

Experimental Review of IPSec Features to Enhance IP Security

By Shilpa Nandamuri

East Carolina University

Introduction

In the interconnected world of today, sensitive information is constantly being exchanged over the Internet or from enormous places where the security of information can be compromised. For the last few decades, most of the information has been stored digitally on huge storage devices. In addition, these storage devices are placed on IP networks. Once storage devices are placed in an IP network, they are vulnerable to both internal and external network attacks. According to Intel “Equally troubling are recent estimates that now the number of attacks from within networks are as high as eighty percent of all successful attacks on corporate networks”. Malicious attacks, such as Viruses, Trojan horses and Spyware cause loss of sensitive data and require use of valuable resources to resolve. Data theft of especially confidential data has become a major concern because of the way the Internet works today. These attacks can come from employees, staff or anyone who has access to the network. The open design of network has opened new avenues of data thefts and attacks. Today, three main concerns of communication or exchange of information are data integrity, authenticity and confidentiality.

In today’s world, changes have been made on the way the Internet operates. The technique used for transmitting data over the Internet is called Internet Protocol. Internet Protocol can be used to transfer any type of data from one part of the world to another. IP is a set of standards for ensuring that communications delivered over the networks are private as well as secure. According to Shoniregun, C. A. IP routes packets to their destination host even though it provides unreliable and connectionless datagram delivery service. The reasons for the later problem are based on the facts that there is no security associated with the IP packets. The packet data can be corrupted during the transit. In order to overcome this problem, it is important to make sure that the data sent over the network must be transmitted only if the data transfer is

authenticated and the environment is tamperproof and confidential to ensure the security of sensitive information. Security of the packet data is needed to protect the information assets, to ensure the data integrity and unauthorized access, to comply with the government regulations and to improve the management of information. The network traffic over the devices connected in the network must be secured from malicious attacks from inside and outside the network to protect the sensitive information.

Network security measures such as firewalls, token authentication and secure routers are used to manage the threats but these devices can be used to secure the data only from external threats. But most of the times the attacks come from local area networks and from internal devices of the network i.e. from inside the system rather than from outside the system. Organizations lose a great deal of sensitive data from the internal attacks where firewalls offer no protection. To overcome these problems Internet Protocol Security (IPSec) has been developed by the Internet Engineering Task Force (IETF) for the Internet Protocol. IPSec supports network-level data integrity, authentication and encryption and provides security within the network unlike firewalls and secure routers.

What we need is global security for sensitive information. In addition, network managers need to implement security for protecting communication among local area network computers, clients and servers, extranets, and mainly to computers that are connected over the Internet to secure sensitive information. How can IPSec provide secure communications regardless of known IP vulnerabilities? What provides security to the network traffic and in addition an end-to-end security at the packet processing layer of the network?

What is IPSec?

An effective solution for many of these questions is a technology developed by the Internet Engineering Task Force (IETF) for secure transmission of IP packets over physical networks is called IPSec. The first IPSec protocols were defined in 1995 (RFCs 1825–1829). Later, in 1998, these RFCs were deprecated by RFCs 2401–2412 (Rosen). IPSec is a collection of protocols to assist safe and secure communications over the network. IPSec is open and a standard that provides a common means of authentication, integrity and IP encryption. One of the principal strengths of IPSec is that encrypted packets can be routed and switched on any network that supports IP traffic. No upgrade to the network elements is necessary. (**IP Security: Building Block for the Trusted Virtual Network**).

IPSec provides three main facilities: an authentication-only function, referred to as *Authentication Header* (AH), a combined authentication/ encryption function called *Encapsulating Security Payload* (ESP), and a key exchange function (William Stallings). The three protocols together ensure that authorized parties may exchange private IP packets securely over a public network. IPSec can be used to securely “tunnel” packets to routers or firewalls over a WAN, or to securely “transport” packets end-to- end between desktops and servers. (Jerry Ryan) The encrypted packets can be routed and switched on any network that supports IP traffic without any upgrade to the network elements. This enables the communication of packets over the LAN, extranet and Internet easily and transparently.

How it works

IPSec-based security starts with the formation of a security association (SA) between the parties interested to communicate. A security association (SA) is an agreement between two

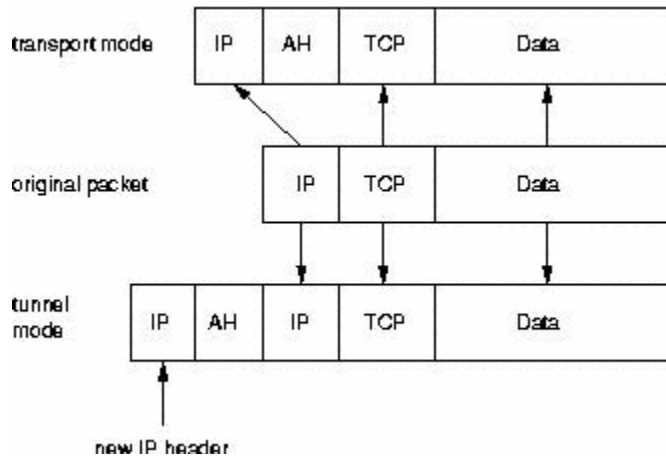
parties or entities that will say how they will support secure communication between each other. The great thing about IPSec is that it not only supports multiple protocols, but that it also allows for various encryption algorithms and different hash types. In order for a secure communication to be established between two entities the encryption method and the hash type must be negotiated. Without this prior negotiation we might have one end using a different encryption algorithm than the entity on the other side of the communication channel. This would result in a breakdown of the communication because the data would not be decrypted correctly. Therefore, all the details must be decided before the information is sent across the medium.

Once the SA has been agreed upon it is placed in a security association database (SAD). This is necessary because each connection might be using different rules and different encryption algorithms. Remember IPSec supports multiple encryption algorithms, so we must keep track of which connection is using which encryption algorithm and hash types.

There are two main modes which IPSec uses in order to operate. The first mode is transport mode and the second is tunnel mode. Transport mode is used when an SA is made between two hosts that usually reside in the same network. It's usually referred to as host-to-host. In this case only the packet's payload is encrypted. This mode can also be used when you don't care whether the IP addresses of the communicating parties are made public or not. Also, transport mode lacks the ability to participate in gateway-to-gateway communications.

Tunnel mode is used when an SA is made between two IPSec gateways. This is usually what is used in VPNs because in tunnel mode not only is the payload encrypted but the entire original packet. This hides the IP addresses of the source and destination of the IP packet. Another advantage of tunnel mode is that it can occur not only with gateway-to-gateway, but

also between host-to-host and host-to-gateway. The image below shows the difference between tunnel mode and transport mode. As you can see in transport mode the original IP packet is used whereas in the tunnel mode a new IP header is planted on the packet.



When packets flow across a WAN, an outsider might deduce something by viewing source and destination addresses contained in the IP header. For example, company A is exchanging high-volume traffic with company B; a thief might use this knowledge to predict a pending joint venture and illegally profit from use of insider information. Addresses can also expose details of the corporate network's internal topology, facilitating denial-of service (DOS) attacks whereby a hacker floods an enterprise server with requests that block access by legitimate users. To keep addresses private, IPsec can be used in tunnel mode. The entire private IP packet, header and payload is hidden inside a public IP packet "envelope". Tunnel mode is typically employed by security gateways: edge devices like routers and firewalls that relay packets on another system's behalf.

But, inside a LAN, the threat of traffic analysis and denial-of-service attacks is minimal. To reduce processing overhead and packet length without sacrificing security, the original header can be used on packets exchanged between hosts. In transport mode, ESP hides only the private packet's payload. Transport mode IPSec can be used to efficiently protect data end-to-end between clients and servers, peers in a workgroup, and extranet partners. Transport and tunnel mode can be used in conjunction to secure the total enterprise network by applying each where appropriate: tunnel mode to WAN security, transport mode to LAN security. (Jerry Ryan)

Internet Key Exchange (IKE)

The protocol that is the authenticator and negotiator of IPSec is the Internet key exchange (IKE) protocol. It is what verifies whether your system has the right to start an encrypted communication with the device in question. It then negotiates which encryption algorithm will be used during the connection. There are two phases in the IKE transaction that support the creation of an SA between two parties. They are referred to as phase 1 and phase 2. Phase 1 begins when an initiator wants to begin a session with a VPN gateway device. In this phase two things occur. One is the authentication of the remote client and the other is to exchange public key information that will be used for the next phase. Various ways exist that can be used to verify authentication. Some of which are pre-shared keys which is a key that has been pre-configured between the communicating devices. This is a very simple way of authentication however it does have many drawbacks because if the key is broken you must reconfigure all the devices that used that key. The second method of authentication that can be used is digital signatures also called digital certificates. In this case a Certificate Authority (CA) remotely manages and administers each certificate. The CA is the center piece of the Public Key Infrastructure (PKI) encryption method. In this concept the PKI is publicly available to anyone who wants it. They are typically available

in certificates. Phase 2 of the IKE transaction deals with the negotiation of the parameters of IPSec SAs. Once Phase 2 is complete IPSec SA is formed and the VPN connection is made. During the Phase 2 exchanges all the packets are encrypted using whatever protocols were negotiated during Phase 1 and any other protection that might be used are hashes that confirm the origin of the packets. IPSec uses IKE to create security associations, which are sets of values that define the security of IPSec-protected connections. IKE phase 1 creates an IKE SA; IKE phase 2 creates an IPSec SA through a channel protected by the IKE SA.

IKE phase 1 works in two modes main mode and aggressive mode. Main mode negotiates the establishment of the IKE SA through three pairs of messages, while aggressive mode uses only three messages. Although aggressive mode is faster, it is also less flexible and secure. The endpoints cannot negotiate Diffie-Hellman parameters, and identity information may not be hidden in some cases. The IKE SA created during phase 1 is bidirectional, meaning that it provides protection for both sides of the communication.

IKE phase 2 has only one mode that is quick mode. Quick mode uses three messages to establish the IPSec SA. Quick mode communications are encrypted by the method specified in the IKE SA created by phase 1. The IPSec SA created by phase 2 is unidirectional; therefore, a pair of SAs need to be created for each AH or ESP connection.

There are many authenticated key exchange protocols, which impose different requirements (pre-shared secret, public key infrastructure ...) and provide different properties (direct authentication, perfect forward secrecy ...).

Within the scope of the key exchange protocols developed for securing exchanges using IP, an additional distinction is necessary between the connection-oriented protocols and the

connectionless ones. In the first case, an authenticated key establishment protocol is used "off-band", before the communication. The resulting key is then used to secure the IP traffic. The disadvantage of this approach is that it requires the establishment and the management of a pseudo session layer under IP, whereas IP is a connectionless protocol. In the second case, a stateless authenticated key establishment protocol is used, which does not require any connection. This is feasible through an "in-band" protocol, where the key that is used to encrypt the packet is transmitted with it, encrypted with the recipient's public key for example. The disadvantage of this system is that it adds data to each transmitted packet (Ghislaine Labouret).

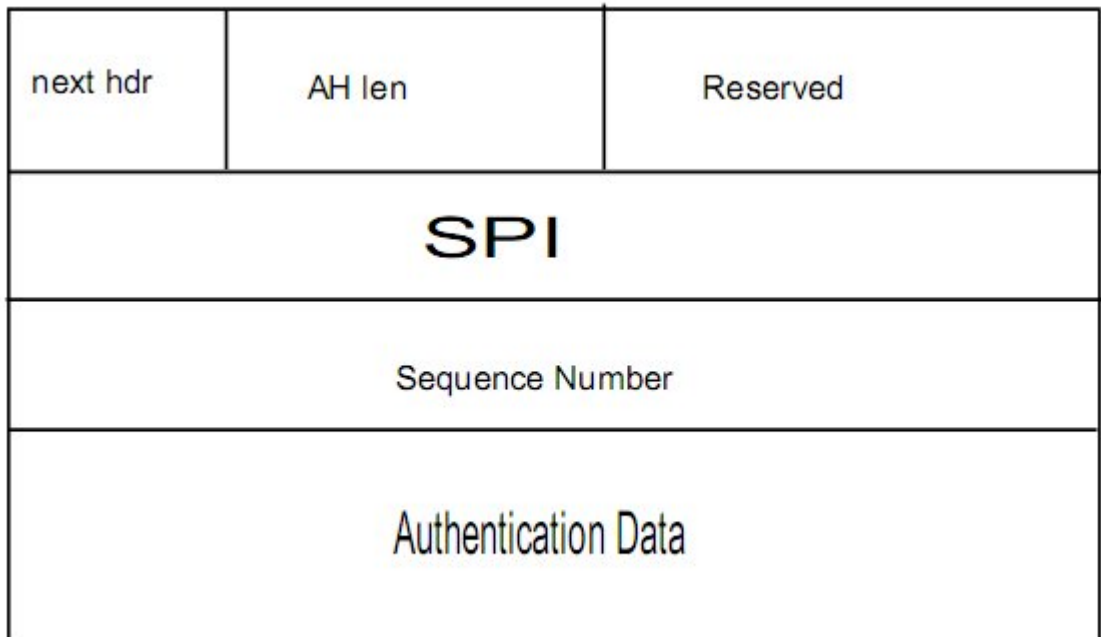
Authentication Header (AH)

Authentication Header in IPSec provides integrity for packet headers and data. It also provides user authentication and it also provides optional replay protection and access protection. AH will not provide encryption for any portion of the packets. Initially ESP protocol could provide only encryption to the data, So AH was used to provide authentication. AH and ESP were often used together to provide both confidentiality and integrity for the data. Later as the authentication capabilities were added to ESP AH has become less significant. Latest IPSec software no longer supports AH. AH is still of value because AH can authenticate portions of packets that ESP cannot.

Authentication Header (AH) protocol is IP protocol 51(S. Kent). It provides authentication and integrity, but it does not offer confidentiality for the packet's payload. AH can only be used, if your concern is confidentiality. AH guarantees that the information it contains came from the person who claimed to have sent it. A good characteristic of AH is that because it

does not use complex encryption algorithms it has a smaller size payload than ESP. AH provides limited security to the packet. It can only provide authentication and integrity but it can't provide any confidentiality as the payload will be visible to anyone on the traffic.

AH works in transport and tunnel modes. Unlike the transport mode in the tunnel mode AH creates a new IP header for each packet. In IPSec architectures that use a gateway, the true source or destination IP address for packets must be altered to be the gateway's IP address. Because transport mode cannot alter the original IP header or create a new IP header, transport mode is generally used in host-to-host architectures. AH provides integrity protection for the entire packet, regardless of which mode is used. AH packets have a smaller processing burden on the device as it is only limited to sending the packet.

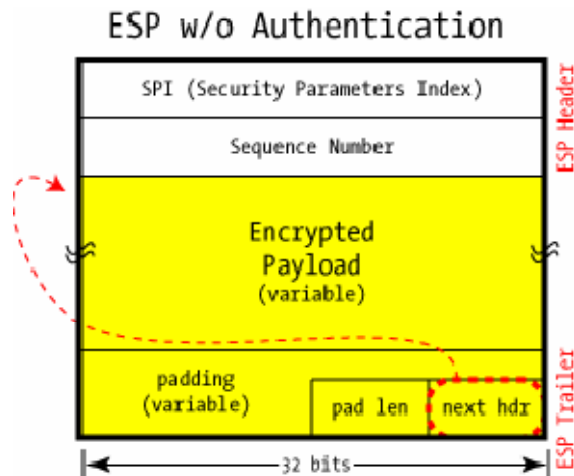


- The AH length field states the length of the AH header information.

- Reserved field is for future extensions of the AH protocol.
- The SPI field shows to which SA the packet belongs to.
- The sequence number field is an incrementing value that prevent against replay attacks.
- The authentication data contains the information for authenticating the packet.

Encapsulating Security Payload (ESP)

The second security protocol that IPsec offers is Encapsulating Security Payload (ESP). ESP is protocol 50 and normally is used to provide encryption and limited traffic flow confidentiality (Roger Younglove). Unlike AH, ESP offers confidentiality. ESP works differently in transport and tunnel modes. When ESP is implemented in transport mode it will adds its own header to the IP header and then encrypts the payload. Packets integrity and authentication can be maintained by ESP when a trailer is added. ESP actually encapsulates the whole packet when implemented in the tunnel mode. It will encrypt the whole original packet and add a new IP header and a new ESP header to the packet. A trailer will then be added for authentication purposes if the ESP authentication service is used. The following diagram shows an ESP packet.



The SPI is the security parameters index.

- The sequence number is used to prevent replay attacks.
- The next field is the encrypted payload.
- The next field uses padding which is optional.
- The next header field shows the protocol number for the information inside the ESP packet.

Initially ESP provided only encryption for packet payload data. Integrity protection was provided by the AH protocol. Later ESP became more flexible as it was able to provide authentication but it is not as effective as AH. ESP's encryption can be disabled through the Null ESP Encryption Algorithm. Therefore, in all but the oldest IPsec implementations, ESP can be used to provide only encryption; encryption and integrity protection; or only integrity protection (Steven Bellovin).

ESP Modes

ESP also works in both transport and tunnel modes. ESP creates a new IP header for each packet when implemented in the tunnel mode. The new IP header lists the endpoints of two IPsec gateways as the source and destination of the packet. Tunnel mode can encrypt and/or protect the integrity of both the data and the original IP header for each packet.²⁸ By encrypting the data is protected from being accessed or modified by unauthorized parties. By encrypting the IP header actual source or destination of the packet are assured and the nature of the communications is secured as well. If the authentication is being used for integrity purpose, each packet will have an ESP Authentication section after the ESP trailer.

ESP tunnel mode is more popular than the ESP transport mode. In transport mode implementation ESP uses the original IP header instead of creating a new one. In transport mode, ESP can only encrypt and/or protect the integrity of packet payloads and certain ESP components, but not IP headers. As with AH, ESP transport mode is generally only used in host-to-host architectures. The same security protocol formats, AH and ESP, are used in ML-IPsec. Both AH and ESP have transport mode or tunnel mode, as indicated by the “protocol mode” field of the designated SA (Yongguang Zhang).

Conclusion

End-to-end network security built upon IPSec with hardware-based encryption offers an optimum balance between security and performance. IPSec enabled operating systems and network adapters provide the building blocks needed to create secure LAN workgroups. Companies must develop policies that reflect business needs then implement them in a phased deployment strategy that secures data at highest risk first.

References

AH is IP protocol number 51. The AH version 2 standard is defined in RFC 2402, IP Authentication Header, available at <http://www.ietf.org/rfc/rfc2402.txt>.

Forouzan, Behrouz, 2006, TCP/IP Protocol Suite, McGraw-Hill, New York, NY, pp 682-683, 736, 749-750, 754-760.

Convery, Sean, 2004, Network Security Architectures, Cisco Press, Indianapolis, IN, pp 353-381.

Stephen, Northcutt, Lenny Zelster, Scott Winters, Karen Kent, Ronald Ritchey, 2005, Inside Network Perimeter Security, Sams Publishing, Indianapolis, IN, pp 170-182.

Shoniregun, C. A. (2007). *Advance in Information Security: Synchronizing Internet Protocol Security (IPSec)*. New York: Springer. Retrieved March 20, 2010, from Google Books: <http://books.google.com/books>

IP Security Features by Intel Ethernet Server Adapters and Microsoft Windows Server 2008. (n.d.). Retrieved 3 12, 2010, from <http://www.intelethernet.com/assets/intelmicrosoftpaper.pdf>

AH is IP protocol number 51. The AH version 2 standard is defined in RFC 2402, IP Authentication Header, available at <http://www.ietf.org/rfc/rfc2402.txt>.

AH is also required by some protocols, such as Cellular IPv6. More information is available in RFC 3316, Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts, at <http://www.ietf.org/rfc/rfc3316.txt>.

RFC 3884, Use of IPsec Transport Mode for Dynamic Routing, proposes a way to use transport mode to provide tunnels via IP-in-IP. It is available at <http://www.ietf.org/rfc/rfc3884.txt>. More information on IP-in-IP is available from RFC 2003, IP Encapsulation within IP, available at <http://www.ietf.org/rfc/rfc2003.txt>.

As specified in RFC 2406, ESP version 2 is only required to support DES for encryption, but most implementations support stronger encryption algorithms. NIST recommends that AH or ESP integrity protection should be used whenever ESP encryption is used.

Research has shown that IPsec is susceptible to multiple types of attacks if ESP

encryption is used without AH or ESP integrity protection. For more information on such attacks, see the paper titled Problem Areas for the IP Security Protocols by Steven Bellovin, available at <http://www.research.att.com/~smb/papers/badesp.pdf>.

Ghislaine Labouret “IPSec: a technical overview “Internal study Initial version on 7 December 1998.Last revised on 16 juin 2000 URL:

<http://www.hsc.fr/ressources/articles/ipsec-tech/index.html.en#3>

Roger W. Younglove “ IP Security What makes-it work?” COMPUTING & CONTROL ENGINEERING JOURNAL FEBRUARY 2001 Downloaded on July 18, 2010 at 18:22:43 UTC from IEEE Explore URL:

<http://ieeexplore.ieee.org.jproxy.lib.ecu.edu/stamp/stamp.jsp?tp=&arnumber=905757>

William Stallings “IP Security” The Internet Protocol Journal - Volume 3, No. 1 URL: http://www.catalyst.info/web/about/ac123/ac147/ac174/ac197/about_cisco_ipj_archive_article09186a00800c830b.html.

Yongguang Zhang, Member, IEEE “A Multilayer IP Security Protocol for TCP Performance Enhancement in Wireless Networks” IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 22, NO. 4, MAY 2004 URL:

<http://ieeexplore.ieee.org.jproxy.lib.ecu.edu/stamp/stamp.jsp?tp=&arnumber=1295063>

Rami Rosen , “How to create IPsec and SSL/TLS tunnels in Linux.” Jan 01, 2008 Linux Journal. URL: <http://www.linuxjournal.com/article/9916>.