GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Security Features in IPv6

© SANS Institute 2000 - 2005, Author retains full rights.

By: Penny Hermann-Seton
GIAC GSEC Practical Assignment v1.4, Option 1

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

List of Figures

© SANS Institute 2000 - 2005, Author retains full rights.

Abstract

This paper will present a brief overview of some of the new features provided by the Internet Protocol version 6 (IPv6). It will take an in-depth view of the new security features in IPv6, namely the use of the Authentication Header and Encapsulating Security Payload (ESP) Header. This document will examine how these security features can prevent certain types of network attacks currently occurring over the Internet and discuss some of the open issues with the IPV6 security features.

Introduction to IPv6 (also known as IPng)

The current version of the Internet Protocol, which is the fundamental protocol used to send information over the Internet, is IPv4. The IPv4 specification dates back to the 1970's. It has known limitations in the area of limited IP addresses and lack of security. IPv4 specifies a 32-bit IP address field, which will be running out of available address space in the near future. Especially taking into consideration the new mobile devices/internet appliances that will be connected to the Internet in the near future. The only security feature provided in IPv4 was a security option field, which addressed DoD specific requirements. As a result of these known limitations, a study effort was directed by the Internet Engineering Task Force (IETF) in the early 1990's to address these limitations along with performance, ease-of-configuration, and network management issues. The IPv6 specification was produced from the IETF study efforts and are defined by various RFC's (RFC 1752, 2460, 2462, 2406, etc.). IPv6 is also referred as the Next Generation Internet Protocol (IPng). The major feature upgrades in IPv6 include:

128-bit IP Address

Instead of allowing for only 32-bit IP addresses of the form 192.168.123.67, IPv6 allows for 128-bit IP address fields in the form of 8 16-bit integers separated by colons. The 16-bit integers are represented as 4 hexadecimal digits. An example of an IPv6 IP address might look like the following: ABCD:EF01:2345:6789:0123:4567:8FF1:2345.

With the increased IP address size, up to 2^{128} or 3.4×10^{38} different IP addresses can be defined, which "provides 655,570,793,348,866,943,898,599 (6.5×10^{23}) addresses for every square meter of the Earth's surface" (Davies, p.9).

New Header Format

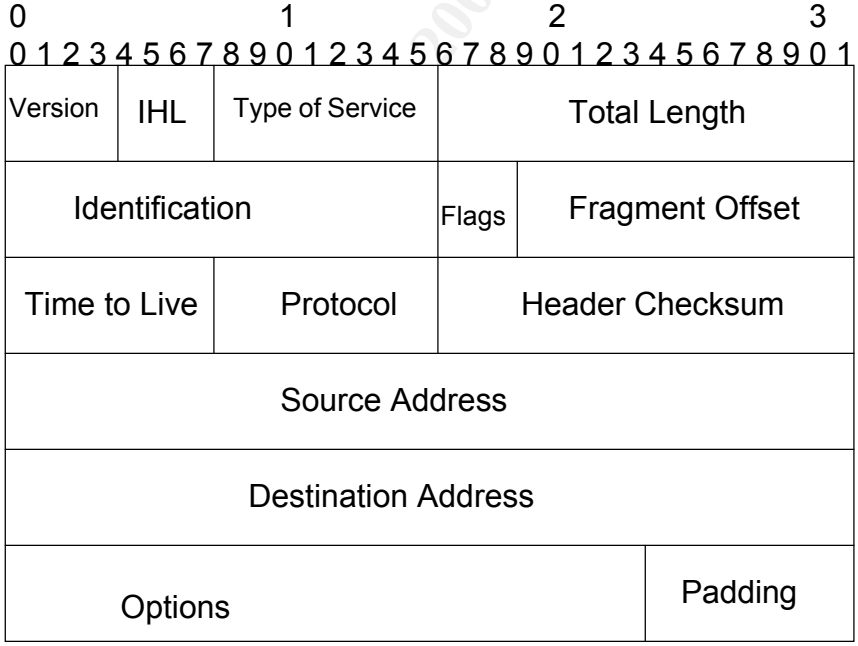
The IP header in IPv6 has been streamlined and defined to be of a fixed length (40 bytes). In designing the IPv6 Header, fields from the IPv4 Header have been removed, renamed (but still providing the same type of functionality) or moved to

© SANS Institute 2000 - 2005 Author retains full rights.

the new optional IPv6 Extension Headers. Please refer to the IPv4 Header format as shown in Figure 1 (Information Sciences Institute, p.11) and the IPv6 Header format as shown in Figure 2 (Huitema, p.63).

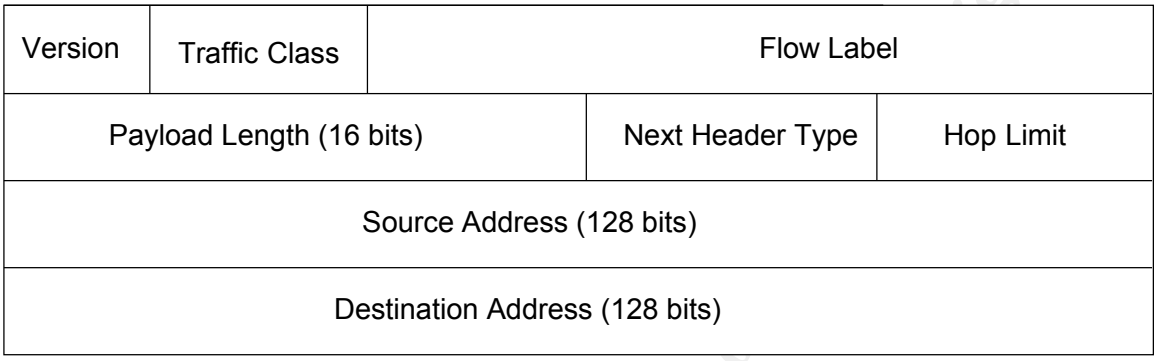
The “IHL” or header length field is no longer needed since the IPv6 Header is now a fixed length. The IPv4 “Type of Service” is equivalent to the IPv6 “Traffic class” field. The “Total Length” field has been replaced with the “Payload Length” field. Since IPv6 only allows for fragmentation to be performed by the IPv6 source and destination nodes, and not individual routers, the IPv4 segment control fields (Identification, Flags, and Fragment Offset fields) have been moved to similar fields within the Fragment Extension Header. The functionality provided by the “Time to Live” field has been replaced with the “Hop Limit” field. The “Protocol” field has been replaced with the “Next Header Type” field. The “Header Checksum” field was removed, which has the main advantage of not having each relay spend time processing the checksum. This, however, also introduces the risk of undetected errors, which is seen as minimal due to checksums being used in most of the encapsulating procedures. (Huitema, p.65), The “Options” field is no longer part of the header as it was in IPv4. Options are specified in the optional IPv6 Extension Headers. The removal of the options field from the header provides for more efficient routing; only the information that is needed by a router needs to be processed.

Figure 1. IPv4 Header



© SANS Institute 2000 - 2005 Author retains full rights.

Figure 2. IPv6 Header



In IPv4, the IPv4 header is followed by the transport protocol data (typically TCP, UDP, or ICMP), also known as the IP packet payload.

In IPv6, the IPv6 header is followed by various Extension Headers (specified in a certain order) and then the transport protocol data (header/data).

Native Security

In IPv6, IP security (IPsec) is part of the protocol suite. It is mandatory. IPsec is a set of security specifications originally written as part of the IPv6 specification. Due to the strong need for security in the current IPv4 Internet, IPsec was also adapted for IPv4. However, support for IPsec in IPv4 is optional and "proprietary solutions are prevalent" (Davies, p.1). IPsec in IPv6, on the other hand, provides end-to-end security, i.e. data is secured from the originating workstation/host (through the various routers, etc. of the Internet) to the destination workstation/host. In IPv4, IPsec typically provides security between border routers of separate networks.

Quality of Service (QoS)

A Quality of Service feature can be implemented using the Flow Label field of the IPv6 header. QoS is a feature needed to ensure that high priority is given to certain packets that need to arrive at their destination in a timely manner. For example, in streaming video or Voice over IP, these packets need to arrive close together since a small delay can make the video or voice choppy. If there is just text being transmitted, a small delay between the packets is really of no consequence.

© SANS Institute 2000 - 2005 Author retains full rights.

Auto-configuration

IPv6 provides the ability for stateful and stateless auto-configuration of IP addresses. Stateful auto-configuration utilizes the stateful Dynamic Host Configuration Protocol (DHCP), in which static tables are maintained to determine the IP address to be assigned to a newly connected node. Stateless auto-configuration occurs without the use of DHCP.

New Extension Headers

The IPv6 specification currently defines 6 Extension Headers:

- Routing Header - Similar to the source routing options in IPv4. Used to mandate a specific routing.
- Authentication Header (AH) - A security header which provides authentication and integrity.
- Encapsulating Security Payload (ESP) Header - A security header which provides authentication and encryption.
- Fragmentation Header - The Fragmentation Header is similar to the fragmentation options in IPv4.
- Destination Options Header - This header contains a set of options to be processed only by the final destination node. Mobile IPv6 is an example of a Destination Options Header.
- Hop-by-Hop Options Header - A set of options needed by routers to perform certain management or debugging functions.

A new version of the Internet Control Message Protocol (ICMP), which is responsible for reporting errors and providing network information, has been defined for IPv6. ICMP for IPv6 (ICMPv6) is part of the IPv6 specifications.

There exists a world-wide test bed for IPv6 called the 6Bone, which is a shortened name for IPv6 backbone. There are currently several commercially available IPv6 networks. vBNS+, a product of Worldcom and the National Science Foundation, supplies an IPv6 network in the US that supports high-performance, high-bandwidth applications. Telia Sweden, a Swedish telecommunication company, currently provides IPv6 network services to a small set of customers. NTT Communications Corporation runs a global commercial IPv6 Gateway Service which was started in April 2001.

The transition to IPv6 is foreseen to occur over a long period of time where both IPv4 and IPv6 will co-exist on the Internet. Techniques that will be utilized to support this include dual-stack IPv4/IPv6 hosts and routers, and tunneling of IPv6 via IPv4.

This paper will focus on the security features and other new features in IPv6 as it relates to security.

© SANS Institute 2000 - 2005, Author retains full rights.

IPsec

IPsec is used in IPV4 to implement Virtual Private Networks (VPNs). IPsec is a security framework defined by RFC 2401, “Security Architecture for the Internet Protocol”. IPsec provides network-level security, which means that an application running over an IPv6 network, e.g. a web-server, browsing the Internet, any application sending/receiving data over the Internet, etc., will also have this security, since the application data is encapsulated within the IPv6 packet.

IPsec utilizes the Authentication Header and Encapsulating Security Payload Header to provide security. The AH and ESP Header may be used separately or in combination to provide the desired security. Both the AH and ESP header may be used in the following modes:

- “tunnel mode” - The protocol is applied to the entire IP packet. This method is needed to ensure security over the entire packet, where a new IPv6 header and an AH or ESP header are wrapped around the original IP packet.
- “transport mode” – The protocol is just applied to the transport layer (i.e. TCP, UDP, ICMP) in the form of an IPv6 header, AH or ESP Header, followed by the transport protocol data (header, data).

Security Associations

A fundamental concept in IPsec is that of a Security Association (SA). A Security Association is uniquely identified by the Security Parameters Index (a field in the AH / ESP header), destination IP address and security protocol (AH or ESP). It is a one-way relationship between sender and receiver. The SA defines the type of security services for a connection. It usually contains the key needed for authentication or encryption, and the authentication or encryption algorithms to be used. The Internet Key Exchange (IKE) describes the process used to negotiate parameters needed to establish a new SA (transfer of secret keys, cryptographic algorithm, etc.).

Authentication Header (AH)

The Authentication Header (AH) provides data integrity and data authentication for the entire IPv6 packet. Anti-replay protection is also provided by the AH.

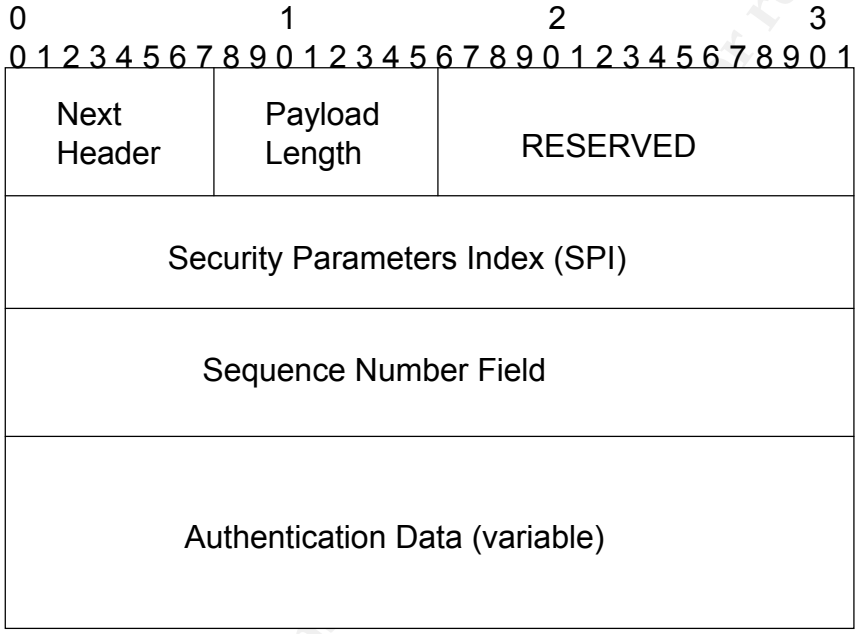
Data authentication refers to the fact that if a given computer receives an IP packet with a given source address in the IP header, it can be assured that the IP packet did indeed come from that IP address. Data integrity refers to the fact

© SANS Institute 2000 - 2005 Author retains full rights.

that if a given computer receives an IP packet, it can be assured that the contents have not been modified along the path from the source node to the destination node. Anti-replay protection means that if a computer has already received a particular IP packet, another packet with modified data won't also be accepted as valid data.

Next, the Authentication Header fields will be examined to determine how these security features are provided. Refer to Figure 3 for the format of the Authentication Header (Kent and Atkinson, RFC 2402, p.3).

Figure 3. Authentication Header



The Authentication Header contains a Next Header field, which identifies the next Extension Header or transport type (e.g. TCP). The Payload Length field contains the length of the Authentication Header. The Security Parameters Index (SPI) field contains the Security Parameters Index to be used in identifying the Security Association.

The Sequence Number field is a counter field. The sequence number is set to 0 when the communication phase between the sender and receiver is established. It is subsequently incremented by 1 when either the sender or receiver transmits data. If the receiver detects an IP packet with a duplicate Sequence Number Field, it is rejected (anti-replay protection). This prevents an attack where a hacker may try to modify data and re-send the altered IP data for

© SANS Institute 2000 - 2005 Author retains full rights.

malicious means similar to that seen in the Session Replay attacks in the current IPv4-based Internet. In the Session Replay attack, the hacker saves off the network transmissions between an authenticated user and server. The hacker then modifies the data and re-sends these modified packets as if they came from the authenticated user in the original session. For example, if in the original session, the authenticated user issued an order to sell a block of shares. The hacker could change certain data to indicate an order to purchase a block of shares.

The variable length Authentication Data contains the Integrity Check Value (ICV), which provides the authentication and data integrity. The authentication algorithm used to compute the ICV is specified by the SA. The ICV is calculated over the IP header fields that remain unchanged during transit, the AH header with the Authentication data set to zero, and the IP packet payload. Some of the fields that may change during transit include Hop Limit, Traffic Class, and Flow Label. The receiver of the IP packet with an AH header, re-computes the ICV value with the authentication algorithm and key identified in the SA. If the ICV is the same, the receiver knows that the data is authenticated and the data has not been modified.

Hash Message Authentication Code (HMAC) with Message Digest No. 5 (MD5) and HMAC with Secure Hash Algorithm No. 1 (SHA-1) are the proposed authentication algorithms required for global interoperability by RFC 2402, “IP Authentication Header”. HMAC is a technique for performing message authentication using a cryptographic hash function. It involves using a secret key with the original message before applying the hash function. MD-5 is a hash function that produces a 128-bit output and SHA-1 is a hash function that produces a 160-bit output. In a one-way hash function, like MD-5 or SHA-1, the algorithm processes an input string or plaintext, and produces an output string or encrypted text from which the original plaintext cannot be retrieved. The size of the encrypted string is a fixed length and much smaller then the original plaintext. However, given the same input, the hash function will produce the same encrypted string. The primary application of a hash function is to provide data integrity. The Authentication Header, however, may support different authentication algorithms.

IPv6 authentication is very valuable where auto-configuration is deployed to prevent illicit auto-configuration (King et al). The use of the Authentication Header prevents IP Spoofing Attacks, one of the network attack methods in use today. In IP Spoofing, the hacker creates IP packets, via various hacker utilities, with a different IP address then the host computer. This can be used for various malicious reasons. The hacker can act as one side of a trust relationship to gain access to a trusting host. For example, if a trust relationship exists with the “r utilities (rlogin, rsh, rcp)”, one computer processes the rlogin command from the other computer without further authentication (i.e. without prompting for a password). This situation where one computer is allowed to “rlogin”,

© SANS Institute 2000 - 2005 Author retains full rights.

unauthenticated, into another computer can be potentially dangerous. If the IP address of one of these trusted computers is spoofed by the hacker, the hacker now has access to the other computer. IP Spoofing is also employed in the TCP Session Hijacking attack. During a currently active established session, the attacker pretends to be one of the session participants, by spoofing the source IP address. IP Spoofing is also seen in the Man-in-the-Middle attack. An attacker basically positions himself in between 2 users communicating, using the technique of IP spoofing to become another user's computer.

IP Spoofing is also used by the following Denial of Service (DOS) attacks. A Denial of Service attack refers to an attack that renders the host incapable of performing its intended service (serving up web-pages, etc.) by either crashing the computer, locking up the computer, keeping the computer so busy performing other tasks that it can't respond to valid service requests, etc. IP Spoofing is seen utilized in the Land attack where the source IP address is spoofed to be the same as the destination IP address in an IP packet using TCP as the transport. This attack crashes Windows 95 machines and CISCO routers. In the Smurf Attack, the source IP address of an ICMP broadcast echo request is spoofed to be the IP address of a targeted machine. This type of attack relies on the inherent function of the broadcast echo request. When this request is received by a computer, it responds with an echo reply to the source IP address, which in this case is the targeted machine. This effectively floods the targeted machine. A SYN Flooding attack takes advantage of the TCP three-way handshake of SYN, SYN-ACK, and ACK that occurs during establishment of a TCP connection. In the TCP three-way handshake, the client first sends a SYN to indicate that the client would like to establish a connection with the server. The server responds with a SYN-ACK indicating that the server has received the client's SYN (denoted by the ACK) and would like to establish its own connection with the client (denoted by the SYN). The client then responds with an ACK indicating that it has received the server's SYN. During a SYN Flooding attack, the source IP address is spoofed with either random or non-existent IP addresses in the first SYN packet received by the server. The server sends out a SYN-ACK and then waits for the final ACK which it never receives. This effectively ties up the server's resources. After receiving numerous invalid SYN requests, thus the name "SYN Flooding", the server's resources are so tied up by the invalid SYN requests, that valid users are unable to establish a connection with the server.

Encapsulating Security Payload (ESP) Header

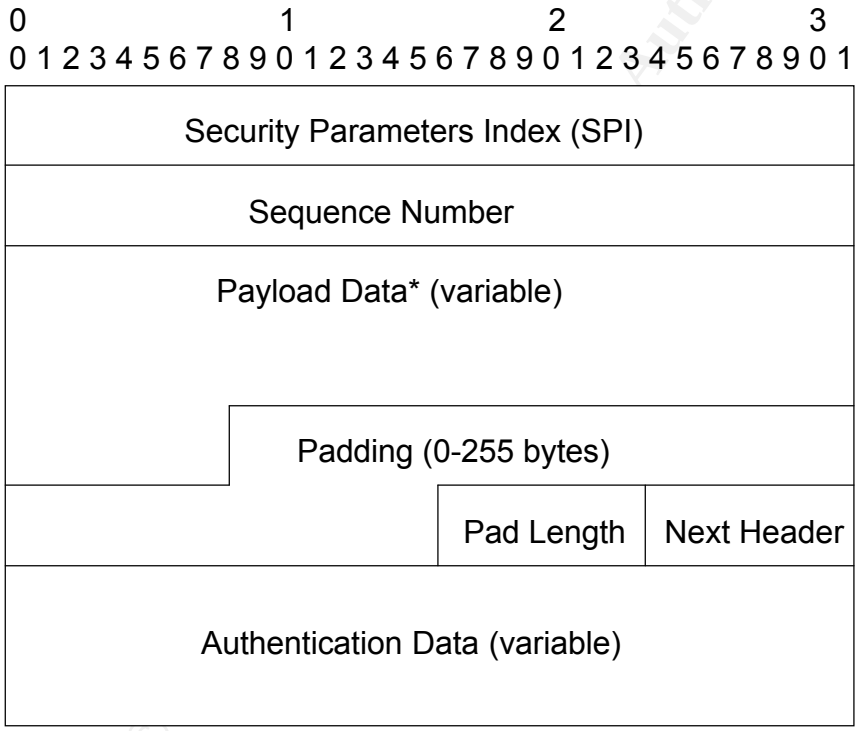
The Encapsulating Security Payload header provides confidentiality and/or authentication and data integrity to the encapsulated payload. Anti-replay protection is also provided by the ESP header. Note: During authentication in the ESP Header, the authentication algorithm is only applied to the data being encrypted. Therefore, the IP header fields are not protected by the authentication algorithm unless those fields are encapsulated in "tunnel mode".

© SANS Institute 2000 - 2005 Author retains full rights.

Confidentiality refers to the fact that a given computer receiving an IP packet can be assured that nobody else has seen the contents of the IP packet, besides the routers needing necessary information.

In the ESP header, both the confidentiality and authentication services are optional, however, at least one of these services must be selected. Next, the ESP Header fields will be examined to determine how these security features are provided. Refer to Figure 4 for the format of the ESP packet (Kent and Atkinson, RFC 2406, p.3).

Figure 4. ESP Packet Format



The Encapsulating Security Payload Header also contains an SPI field containing the Security Parameters Index that is used to identify the Security Association. The Sequence Number field is used to provide anti-replay protection as described in the section on the Authentication Header. The encrypted data is placed in the “Payload Data” field, as seen in Figure 4. The ESP trailer consists of the Padding, Pad Length, Next Header and

© SANS Institute 2000 - 2005 Author retains full rights.

Authentication Data fields. The Padding field contains any padding bytes that may be needed by the encryption algorithm. The Pad Length field contains the number of bytes in the Padding field. The Next Header Field describes the type of data contained in the Payload Data field (e.g., the entire IP packet if "tunnel mode" was employed or transport payload (TCP, UDP, ICMP) if "transport mode" was employed).

If the authentication security service is specified by the SA associated with the SPI, the Authentication Data field contains the Integrity Check Value (ICV) which provides the authentication and data integrity. The authentication algorithm used to compute the ICV is also specified by the SA. The ICV is calculated over the entire ESP packet, excluding the Authentication Data field.

The Payload Data is encrypted with the encryption algorithm, and key(s) identified by the SA. In "transport" mode, only the transport data is encrypted. In "tunnel mode", the entire IP packet is encrypted. The encrypted data is placed in the "Payload Data" field, as seen in Figure 4. Confidentiality by the ESP header is achieved via encryption. ESP is designed to be used with symmetric encryption algorithms (Kent and Atkinson, RFC 2406, p.10). In symmetric encryption, or secret key encryption, a single key is used for both encrypting and decrypting the data.

The Data Encryption Standard (DES) in Cypher Block Chaining (CBC) mode is the proposed encryption algorithm required for global interoperability by RFC 2406, "IP Encapsulating Security Payload (ESP)." DES is considered a weak encryption algorithm and no longer secure since it has been proven crackable. However, the ESP Header is also algorithm independent. It can be used with stronger encryption algorithms like Triple-DES or AES. The Advance Encryption Standard (AES) encryption algorithm is the latest standard for encryption, replacing DES. The weaker encryption algorithm is defined for global interoperability due to the US export restrictions on strong encryption algorithms.

The use of the ESP header, with the confidentiality service enabled, prevents use of a technique called "sniffing". "Sniffing" is a process of getting network transmission either for the data itself or for providing valuable information which may be used later in attacking other computers. Sniffers are one of the most common tools used by hackers. Examples of sniffers include TCPdump (for UNIX systems) and windump (for WINDOW systems), which is a tool used to collect and print IP packets being transmitted over a network. Sniffers can be used to gather information such as passwords, TCP sequence numbers (which may be used in TCP Session Hijacking attacks), any sensitive information transmitted in clear text between a Web browser and Web server, etc. With the IP packet payload data being encrypted, sniffers will no longer provide such valuable information.

Problems with IPv6 Security Features

© SANS Institute 2000 - 2005 Author retains full rights.

Although, the security provided by IPv6 is a great improvement over IPv4, it has its shortcomings. Among these are the following:

- Due to export laws, the strength of the encryption algorithms to be used to ensure global interoperability is limited.
- IPsec relies on a public-key infrastructure (PKI) that has not yet been fully standardized.
- There is some additional work needed in the IKE area and in improving protection against Denial of Service/Flooding attacks. (Hagen, p.104)

Conclusion

IPv6 supports many new features including increased address space, auto-configuration, QoS capabilities, and network-layer security. The IPv6 Authentication Header (AH) provides data integrity and data authentication for the entire IPv6 packet. The IPv6 Encapsulating Security Payload header provides confidentiality and/or authentication and data integrity to the encapsulated payload. Anti-replay protection is provided by both the AH and ESP Header. These security Extension Headers may be used separately or in combination to support different security needs. The security features in IPv6 can be used to prevent various network attack methods including IP spoofing, some Denial of Service attacks (where IP Spoofing has been employed), data modification and sniffing activity.

Open issues with the security features still exist, however, concerning IKE, PKI and the strength of the encryption algorithms used for global interoperability. It will be interesting to see how the migration to IPv6 transpires. It will also be interesting to see what new exploits will be used by the hacking community with the introduction of IPv6.

© SANS Institute 2000 - 2005 Author retains full rights.

List of References:

Cisco Systems, Inc. “Reference Guide Deploying IPSec.” May 2001. URL: http://www.cisco.com/warp/public/cc/so/neso/sqso/eqso/dplip_in.htm (24 August 2002).

Davies, Joseph. “Introduction to IP Version 6.” Microsoft Word Version. February 2002. URL: http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadrmgmt/introipv6.asp (24 August 2002).

Estala, Adrian. “Internet Protocol Version 6 : IPv6.“ June 1998. URL: http://www.geocities.com/SiliconValley/Foothills/7626/defin.html#_Toc424403782 (18 August 2002).

Hagen, Silvia. IPv6 Essentials. Sebastopol: O’Reilly & Associates, Inc, 2002.

Hinden, Robert. “IP Next Generation Overview.” May 1995. URL: http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html (24 August 2002).

Huitema, Christian. Routing in the Internet. Upper Saddle River: Prentice Hall PTR, 2000. 55-81.

Information Sciences Institute. “RFC 791 Internet Protocol.” 1 September 1981. URL: ftp://ftp.isi.edu/in-notes/rfc791.txt (18 Aug 2002).

Kent, Stephen, and Randall Atkinson. “RFC 2401 Security Architecture for the Internet Protocol.” November 1998. URL: ftp://ftp.isi.edu/in-notes/rfc2401.txt (18 August 2002).

Kent, Stephen, and Randall Atkinson. “RFC 2402 IP Authentication Header.” November 1998. URL: ftp://ftp.isi.edu/in-notes/rfc2402.txt (18 August 2002).

Kent, Stephen, and Randall Atkinson. “RFC 2406 IP Encapsulating Security Payload (ESP).” November 1998. URL: ftp://ftp.isi.edu/in-notes/rfc2406.txt (18 August 2002).

King, Steve, et al. “White Paper IPv6.” July 1997. URL: http://www.cs-ipv6.lancs.ac.uk/ipv6/documents/papers/BayNetworks/ (18 August 2002).

© SANS Institute 2000 - 2005 Author retains full rights.

Mahmood, Raja Azlina Raja. “IPv6 Deployment in Malaysia: The issues and challenges.” SANS Institute Information Security Reading Room. 4 April 2002. URL: http://rr.sans.org/country/malaysia.php (28 August 2002).

Stallings, William. “IPv6: The New Internet Protocol.” April 1997. URL: http://www.cs-ipv6.lancs.ac.uk/ipv6/documents/papers/stallings/ (24 August 2002).

© SANS Institute 2000 - 2005, Author retains full rights.