SafeNet™

VPN Solutions from IRE

Information Resource Engineering, Inc.
8029 Corporate Drive
Baltimore, MD 21236
Tel: 410.931.7500
Fax: 410.931.7524
www.ire.com

IPSec White Paper

I. Introduction

What is IPSec?

The acronym IPSec, a short form of the longer term - "Internet Protocol Security," is an evolving standard for security at the network or packet layer of network communication. In essence, IPSec is a set of protocols being developed by the Internet Engineering Task Force (IETF) that will be used to help implement Virtual Private Networks (VPNs) that operate over the Internet.

IPSec ensures the confidentiality, integrity, and authenticity of data communications across a public network. It provides a necessary component for a standards-based, flexible, network-wide security policy. IPSec is important because it provides a flexible, practical, and sound basis for extensive business use of VPNs that use the Internet. It is the security standard that is paving the way to full fruition of the Information Age in the 21st century.

Why do Standards Matter?

IPSec, FIPS 140-1, and other standards represent the sum total of years of expert analysis of the best methods for implementing Internet VPN security. Products that meet the IPSec standard offer the strongest security available for an Internet VPN. There is a special assurance that comes from having independent experts validate a security standard.

A buyer who chooses a standards-compliant product meets their fiduciary responsibility to their company. The buyer is assured that due care has been taken and that a commercially reasonable technology was chosen. The buyer and their organization have a firm, legally responsible foundation for operating a VPN.

Finally, standards compliance creates the basis for interoperability among different vendors. With applications such as network solutions from router companies, specialized VPN products, and other new software, interoperability has become a critical issue. Interoperability is feasible with IPSec. The International Computer Security Association (ICSA), an independent organization, tests and certifies VPN security products for compliance with IPSec.

Purpose of This Paper

This paper gives a general description of IPSec and explains why the global network security industry needs it. There is also an explanation of the forces driving IPSec and a projection of the global impact the new standard will make in the years ahead.

II. IRE'S Position on IPSec

IPSec's Features and Benefits Summarized

At IRE, IPSec is viewed as an integral part of the company's SafeNet line of products. SafeNet IPSec products allow users to enjoy the following benefits:

> ***Data Security*** *– IPSec provides confidentiality, integrity, and data authenticity through encryption and authentication technologies. Data can be sent across the Internet without fear of observation, modification, or spoofing. Applications such as VPNs are enabled.*
> *Key Benefit: Strong security*
>
> ***Integrated Solution*** *– Security can often be implemented without the necessity of elaborate and costly upgrades to every personal computer. VPN products can be "dropped in" to the network. As a result, IPSec reduces impact on existing network infrastructure.*
> *Key Benefit: No network disruption*
>
> ***Certificate Support*** *– All SafeNet products that are public-key-capable can be automatically authenticated using digital certificates. This feature can be scaled to large networks that serve thousands of connections.*
> *Key Benefit: Scaleability*
>
> ***IKE*** *– This protocol, an updated version of ISAKMP/Oakley, enables automatic negotiation of security associations. It also enables secure communications without the performance limitation of centralized key distribution. IKE is, of course, an integral part of IPSec.*
> *Key Benefit: Standards based key management*
>
> ***Security Policy*** *– IRE's SafeNet/Security Center enables communications among SafeNet devices to be handled with maximum flexibility. Selected traffic can be secured in different ways to increase performance and efficiency. Developing a sound security policy is as important as dealing with the equipment used in a VPN.*
> *Key Benefit: Centralized policy management*
>
> ***Current Standards*** *– IPSec is the Internet Engineering Task Force's (IETF) standard. IPSec creates the foundation for multivendor interoperability among network devices, PCs, and other computing systems.*
> *Key Benefit: The basis for interoperability*

As of June 1998, IRE's SafeNet/Soft-PK was one of only seven ICSA-certified, IPSec-interoperable products. In addition, SafeNet/Soft-PK is one of only two client products that have been IPSec certified by ICSA. IRE's SafeNet version 3.0 network security products are IPSec compliant, and company management is committed to the further development and deployment of the IPSec standard.

III. Business Considerations

Networks and Security - The Limits of IP

The Internet Protocol (IP) is unequaled as the foundation of large networks. It enables networks ranging in size from small Local Area Networks (LANs) to large corporate Wide Area Networks (WANs) and beyond to communicate over the Internet. Simply stated, IP is the leading medium for network communications between computers. It is the most capable protocol in use today for negotiating communications between systems that have varying capabilities.

However, IP-based networks are not perfect. The structure of IP itself makes them vulnerable to various forms of attack. IP was designed to be flexible, so traffic auditing, access control, and many other security measures do not work well, or at all, with it. As a result, IP-based data is vulnerable to hackers' tampering and eavesdropping.

IP's strength is that it has small, manageable packets of electronic information that can be routed quickly and easily. These "chunks" of information create breaks in the data stream that allow them to be transmitted efficiently through the network. However, the way IP routes these packets causes large IP networks to be vulnerable to a number of security attacks.

Spoofing is an attack that involves one machine on a network masquerading as another. Sniffing is an attack that involves an eavesdropper listening in on communications between two other parties. Session hijacking is an attack in which a conniving hacker uses both spoofing and sniffing to take over an established communications session and pretends to be one of the parties involved. In each instance, an unauthorized individual has gained access to private, or even critical, company information.

These security risks make secure communications over large IP networks, such as the Internet, intimidating. To remedy the problem, an international group organized under the Internet Engineering Task Force (IETF) created the IPSec protocol suite, a set of IP protocols that provide security services at the network level. IPSec is based on state-of-the-art crytographic technology that makes secure data authentication and privacy on large networks, including the Internet, a reality.

Forces Behind the use of IPSec and the Internet

The Internet is rapidly changing the way business is conducted. While the speed of communications is increasing, the costs are decreasing. This new potential for increased productivity and cost savings offers large rewards to anyone who takes advantage of it. When used with IPSec security, the Internet enables extranets, intranets, and remote access for a much lower cost.

With extranets, companies create links with their suppliers and business partners to share information and gain productivity and communication efficiencies. Before the Internet, this link had to be established with dedicated leased lines or slow dial-up lines. The Internet enables companies to maintain instant, real time, high-speed communications.

Today, many large companies maintain cumbersome and costly WANs. While the cost of dedicated lines has been greatly reduced, the Internet offers an even greater cost savings. As a result, intranets are an irresistible alternative for companies that want to maximize efficiency and cost savings.

Service	Current vs.	VPN	Savings	Percent
Dial-up	$300/10 Hrs	$40/mo.	$260/mo.	87%
T1	$8,690/mo.	$2400/mo.	$6290/mo.	72%
10 Mbit/s	$35,312/mo.	$15,000/mo.	$20,312/mo.	58%
T3	$68,500/mo.	$32,000/mo.	$46,500/mo.	53%

Figure 1. Cost comparison of dedicated lines vs. Internet VPN's

The Internet provides a low-cost alternative for remote users who want to access the corporate network. Rather than maintain large modem banks and large telephone bills, a remote user can access the home office network via the Internet. With just a local telephone call to the Internet Service Provider (ISP), a user can access the corporate network.

Extranets, Intranets and other Internet-based applications are changing the way businesses communicate, and the Internet provides the public infrastructure necessary to make it possible. Unfortunately, the Internet is missing some key components, such as security, quality of service, and manageability. IPSec is one of the key technologies that is changing all that by making security a fundamental component and foundation of network service.

IV. A Search for the Solution

Understanding Layers

A solution to the Internet security problem exists. The key to understanding this solution lies in learning about the network layer in IP networks.

To isolate problems that occur when networks are being constructed, it is useful to imagine a network as a series of layers. Each layer solves problems that are unique to that layer. Stated simply, an IP network has three layers: the physical layer, the IP network layer, and the application layer. Each layer provides services to the layer above it.

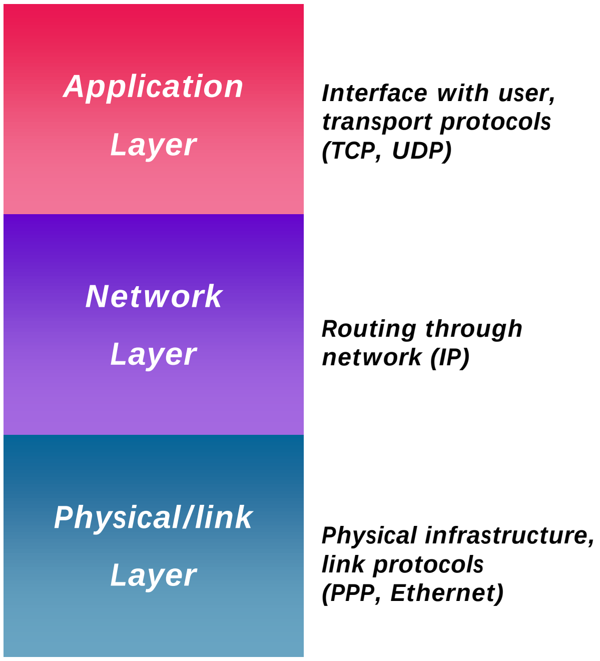
Application Layer
Interface with user, transport protocols (TCP, UDP)
Network Layer
Routing through network (IP)
Physical/link Layer
Physical infrastructure, link protocols (PPP, Ethernet)

Figure 2. Network layers (simplified)

The physical layer (the lowest level) consists of the actual equipment: electrical cables, network cards, and/or radio links where information travels. In addition, the physical layer contains simple data-carrying protocols that provide an interface for higher level protocols. In an IP network, different parts of the network use different types of physical media – Ethernet in some places, point-to-point lines in others.

Above the physical layer, the network layer (the IP layer in IP networks and the level where IPSec operates) sends information from network node to network node across the whole network. The network layer uses the lower level protocols to move the data, and it uses its own routing logic to find the best subnets through which to send the data.

Above the network layer are higher level protocols that set up links between nodes for different types of communications. Also above the network layer is the application layer where applications run. Applications use the capabilities of the network layer to determine how to move data from network node to network node. The network layer in turn uses the physical layer to move data from one computer's network card to the next.

The most important thing to remember about IP networks is that the network layer is entirely uniform. It is the only layer that is uniform. As a result, any communication going through an IP network (e.g., the Internet) has to use the IP protocol. In other network layers, different protocols operate for different reasons (depending on the network's architecture and types of communication). However, eventually all communications have to go through the network layer, and for all IP networks there is only one protocol in that layer - IP. Consequently, if the IP (network) layer is secure, the network is secure.

Using IPSec to Secure the IP Layer

The international group organized under the Internet Engineering Task Force (IETF) has developed a way to secure the IP layer. That method is called the IP Security (IPSec) protocol suite. The IPSec protocol suite has a foundation of powerful new encryption technologies. The suite adds security services to the IP layer in a way that is compatible with both the existing IPv4 IP standard and the emerging IPv6 standard.

Essentially, if the IPSec suite is used where IP is normally used (in the network layer), communications are secured for all applications and for all users more transparently than would be the case if any other approach was employed. With IPSec, a secure VPN can be built that is as secure as a private network. The incredible part is that the VPN resides on an unsecured, public network (e.g., the Internet). With IPSec, a secure VPN can be created as needed, on demand, and with any other device that is using the IPSec standard.

Because IPSec works with both existing and future IP standards, regular IP networks can still be used to carry data. The sending device has to be IPSec-compliant, and the receiving device has to be IPSec-compliant, but the rest of the network between the sender and recipient does not have to be IPSec compliant.

The primary strength of the IPSec group's approach is that their security works at a low network level. As a result, IP is transparent to the average user, and IPSec-based security services are also not seen, functioning behind the scenes to ensure that all network communications are secure.

IPSec's power and flexibility promise to make it the international standard. IPSec meets a broad range of security needs and allows different networks around the world to interconnect and to communicate securely. In addition, IPSec offers almost infinite scaleability with transparent and reliable service, no matter how demanding a company's security needs.

V. Technical Considerations

How IPSec Works

IPSec implements network layer encryption and authentication, embedding end-to-end security within the network architecture. The advantage to this is that individual applications do not need to be modified to take advantage of strong security. All packets routed through the network are automatically secured.

IPSec supports two encryption modes: transport and tunnel. Transport mode encrypts only the data portion (payload) of each packet and leaves the packet header untouched. The more secure tunnel mode encrypts both the payload and the header. Tunnel mode is often used in networks with unregistered IP addresses. The unregistered address can be "tunneled" from one gateway encryption device to another by hiding the unregistered addresses in the tunneled packet.

For IPSec to work, both the sending and receiving devices must have access to each other's public keys. This is accomplished through a Certificate Authority (CA) that allows the receiver of an encrypted message to obtain a public key and authenticate the sender using a digital certificate issued by the CA.

IPSec standards define several new packet formats, such as an Authentication Header (AH) to provide data integrity and the Encapsulating Security Payload (ESP) to provide confidentiality. IPSec parameters between devices are negotiated with the Internet Key Exchange (IKE) protocol, formerly referred to as the Internet Security Association Key Management Protocol (ISAKMP/Oakley). IKE can use digital certificates, such as those provided by various vendors, for device authentication. The fundamental building blocks of IPSec, the ESP and the AH, use cryptographic techniques to ensure data confidentiality and digital signatures that authenticate the data's source.

The IP datagram, or IP packet, is the fundamental unit of communications in IP networks. IPSec handles encryption at the packet level, and the protocol it uses is the ESP. ESP supports any type of symmetric encryption. The default standard built into ESP that assures basic interoperability is 56-bit DES. ESP also supports message authentication as can the AH. The two have been designed with some overlap.

The ESP

The ESP contains six parts as follows. The first two parts are not encrypted, but they are authenticated. Those parts are:

- *The Security Parameter Index (SPI) is an arbitrary 32-bit number that tells the device receiving the packet what group of security protocols the sender is using for communication. Those protocols include the particular algorithms and keys, and how long those keys are valid.*

- *The Sequence Number is a counter that is incremented by 1 each time a packet is sent to the same address and uses the same SPI. The sequence number indicates which packet is which, and how many packets have been sent with the same group of parameters. The sequence number also protects against replay attacks. Replay attacks involve an attacker who copies a packet and sends it out of sequence to confuse communicating devices.*

The remaining four parts of the ESP are all encrypted during transmission across the network.
Those parts are:

- Payload Data is the actual data that is carried by the packet.

- The Padding, from 0 to 255 bytes of data, allows certain types of encryption algorithms to require the data to be a multiple of a certain number of bytes. The padding also ensures that the text of a message terminates on a four-byte boundary (an architectural requirement within IP).

- The Pad Length field specifies how much of the payload is padding rather than data.

- The Next Header field, like a normal IP Next Header field, identifies the type of data carried and the protocol.

Note that the ESP is added after a standard IP header. Because the packet has a standard IP header, the network can route it with standard IP devices. As a result, IPSec is backwards-compatible with IP routers and other equipment even if that equipment isn't designed to use IPSec.

ESP can support any number of encryption protocols. It's up to the user to decide which ones to use. Different protocols can be used for every person a user communicates with. However, IPSec specifies a basic DES-Cipher Block Chaining mode (CBC) cipher as the default to ensure minimal interoperability among IPSec networks. ESP's encryption capability is designed for symmetric encryption algorithms. IPSec employs asymmetric algorithms for such specialized purposes as negotiating keys for symmetric encryption.

Tunneling with ESP

Tunneling takes an original IP packet header and encapsulates it within the ESP. Then, it adds a new IP header containing the address of a gateway device to the packet.
Tunneling allows a user to send illegal IP addresses through a public network (like the Internet) that otherwise wouldn't accept them.

Tunneling with ESP offers the advantage of hiding original source and destination addresses from users on the public network. Hiding these addresses reduces the power of traffic analysis attacks. A traffic analysis attack employs network monitoring techniques to determine how much data and what type of data is being communicated between two users.

The ESP Authentication Field

The ESP authentication field contains an Integrity Check Value (ICV), what amounts to a digital signature that is computed over the remaining part of the ESP. It varies in length depending on the authentication algorithm used. It may also be omitted entirely if authentication is not needed for the ESP. Authentication is calculated on the ESP packet once encryption is complete. The current IPSec standard requires HMAC (a symmetric signature scheme) with hashes SHA1 and MD5 as algorithms for IPSec-compliant hardware and software in the ESP packet's authentication field.

The ICV supports symmetric type authentication. The sending device encrypts a hash of the data payload and attaches it as the authentication field. The receiving device confirms that nothing has been tampered with and that the payload did come from the correct source device.

The Authentication Header (AH)

The IPSec suite's second protocol, the AH, provides authentication services. The AH may be applied alone, together with the ESP, or in a nested fashion when tunnel mode is used. Authentication provided by the AH differs from what is provided in the ESP in that the ESP's authentication capabilities do not protect the IP header that lies in front of the ESP, although an encapsulated IP header in tunneling mode is protected. The AH services protect this external IP header, along with the entire contents of the ESP packet.

The AH does not protect all of the fields in the external IP header because some change in transit, and the sender cannot predict how they might change. The AH protects everything that does not change in transit. In the packet, the AH is located after the IP header but before the ESP (if present) or other higher level protocol, such as TCP.

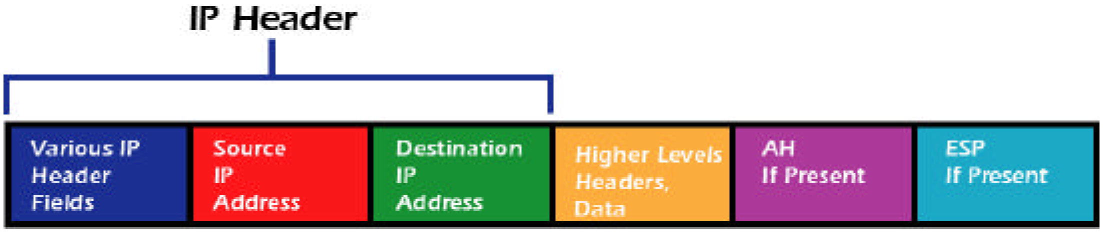

Figure 3. The Basic IP Packet

Like the ESP, the AH can implement tunneling mode. Also, like the ESP, IPSec requires specific algorithms to be available for the AH to be implemented. Under the standard, all IPSec implementations must support at least HMAC-MD5 and HMAC-SHA1 (the HMAC symmetric authentication scheme supported by MD5 or SHA1 hashes) for the AH.

VI. Key Management - The Rest of the IPSec Story

Infrastructure – the Key

The AH and ESP protocols are the building blocks of IPSec. The encryption services provided by the AH and ESP are powerful tools for keeping data secret, for verifying its origin, and for protecting it from undetected tampering. But these tools will not work unless there's a carefully designed infrastructure to work with them. VPN security succeeds or fails depending on the reliability and scaleability of this infrastructure.

Secure communication with authentication and encryption requires negotiation, an exchange of keys, and a capability to keep track of the keys. IPSec provides the capability to do all three of these things. The first item IPSec's designers dealt with was how to keep track of the details and which keys and algorithms to use. The solution was to bundle everything together in a Security Association (SA). The SA groups together everything needed for two parties to communicate securely.

Under IPSec, the SA specifies the following:

- The mode of authentication algorithm used in the AH and the keys to that authentication algorithm
- The ESP encryption algorithm mode and the keys to that encryption algorithm
- The presence and size of (or absence of) any cryptographic synchronization to be used in that encryption algorithm
- The key lifetimes

The SA is the secure channel through the public network. The SA also lets the system construct classes of security channels. If more secure safeguards are needed, more care can be taken, and the rules of the SA can be changed to specify stronger measures.

IKE

Internet Key Exchange or IKE is a protocol that is the IETF's choice for protocol negotiation and key exchange through the Internet. IKE integrates ISAKMP with a subset of the Oakley key exchange scheme. IKE enables an agreement to be negotiated on which protocols, algorithms, and keys should be used. It ensures secure authentication services from the beginning of the exchange. It manages keys securely after they've been agreed upon, and it exchanges those keys safely.

Key exchange is closely related to SA management. When an SA is created, there is a need to exchange keys. So, IKE wraps them together, and delivers them as an integrated package.

IPSec specifies that compliant systems support manual keying as well. As a result, manual key exchange is possible in certain situations. However, for most large enterprises manual key exchange is impractical. So IKE is expected to continue to negotiate SAs and exchange keys automatically through public networks.

IKE functions in two phases. Phase one involves two IKE peers establishing a secure channel for performing phase two. Phase two involves the two peers negotiating general purpose SAs. An IKE peer is an IPSec-compliant node capable of establishing IKE channels and negotiating SAs.

IKE provides three modes for the exchange of keying information and set up of IKE SAs. Two modes are for IKE phase one exchanges, and one mode is for phase two exchanges. Main mode establishes a phase one IKE exchange through a secure channel. Aggressive mode is another way of accomplishing a phase one exchange, but it's easier and a little faster than main mode. Quick mode accomplishes a phase two exchange by negotiating an SA for general communications.

Main Mode

Main mode provides a way to establish the first phase of IKE SA, which is then used to negotiate future communications. The first step, securing an IKE SA, occurs in three two-way exchanges between the sender and the receiver. In the first exchange, the sender and receiver agree on basic algorithms and hashes. In the second exchange, public keys are sent for a Diffie-Hellman exchange. Nonces (random numbers each party must sign and return to prove their identities) are then exchanged. In the third exchange, identities are verified, and each party is assured that the exchange has been completed.

Aggressive Mode

Aggressive mode provides the same services as main mode. It establishes the phase one SA, and operates in much the same manner as main mode except that it is completed in two exchanges instead of three.

In aggressive mode, the sender generates a Diffie-Hellman pair at the beginning of the exchange, doing as much as is reasonable with the first packet (proposing an SA, passing the Diffie-Hellman public value, sending a nonce to the other party to sign, etc.). The recipient then sends back everything needed to complete the exchange, essentially a consolidation of all three response steps that occur in main mode.
The result is that aggressive mode accomplishes as much as main mode, with one exception. Aggressive mode does not provide identity protection for communicating parties. In other words, in aggressive mode, sender and recipient exchange identification information before they establish a secure channel where the information is encrypted. As a result, a hacker monitoring an aggressive mode exchange can determine who has just formed a new SA. Aggressive mode's value, though, is speed.

Quick Mode

After two parties have established a secure channel using either aggressive mode or main mode, they can use quick mode. Quick mode has two purposes, to negotiate general IPSec security services and to generate newly keyed material. Quick mode is much simpler than both main and aggressive modes. Quick mode packets are always encrypted under the secure channel (or IKE SA established in phase one) and start with a hash payload that is used to authenticate the rest of the packet. Quick mode determines which parts of the packet are included in the hash.

Key refreshing can be done in two different ways. If perfect forward secrecy is not needed, quick mode can refresh the keying material already generated in main or aggressive mode with additional hashing. Sender and recipient can then exchange nonces through the secure channel, and use them to hash the existing keys. If perfect forward secrecy is desired, an additional Diffie-Hellman exchange is requested through the existing SA, and the keys can be changed that way. Basic quick mode is a three-packet exchange.

Perfect Forward Secrecy

A user can reduce the risk of hackers ever deciphering a message through the use of larger and larger keys. But, the larger the key, the slower encryption will be accomplished, and network performance will also decrease. Use of fairly large keys and frequent changes of them is a good compromise. However, coming up with ways to generate these new keys is the challenge.

A method to generate a new key that does not depend on the current key is needed. Then, if a hacker knows the current key, he or she will know only a small amount of information. The hacker would have to find out an entirely unrelated key to get to the next part. This concept is called "perfect forward secrecy." The way that perfect forward secrecy is done through IKE is called "Diffie-Hellman."

A Diffie-Hellman exchange allows two users who wish to communicate with each other to randomly generate keys that are similar to a public/private key pair. Each user sends a public key value to the other. Each then combines the public key they receive with the private key they just generated using the Diffie-Hellman combination algorithm. The resulting value is the same on both sides. No other users in the world can come up with the same key from the two public keys that traveled across the Internet, because the final key depends on each user's private key, which is secret.

The derived Diffie-Hellman key can be used either as a session key for subsequent exchanges or to encrypt another randomly generated key. Diffie-Hellman allows new shared keys, that are independent of older keys, to be generated for symmetric encryption, thus providing perfect forward secrecy. Because symmetric encryption operates quickly, Diffie-Hellman is valuable to network communications.

VII. Certificate Authority – The Final Piece

The final component of the IPSEC-compliant secure VPN is the Certificate Authority, or CA. While not an integral part of IPSec, the CA is, nevertheless, a critical element in the public key infrastructure. A CA is a trusted third party, an entity whose identity has already been established and proven. The CA's role is to vouch for the identities of people with whom a user is trying to communicate.

The CA is a public figure of sorts, something like a notary public, who is known well enough to trust, and who can vouch for other people. When verifying online communications, the CA software issues certificates tying the following three things together:

- an individual's identity (e.g., name and address)
- the public key the individual uses to "sign" online communications
- the CA's public key (used to sign and authenticate communications)

The CA defends against the "middle-man" hacker who attempts to work his way into key exchanges. Whenever an exchange is initiated, users sign their communications packages with their digital signatures. Those signatures are checked against the ones on record with the CA. They have to match. Users then check the CA certificate's signature with the CA's signature. They have to match too. Otherwise, a SA will not be established and no communications will take place.

VIII. Conclusion

IPSec as a Universal Standard

From the beginning, the IETF's IPSec Work Group has attempted to provide a new version of IP. Though technology continues to evolve, the group's initial objectives have been met. The IETF's efforts may have changed the capabilities of the Internet forever. IPSec has made the Internet capable of transporting secure communications, ushering in the era of secure virtual private networks and low-cost communications.

Perhaps the most important aspect of the IPSec protocol suite is the fact that it is an Internet standard, so vendors and service providers can both specialize and cooperate to provide all of the IPSec equipment and services needed. With an IPSec-secure VPN, a secure and inexpensive network is available. A laptop with an IPSec-compliant program can connect securely and transparently to a corporate network through a dial-up ISP from anywhere in the world.

Complete Interoperability – The Final Frontier

While it is safe to say that the VPN world is committed to IPSec, it is accurate to say that IPSec is not completely ready for the VPN world. To put it another way, vendors in the VPN world are not yet completely *standardized and synchronized in their use of IPSec. Total interoperability among any and all users of network security products is not yet a reality. Some compatibility issues still need to be addressed before all network security vendors are in synch.*

While some IPSec incompatibilities will not be difficult to fix, others will take more time. The reality is that creation of a completely interoperable VPN standard is still some distance away, and today's IPSec standard does not solve all VPN security issues. Some experts believe this lack of true and complete interoperability may slow widespread VPN deployment.

We disagree.

SafeNet IPSec Plus

IRE is committed to providing IPSec compliant solutions that can be deployed today. We are in the unique position of being able to apply our fifteen years of experience in deploying large, secure networks to the emerging IETF IPSec standards. The result is SafeNet IPSec Plus, a solution that provides all the advantages of IPSec and addresses all its current weaknesses. A solution that allows our customers to deploy an Internet VPN today, with the comfort of knowing enhancements will come as security standards and needs evolve.