm that computes a characteristic value, or hash, for a message in such a way that it is not feasible, given only the hash, to re-construct the original message. Computing this type of hash and transmitting it with the original message would be sufficient to alert a recipient to transmission errors that occurred as a result of equipment malfunction or transmission "noise." It does not protect a message from purposeful tampering, since the entity that tampers with the message can simply recompute the hash so that it matches the newly changed message. What is required is a keyed hash, one that permeates every bit of the hash with information from a secret key. This type of hash, which is also called a Message Authentication Code, or MAC, can only be computed by an entity that possesses the secret key. If that key is known only to the sender and the recipient of a message, the sender can compute the MAC before transmitting the message, and the recipient can recompute the MAC to verify that the message as received is identical to the message that was originally sent. This also serves to provide data origin authentication. The mandatory IPsec MACs, used in both AH and ESP, are HMAC-MD5 and HMAC-SHA-1.

The ESP Header encryption algorithms are all block-oriented algorithms. Each block of input text, or plaintext, is transformed, through the use of the encryption algorithm in conjunction with a secret key, into its encrypted counterpart, known as ciphertext. If each block were encrypted separately, it would make an attacker's job much easier, since the contents of some portions of an Internet packet are known. Thus, if each block could be decrypted separately, without reference to any other block, the predictable blocks could be more easily attacked. Once the key was known, every block could be decrypted. For this reason, every mandatory IPsec algorithm incorporates within its definition a feedback mechanism; the encryption of each block has, as one of its inputs, the cryptographically computed output of the previous block. The mandatory IPsec encryption algorithm is DES (the Data Encryption Standard). However, in recent years DES has become vulnerable to attack; most IPsec implementations include a stronger variant of DES, called Triple DES. Other encryption algorithms that can be used with the ESP header include Blowfish, CAST, IDEA, and RC5. The Null Encryption Algorithm does not provide encryption, enabling the use of ESP for authentication alone. The AES (Advanced Encryption Standard), NIST's newly defined DES replacement, can also be used once the AES is finalized.

The Internet Key Exchange (IKE)

Before two communicating entities can exchange secure communications, they need to agree on the nature of the security to be applied to those communications: which security headers (AH, ESP, or both) will be applied; the cryptographic algorithms to be used; the secret keys; the types of communications to be protected; the lifetime of the agreement; etc. A security association, or SA, consists of all the information that is needed to characterize and exchange protected communications. The goal of an IKE negotiation is to enable the peers to dynamically agree on the IPsec protections that will be applied to future communications. This is accomplished through a two-phase negotiation: Phase 1 establishes an ISAKMP (Internet Security Association and Key Management Protocol) SA, which is a secure channel through which the IPsec SA negotiation can take place. Phase 2 establishes the actual IPsec SA or, more precisely, a pair of one-way IPsec SAs: an inbound SA and an outbound SA.

The most common Phase 1 exchanges are Main Mode and Aggressive Mode. A Main Mode exchange consists of six messages; an Aggressive Mode exchange, three messages. At the cost of three extra messages, Main Mode provides identity protection, enabling the peers to hide their actual identities from potential attackers. This means that the peers' identities are never exchanged unencrypted in the course of the IKE negotiation. In the case in which the identity of the SA's owner differs from the negotiator's IP address, this results in hiding that identity from eavesdroppers on the Internet. Identity protection is useful even when a system is negotiating its own host-to-host SA, since an attacker can't be sure whether the encrypted identity is the sender's IP address or not. Under certain circumstances, if the peers possess and have previously exchanged Public Key Certificates, Aggressive Mode can also provide identity protection. A Phase 1 exchange has three goals:

- **Negotiate Security Parameters**: The initiator and responder must agree on the values and settings of a number of parameters that will govern the format of the last two (encrypted) messages of Phase 1 and all of the Phase 2 messages. They must also negotiate which method the peers will use to authenticate each other; the maximum lifetime of the Phase 1 SA, and how that lifetime will be measured; the method to be used to establish the shared secret that will be used to calculate the Phase 1 keying material, and the parameters used to generate the shared secret. These values collectively make up the ISAKMP SA.
- **Establish a shared secret**: Once the peers have agreed upon the method and parameters to be used to generate the Phase 1 shared secret, a Diffie-Hellman exchange is conducted to establish that shared secret, which will be used in the generation of secret keys.
- **Authenticate identities**: The peers authenticate each other's identities based on some additional out-of-band information. This information can be a pre-shared secret key, a digital signature, or encryption and decryption using each peer's public-private key pair. Peer authentication ensures that the SA is being established with a provably identifiable peer.

Once the ISAKMP SA is established, it can be used to protect multiple Phase 2 exchanges until its lifetime expires

or some other untoward event occurs (such as a rebooting of the machine, causing the current SAs to be lost). The most common Phase 2 exchanges are Quick Mode Exchanges and Informational Exchanges. An Informational Exchange uses the Phase 1 SA to protect a diagnostic or informational message. A Quick Mode Exchange negotiates an IPsec SA. A Phase 2 Quick Mode exchange has three goals:

- **Negotiate Security Parameters**: The initiator and responder must agree on the values and settings of a number of parameters that will govern the operation of the negotiated IPsec SA. They must also negotiate the maximum lifetime of the SA and how that lifetime will be measured. If perfect forward secrecy is desired, they must also communicate the parameters used to generate the shared secret that will be used to calculate the Phase 2 keying material and establish the shared secret itself.
- **Replay Prevention**: Authenticating hashes, which include freshly generated random values (nonces), are exchanged and verified to ensure that this negotiation is not merely a replay of a previous Phase 2 Negotiation.
- **Generate Keying Material**: Using the shared secret from Phase 1 (or a newly generated shared secret if perfect forward secrecy is required), the keying material for the IPsec SA is produced. The Phase 2 nonces are also used in this process, to ensure the freshness of the keying material.

In addition, two additional goals may be satisfied:

- **Provide Perfect Forward Secrecy (PFS) of Keys and/or Identities**: PFS is a guarantee that only one key has been generated from a single Diffie-Hellman exchange, and that key has no relationship to any other keys used between the peers. This ensures that discovery of the key by a third party will jeopardize only traffic that was protected with the single discovered key, but not traffic that was protected by another key negotiated by the peers. PFS of keys is provided by performing a second Diffie-Hellman exchange during Phase 2 and generating the IPsec SA's key from the new shared secret, rather than using the same shared secret that was used to generate the Phase 1 keys. PFS of identities is provided by deleting the Phase 1 SA after it has been used for a single Phase 2 Quick Mode Exchange.
- **Exchange Identities**: If the address of the negotiating peer is not sufficient to characterize the IPsec SA, the endpoint identities must be exchanged. This is necessary in the following cases:
  - The peer is negotiating an SA on behalf of another entity (for example, a gateway negotiating a tunnel-mode SA for one or more clients).
  - Multiple SAs exist between the peers, each of which is used to protect different types of traffic.

The renegotiation of an IPsec SA is triggered by the end of the SA's lifetime as measured in elapsed time or number of kilobytes of data protected by the SA. Although a new SA must be negotiated, including the complete set of SA parameters, this process is often referred to as re-keying, since it is the exposure of the secret keys that motivates the SA renegotiation. Too much elapsed time since the SA negotiation or too much data encrypted by the encryption key can provide enough time and ammunition for a variety of attacks aimed at discovering the secret key. If the ISAKMP SA through which the IPsec SA was negotiated is still alive, it can again be used to negotiate the IPsec SA's successor, and only a Phase 2 negotiation takes place. If the ISAKMP SA has also expired, a full-blown two-phase negotiation must again occur. In any IKE exchange, one peer assumes the role of initiator and the other the role of responder. However, in any subsequent IKE exchange, the roles can be reversed. This applies to a Phase 2 negotiation that follows a Phase 1, or to a Phase 1 exchange that renegotiates an about-to-expire Phase 1 SA, or any other IKE negotiation.

IKE and the Road Warrior

The original IKE standards work well for peers with fixed IP addresses. For example, a business with several branch offices, suppliers, and trading partners can use IKE to establish a variety of SAs for the different classes of secure communications, classifying the traffic into different categories according to IP address, subnet, and/or application type. IKE can also handle peers with address-independent credentials verified through the use of Public Key Certificates. For those that have neither a fixed address nor a Public Key Infrastructure (PKI), it is a different situation. In particular, it is necessary to consider the road warrior, a business employee who would like to access a network protected by a security gateway, but whose IP address is either not known or not trusted by the gateway. The case of the unknown IP address occurs when the road warrior dials into an Internet Service Provider (ISP) and then connects to the gateway over the Internet. Since the ISP-assigned address is variable, it cannot be known in advance by the gateway. An untrusted IP address can arise when the road warrior uses someone else's host, either an Internet kiosk in an airport, shopping mall or library or a host that is in a location that can be accessed both by trusted company employees and by outsiders. In this case, the IP address only suffices to authenticate the host machine. Some active user input is required to ensure that the host is being used by an authorized user.

A spin-off group was formed within the IETF to handle the road warrior problem and other, related issues involved in secure remote access. This group is called IPsra, or IP Secure Remote Access. Solutions proposed within IPsra need to follow several guidelines:

- No changes to IKE. IKE is a highly complex protocol, which will most likely be redesigned at some future time. However, that will be done by the IPsec group. Meanwhile, IPsra solutions must be capable of working within the context of currently deployed IKE implementations.
- Facilitate the transition to full-scale PKI deployment. Today's IPsra solutions will use legacy authentication methods, such as RADIUS, to generate short-term certificates or credentials. The generated certificates/credentials can be used today to authenticate road warriors that lack long-term PKI certificates. As

certificates and PKI are more widely deployed, these short-term solutions will become less critical to widespread IKE deployment.

Two IPsra solutions are currently defined: GetCert and PIC (pre-IKE Credential Provisioning Protocol). Both can issue user credentials in the form of a certificate; PIC's credentials can also take the form of a pre-shared secret key. Both rely on the fact that the authentication server or security gateway already has a certificate that is trusted by the road warrior. It only remains to leverage the legacy authentication method to issue a credential, possibly a short-lived one, which can serve to authenticate the road warrior to the gateway. Thus, the information that is exchanged for the purpose of user authentication, including the user's identity, can be secured against eavesdropping and replay attacks. The proposed solutions differ in several respects: the protocol used to transport the authentication information (HTTP vs. EAP); the mechanism used to secure the authentication information (TLS vs. a variant of IKE); which entity generates the public-private key pair (server vs. client); and the certificate enrollment mechanism (SCEP vs. new IKE payloads). One of them will be selected as the IPsra approach of choice. However, the scheme that is adopted may be revised to incorporate aspects of the other approach as well.

Policy Determination and Enforcement

IKE negotiates IPsec SAs. On the local level, these SAs control IPsec communications, both inbound and outbound, for a single host or gateway relative to its potential peers. But now other questions arise: How does a host decide upon and configure its IPsec security policies? These policies govern what types of traffic can be exchanged without IPsec protection, as well as the types of IPsec protection to be applied to traffic that requires this security. How can two peers minimize the probability that their IPsec policies are totally different, thus maximizing the possibility that an IKE negotiation between the peers will be successful, resulting in the establishment of one or more SAs? There are also issues related to the use of security gateways. How can peers that require IPsec protection, but cannot provide it themselves, locate security gateways to accomplish this task? How can a host determine whether to negotiate policy directly with its peer or with a security gateway? If the peer is protected by a gateway, how does the host securely ascertain its own gateway's location? A separate IETF group, the IPsec Policy (IPSP) Working Group, was established to address these issues. Its tricky mandate is to solve these problems in a manner that is consistent with existing policy-related terminology, theory and solutions, requiring no changes to the classic IPsec protocols or IKE, but filling in the blanks with approaches that are both generally applicable and secure. The group is currently in the process of defining a policy framework and architecture, the pieces that comprise a policy-based solution, and their interactions.

Recommended Use of IPsec by Government Agencies

- Agencies would be well advised to consider IPsec to accomplish two goals:
  - ❒ enabling road warriors and telecommuters to securely access the agency's network
  - ❒ establishing a VPN to connect multiple agency branches or offices
- IPsec lends itself very well to incremental deployment. An initial pilot could connect two offices and/or a small number of telecommuters. This could then be expanded in stages until full deployment is achieved.

The Future of IPsec

IPsec is currently used to establish VPNs and to enable road warrior communications. Many implementations incorporate proprietary elements to enable those aspects of the solution that are not yet completely standardized. It is also expected that IPsec will be used to secure other Internet protocols and technologies. At a recent conference whose sole focus was IPsec [IPsec2000, Paris Le Defense, October 2000, http://www.upperside.fr/baipsec2.html], a panel of experts was convened to answer the questions: Where are we now? What are the most pressing issues? What changes can we expect to see? It was agreed that IPsec and IKE interoperate, and that it is possible to create a working IPsec VPN using the products of any two different vendors. Three or more vendors in an operational (as opposed to experimental or research) environment are still a tricky business. The consensus was that the following features remain to be addressed:

- Transparent interoperability among the IPsec implementations of more than two vendors.
- Simple, failsafe configuration of IPsec devices.
- Secure, user-friendly VPN management and administration.
- A non-proprietary uniform approach to IPsec remote access, including authentication that crosses administrative boundaries.
- Inter-domain and intra-domain policy issues: non-proprietary policy configuration that is applicable to a wide range of devices (wireless devices, palm pilots, household appliances); a secure policy distribution mechanism; gateway discovery.
- Facilitation of IPsec-based VPNs managed by ISPs. Adding accounting, auditing and billing capabilities to IPsec devices will allow ISPs to provide different levels of service to different customers. It will also allow customers to include quality of service as a criterion for satisfactory VPN management.
- The inclusion of high-availability backup capability and resiliency in IPsec devices.
- The seamless integration of IPsec as an integral part of the networking infrastructure.

Additional issues will doubtless crop up as a result of the widespread deployment of IPsec and the increased installation of very high-speed networks.

Further Information

All of the Internet protocols, including IPsec, are defined in documents that were developed under the sponsorship of the Internet Engineering Task Force (IETF). An Internet Draft (ID) describes a protocol that is in the early stages of development. Once the technology reaches a certain level of consensus and there are multiple vendor implementations of the protocol, it is reclassified as a Request for Comments (RFC). All current Internet Drafts and RFCs can be found at the IETF's web site, http://www.ietf.org.

The charter of each working group, along with a list of the group's current Internet Drafts and RFCs, can be found at http://www.ietf.org/html.charters/wg-dir.html.

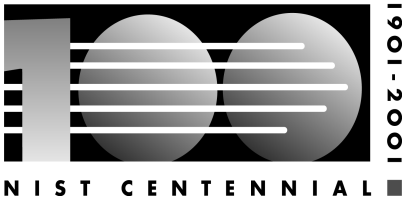
A list of each working group's current Internet Drafts, including a short description of each draft, can be found at http://www.ietf.org/1id-abstracts.html.

The e-mail discussion list archive of each working group can be found at http://www.vpnc.org.

A description of NIST's IPsec project can be found at http://csrc.nist.gov/ipsec. This includes information about NIST's IPsec reference implementation (Cerberus), NIST's IKE reference implementation (PlutoPlus), and NIST's interactive web-based interoperability tester, IPsec-WIT.

Portions of this security bulletin were taken from the upcoming book, *Demystifying the IPsec Puzzle*, by Sheila Frankel, to be published by Artech House Publishers in April 2001.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.



U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8901
Gaithersburg, MD 20899-8901