



Interested in learning more about security?

## SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

### IPsec's Role in Network Security: Past, Present, Future

What is this term IPsec that I keep hearing, and reading about? IPsec stands for Internet Protocol Security. Simply put, IPsec is a set of open standard protocols that govern the secure, private exchange of data across public networks, such as the Internet. It was developed by the Internet Engineering Task Force (IETF), and explained primarily in RFC 2401-2412. IPsec works on Layer 3, the Network layer of the Open Systems Interconnection 7-layer networking model. By running on Layer 3, IPsec is ...

Copyright SANS Institute  
Author Retains Full Rights

**utimaco**<sup>®</sup>  
The Data  
Security Company

Choose the software that protects your:

♦ Data at Rest ♦ Data in Motion ♦ Data in Use



## **IPsec's role in Network Security: Past, Present, Future**

### **Introduction**

What is this term IPsec that I keep hearing, and reading about? IPsec stands for Internet Protocol Security. Simply put, IPsec is a set of open standard protocols that govern the secure, private exchange of data across public networks, such as the Internet. It was developed by the Internet Engineering Task Force (IETF), and explained primarily in RFC 2401-2412. IPsec works on Layer 3, the Network layer of the Open Systems Interconnection 7-layer networking model. By running on Layer 3, IPsec is able to function transparently to applications running on Layer 7; the applications do not require any knowledge of IPsec in order to use it. IPsec is used to create tunnels for Virtual Private Networks (VPN), and also provide confidentiality, authenticity, and integrity of data through use of encryption algorithms. Combined with Internet Key Exchange (IKE), IPsec users can exchange keys, authenticate one another, and securely tunnel encrypted data between peers.

### **IPsec Past**

The ghost of IPsec past is buried in the Internet Protocol Version 4 (IPv4) standard. IPv4 does not inherently provide any security for data transmitted across networks, it's sent in clear text across the Internet for anyone to intercept and read. In addition, IPv4 can't ensure that the source IP address, or the sender of the data, really is what it says it is – that the IP address hasn't been spoofed. The need for an update to IPv4 was clear, one that provided encryption for certain data as it traversed the Web. Prior to IPsec, Secure Sockets Layer (SSL) was developed as a method of encrypting data that provided piecemeal IP security. SSL encrypts data between the application running on the client, such as a web browser, and the web server. However, this solution is incomplete because the only encrypted data is between that application (browser), going to and from the specific https URL. The rest of the http traffic the browser is sending and receiving, in addition to all other data, is sent in non-encrypted form. This is only a partially secure transmission!

This is where the IETF steps in. As the governing body of Internet standards, the IETF establishes Working Groups to develop RFC's, or Request For Comments, that carefully explain in detail the fundamentals of the Internet technologies we use daily. This is a description of the IPsec Working Group, from it's IETF charter: "Rapid advances in communication technology have accentuated the need for security in the Internet. The IP Security Protocol Working Group (IPSEC) will develop mechanisms to protect client protocols of IP. A security protocol in the network layer will be developed to provide cryptographic security services that will flexibly support combinations of authentication, integrity, access control, and confidentiality". 1

Clearly the need existed for IPsec. The IETF began designing IPsec in 1992 in open committees, and under close public scrutiny. This openness in developing cryptographic algorithms is much preferable to proprietary security, such as Microsoft's PPTP, which has had all sorts of security issues since inception. In his book Secrets and Lies: Digital Security in a Networked World, Counterpane Labs' Bruce Schneier discusses the need for public development of cryptographic algorithms, and protocol groups such as IPsec: "You want to minimize your risk. If you go with IPsec, you have a much greater assurance that the algorithms and protocols are strong. Of course, this is no guarantee of security – the implementation could be flawed, or a new attack could be discovered – but at least you know that the algorithms and protocols have withstood a level of analysis and review that the other options have not".<sup>2</sup>

## IPsec Present

Today, IPsec is used widely by nearly all security vendors. It is the primary security protocol used in VPNs. IPsec was defined in RFC 2401. There are numerous other RFC's that deal with IPsec also, including 2402-2412, 2451, and 2857. RFC 2401 was published November 1998, and obsoletes RFC 1825. Let's take a closer look under the hood of IPsec, and explain the inner workings.

IPsec provides IP datagrams with confidentiality, authenticity, data integrity, and replay protection. Sounds great, but what do these terms mean? Confidentiality of data means that you protect it from the prying eyes of anyone packet sniffing the wire. The goal is to keep the data private, and only allow access to people you choose. Good encryption algorithms help achieve data confidentiality. Authenticity means if someone sends you data, then you can confirm their identity, and they can confirm your identity, through a digital signature or other means. Data Integrity means that the data has not been intercepted and altered en route from source to destination. Replay protection means that a data transaction is only carried out once unless there is proper authorization to repeat it, so a forger can't repeatedly send the same data which allows him to deposit that same \$500 into his bank account over and over. According to the RFC however, replay protection is only available in an IPsec implementation using Internet Key Exchange (IKE), and not when using manual-keyed IPsec.

## Protocols

IPsec uses two new protocols to provide data confidentiality, authenticity, integrity, and replay protection: Authentication Header and Encapsulating Security Payload. They are appended to the data in the form of packet headers. The following description is taken from the Cisco Systems White Paper on IPsec.

- *Authentication header (AH)*—This header, when added to an IP datagram, ensures the integrity and authenticity of the data, including the invariant fields in the outer IP header. It does not provide confidentiality protection. AH uses a keyed-hash function rather than digital signatures, because digital signature technology is too slow and would greatly reduce network throughput.
- *Encapsulating security payload (ESP)*—This header, when added to an IP datagram, protects the confidentiality, integrity, and authenticity of the data. If

ESP is used to validate data integrity, it does not include the invariant fields in the IP header. <sup>3</sup>

AH and ESP are appended to the IP datagram after the IP header (Layer 3), and just before the Layer 4 protocol – most often TCP or UDP. For both AH and ESP, IPsec allows any standard algorithms to be used for security. AH is defined further in RFC 2402, and ESP in RFC 2406.

IPsec uses a Security Association (SA) to define a secure link from source to destination. Defined in RFC 2401, “A Security Association (SA) is a simplex "connection" that affords security services to the traffic carried by it”. <sup>4</sup> Each SA is created for a unidirectional flow of data. In order to achieve duplex communication between nodes, at least 2 SA's must be created – one SA for node A to send data and node B to receive; another SA for node B to send data and node A to receive. An SA can use AH or ESP to secure communications, but not both. How do incoming or outgoing packets know which SA they are associated with? Each Security Association has a unique identifier assigned to it that consists of the destination IP address, security protocol (AH or ESP), and the Security Parameter Index (SPI).

### **Modes**

There are two modes available for IPsec -- Transport mode and Tunnel mode. Transport mode only encrypts the payload, or data in the packet. The header is left in clear text. Tunnel mode is more secure, as it encrypts both the data payload and the header. There are further differences between the two modes. Transport mode can only be used between two hosts, whereas tunnel mode must be used when one endpoint of the SA is a security gateway. Here's the breakdown:

Host to Host = Transport mode

Host to Security Gateway = Tunnel mode

Security Gateway to Security Gateway = Tunnel mode

IPsec is typically implemented in tunnel mode. The security gateways – usually a firewall, router, or VPN concentrator – create the SA and handle encryption. This allows an IPsec deployment without having to modify the OS or applications on your systems, whether servers or workstations. This is a benefit in terms of VPN deployment, as the network administrator only needs to configure the security gateway endpoints, and not each system that will benefit from using IPsec. This helps to reduce total cost of ownership (TCO), and keeps your manager happy. There are numerous implementations of IPsec VPNs, and I will discuss these in the IPsec Future section.

Since IPsec by definition allows an open framework for different types of encryption and authentication, these items must be worked out between the two endpoint nodes. The nodes need to decide which algorithms to use, and also share session keys. Once the SA is configured on your security gateway, when a system on your network sends a packet that needs IPsec encryption, it travels to the security gateway, and the gateway looks up the security association in its Security Policy Database (SPD) for outbound

traffic. Once the gateway processes the packet according to the specific SPD entry for it, a SPI is inserted into the IPsec header from the SA. When the peer system on the destination network receives the packet it looks up the security association in its SPD, according to destination address and SPI. The destination system now knows how to process this IPsec packet, assuming there is an entry for it in the destination security gateway Security Policy Database for incoming traffic.

### **Internet Key Exchange**

IPsec works hand-in-hand with ISAKMP, otherwise known as IKE, or Internet Key Exchange. IKE provides a key exchange mechanism, when used in conjunction with IPsec you can encrypt data, create security associations (SA), and operate VPNs. IKE is further explained in RFC 2409. IKE provides the auto-management of cryptographic key exchange between security endpoints. Without IKE, you would have to manually key each device. This solution may be acceptable for small environments with few users, but it does not scale well. If you plan to have more than just a handful of systems passing IPsec traffic, then Internet Key Exchange is a beautiful thing – another TCO triumph! Also, recall that when using manual-keyed IPsec, no replay protection is provided.

IKE uses a two-phase process for establishing the IPsec parameters between two IPsec nodes. Taken from RFC 2409:

- Phase 1 is where the two ISAKMP peers establish a secure, authenticated channel with which to communicate. This is called the ISAKMP Security Association (SA). "Main Mode" and "Aggressive Mode" each accomplish a phase 1 exchange. "Main Mode" and "Aggressive Mode" MUST ONLY be used in phase 1.
- Phase 2 is where Security Associations are negotiated on behalf of services such as IPsec or any other service which needs key material and/or parameter negotiation. "Quick Mode" accomplishes a phase 2 exchange. "Quick Mode" MUST ONLY be used in phase 2. 5

In Phase 1, Main Mode allows for the key exchange with identity protection, as the IKE SA is negotiated over a sequence. Aggressive Mode does not provide identity protection since all authentication data is sent at once. As a result, it should only be used when bandwidth is scarce, and security not completely crucial. During Phase 1, both IPsec nodes establish a connection where they authenticate each other. This is usually done using a pre-shared secret, or a X.509 digital certificate from a well-known, mutually trusted certificate authority. In Phase 2, IPsec creates the actual tunnels between IPsec hosts that will be used. Quick Mode can be used in Phase 2 since the SA was created during Phase 1, and it's not necessary to repeat full authentication. Finally, the main purpose of Phase 2 is to exchange cryptographic keys, and get the IPsec VPN up and running.

## **Cryptography**

Cryptographic algorithms are the lifeblood of IPsec. Without good cryptography, you effectively remove the security from IPsec, and you're left with plain old clear text IP. As Bruce Schneier mentioned, publicly tested industry-standard cryptography is best. Since IPsec allows freedom in implementing crypto, why bother going to all the trouble to configure and use IPsec if you choose a weak algorithm?

DES and 3DES are widely used, although DES has been repeatedly, publicly cracked. It's possible to use DES in your IPsec implementation, provided you realize its limitations and plan accordingly. This means to limit the life of the security association when using DES, so that the SA is renegotiated well before any computer could crack DES – roughly 22 hours. The upside of this strategy is less hardware encryption processing power is needed on your router, firewall, or VPN concentrator. The downside is that more bandwidth is used in renegotiating the SA, and the fact that you're using a well-known crackable algorithm. Diffie-Hellman is used initially between peers, and public key cryptography to guarantee both parties' identity helps to eliminate the man-in-the-middle attack. For hash algorithms, there is MD5, SHA, and HMAC combines with these for packet authentication. There are numerous RFC's written specifically about these algorithms, and how they are used with IPsec, mostly in the 2401-2412 group.

## **VPN Implementations of IPsec**

Commercial IPsec VPN products are everywhere in 2001. Cisco, Nokia, Redcreek, SonicWall, and WatchGuard are a few of the most common hardware VPNs offered. Microsoft Windows 2000 Advanced Server, and Novell BorderManager are software alternatives to a hardware device. In terms of network security, a hardware VPN concentrator is much preferable to a VPN running on top of an OS. This is because you have more network services running on the OS that, if exploited, could become points of entry into your network. Also, servers have numerous moving parts (e.g. disk drives) that can and will fail. What will your remote users or branch offices do when they can't authenticate to your home office VPN due to a hard drive failure? Chances are the boss won't be happy about that one.

FreeS/WAN is an open source, Linux based IPsec implementation. The most current stable release is Version 1.91. Here we have a completely free alternative for running IPsec on an OS, rather than paying for Microsoft or Novell licences. If you choose to go the software route with deploying IPsec, then FreeS/WAN is definitely the cheapest. The downside of FreeS/WAN is the same as the for-profit operating systems: potential security holes and moving parts. Plus, you don't have direct support as with a commercial product, but must rely on the support of the open source community if you have problems. Some would say this is a better alternative than most commercial support call centers! I must admit that using FreeS/WAN for IPsec is an extremely attractive proposition, and the TCO is zero.

To allow IPsec through a firewall, you must open UDP port 500 (for IKE), IP type 50 (for ESP) and/or IP type 51 (for AH). Most configuration occurs on the security gateway

itself, and commercial router vendors have good documentation for configuring IPsec. In addition you must configure remote clients to connect to the office VPN, unless you have technically savvy users, or you're using a product that provides a configuration wizard such as Redcreek's Ravlin Soft VPN client.

### **IPsec Future**

Where do we go from here? IPv6 has been designed with IPsec at its center. Hopefully, this will create a more secure protocol by engineering IPv6 with IPsec built-in, rather than retroactively applying it in the case of IPv4.

The corporate use of VPNs continues to grow, with IPsec planted firmly at the center. This projection is from PC Magazine: "More than 56 percent of companies with 1,000 or fewer employees and 70 percent of larger companies already have VPNs in place or are in the process of installing them, according to a recent study by *CIO Insight* magazine. Datamonitor projects that last year's \$585 million in VPN sales will grow to reach \$6 billion by 2005".<sup>6</sup>

From initial planning meetings in 1992, to RFC 2401 in November 1998, to the quickly growing VPN market in 2001 and beyond, IPsec has been a steady workhorse. It has been used in corporate extranets for business partners and customers, as well as applications internal to a company. The increasing trend of mobile workers and telecommuters will see VPNs with IPsec pumping away behind the scenes, creating secure tunnels for all.

### **References**

1. Fraser, Barbara and Ts'o, Theodore. IETF IPsec Working Group Charter. 31 July 2001. URL: <http://www.ietf.org/html.charters/ipsec-charter.html> (15 September 2001).
2. Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons, Inc, 2000. 117.
3. Cisco Systems White Paper – IPsec.  
URL: [http://www.cisco.com/warp/public/cc/so/neso/sqso/eqso/ipsec\\_wp.htm](http://www.cisco.com/warp/public/cc/so/neso/sqso/eqso/ipsec_wp.htm)
4. Kent & Atkinson. "Security Architecture for the Internet Protocol". RFC 2401. November 1998. URL: <http://www.ietf.org/rfc/rfc2401.txt>
5. Harkins & Carrel. "The Internet Key Exchange". RFC 2409. November 1998. URL: <http://www.ietf.org/rfc/rfc2409.txt>
6. Bannan, Karen J. "Safe Passage: Virtual Private Networking". PC Magazine September 25, 2001. (2001): 116.



# Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS SOS London 2009	London, United Kingdom	Jul 13, 2009 - Jul 18, 2009	Live Event
SANS Future Visions 2009 Tokyo	Tokyo, Japan	Jul 15, 2009 - Jul 17, 2009	Live Event
SANS IMPACT 2009	Kuala Lumpur, Malaysia	Jul 27, 2009 - Aug 01, 2009	Live Event
SANS SEC563: Mobile Device Forensics Debut	Baltimore, MD	Jul 27, 2009 - Jul 31, 2009	Live Event
SANS Boston 2009	Boston, MA	Aug 02, 2009 - Aug 09, 2009	Live Event
SANS WhatWorks in Virtualization and Cloud Computing Security Summit 2009	Washington, DC	Aug 17, 2009 - Aug 21, 2009	Live Event
SANS Atlanta 2009	Atlanta, GA	Aug 17, 2009 - Aug 28, 2009	Live Event
SANS Virginia Beach 2009	Virginia Beach, VA	Aug 28, 2009 - Sep 04, 2009	Live Event
SANS SCDP SEC556: Comprehensive Packet Analysis - Sept. 2009	Ottawa, ON	Sep 09, 2009 - Sep 10, 2009	Live Event
SANS Critical Infrastructure Protection at Oceania CACS2009	Canberra, Australia	Sep 10, 2009 - Sep 11, 2009	Live Event
SANS Network Security 2009	San Diego, CA	Sep 14, 2009 - Sep 22, 2009	Live Event
SANS SCDP Cutting Edge Hacking Techniques - June 2009	Ottawa, ON	Sep 15, 2009 - Sep 15, 2009	Live Event
SANS Rocky Mountain 2009	OnlineCO	Jul 07, 2009 - Jul 13, 2009	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced