IPV6 Security Enhancements Still Not Everything You Need

Bill Hancock
Network-1 Security Solutions Inc.

With all the hype about IPV6 starting to finally come to some levels of fruition, there comes the hype about IPV6 security. Yes, it is true that there are some optional security facilities in IPV6. It is also true that they greatly improve security of a connection, overall, if used. But, before you get too excited or complacent (depending upon your mindset) about the facilities, it's a good idea to know what, exactly, the facilities are and the fact that they will not solve all the security problems that are encountered on IPV6 networks.

IPV6 includes the ability to support an authentication header (AH) method as well as an MD5 authentication method and an encrypted data area called an encapsulating security payload (ESP) to encrypt information contained in an IPV6 datagram. Both of these functions may be used together or separately in various application requirements as deemed fit with the application using IPV6 for transport over a network.

Five Internet RFCs define the security functionality for IPV6 as follows:

1825 Security Architecture for the Internet Protocol

- 1826 IP Authentication Header (AH)
- 1827 IP Encapsulating Security Payload (ESP)
- 1828 IP Authentication Using Keyed MD5
- 1829 ESP DES-CBC Transform

For those not familiar with RFCs (request for comment) IETF documents, they may be retrieved from the Web site at the InterNIC at:

http://ds.internic.net/ds/rfc-index.1800-1899.htm>http://ds.internic.net/ds/rfc-index.1800-1899.htm

Basically, IPV6 provides two cryptographic mechanisms to move data between two systems as follows:

1. The Authentication Header (AH) method provides a cryptographic checksum to provide data integrity and source authentication. It is intended to provide integrity verification of information transmitted over public networks between two systems that require some method to ensure they are the originator and proper destination. It is also used to verify the size of the message and the integrity of the message (i.e. the message has not been modified in transit from the source to the destination in some manner). Finally, the AH also provides a non-repudiation function. By definition, a keyed MD5 method using a 128-bit secret key method is required, but other cryptographically strong algorithms such as SHA may be used. Conventional CRC-16 and CRC-32 checksums may not be used as they are not secure enough cryptographically to be trusted with integrity verification.
2. The Encapsulating Security Payload (ESP) provides IP datagram integrity and privacy of content. Depending upon the algorithm selected for the ESP, it may also provide authentication functionality. The ESP requires the use of Data Encryption Standard (DES) with Cipher Block Chaining (CBC), but other optional algorithms may also be provided such as the RC5 stream cipher. The ESP can encompass the entire IP datagram (this mode is called 'tunnel mode') or only the upper layer transport protocol (called 'transport mode'). ESP with AH functionality means that the message is subject to session hijacking and packet fragmentation. Also, AH and ESP functionality do not provide any levels of access control, filtering, traffic analysis attack profiles and other types of attacks that may be encapsulated in a message between systems utilizing AH and/or ESP facilities.

All security functions described above when used between trusted facilities encompass an overall scheme known as IPSEC. This technology is commonly deployed for Virtual Private Network (VPN) facilities under

IPV4 as well as IPV6.

Of concern at this writing is a lack of definition of a key exchange method that is common to both IPV6 components. Under consideration are:

- Qualcomm's Photuris. A session-based key management protocol, it supports frequent exchange of limited lifetime individual session-keys by an unpredictable number of other nodes with a minimum of configuration, support for a variety of authentication methods, defeat certain types of denial-of-service attacks on hosts and do all with a minimum of computational loading with minimal network traffic levels.

- Sun Microsystems SKIP. Simple Key Management for Internet Protocols (SKIP) is a connection-less key management protocol which requires no prior communication for key management functionality. Each participating host must have a certified public key (static key paradigm). If the keys are compromised, all previous traffic can be exploited. SKIP also requires an automated distribution of authenticated public keys using a certificate delivery protocol (CDP) which allows node-to-node support or certificate server support for key distribution and control. An advantage is the support of many different types of certificate authorities (X.509, hashed public keys, secure DNS resource records, etc.).

- National Security Agency ISAKMP. Internet Security Association and Key Management Protocol (ISAKMP) basic facilities guard against denial-of-service, replay/reflection, man-in-the-middle and connection hijacking attacks. It does not require specific cryptographic algorithms, key generation techniques or other security mechanisms. It's more of an architecture than specific definition of algorithms, keys and methods. This works both for and against it.

The IETF is still working with the above although ISAKMP seems to be winning at least the political war. Current information is usually kept in the IETF minutes on IPSEC at:

http://www.ietf.crni/reston.va.us/ids.by.wg/ipsec.htm>http://www.ietf.crni/reston.va.us/ids.by.wg/ipsec.htm

So now that you have a basic understanding of what IPV6 offers in the way of security, how is it used? Basically:

- Virtual Private Networks. The combination of AH and ESP with proper key distribution methodology allows the use of either tunnelling IP VPNs or transport-specific IP VPNs. By using the same authentication and encryption of payload methods, interoperability of dissimilar packages offering similar services is possible (this will take some additional work on the RFC, but it is not unimaginable at this stage).

- Application-independent data security. Currently, use of SSL, SHTTP and other types of session cryptographic methods are limited to those applications specifically coded to support the specific techniques used. With ESP at the transport level, general-purpose cryptographic solutions are available to any application on the supported transport protocols or via tunnelled session between cooperating systems.

- Authenticated source and destination in communications dyads. One of the more persistent security problems with nodes, transports and applications is knowing, exactly, who is on the other end of the dyad being established at various levels of the protocol suite. Using AH and certain types of ESP facilities, it will be clear as to what is at each end of a dyad and a connection of trust can be established.

And, while all the above is noble, needed and good, there is bad news as well. IPV6 facilities do not solve security problems such as:

- Filtering of content of any level of the protocol stack. There are no filtering facilities in the proposed solutions similar to those found in routers and firewall facilities.

- Trusted attack defeat. If the attacker is internal, the proper keys and facilities will be available to the attacker and the security features will not help. Remember that almost any study on who does the attacking in a network still pinpoints internal attacks as the most common. If the attacker is a valid participant in the network, IPV6 facilities do not stop them from attacking.

- Denial-of-service attacks. While some recommendations for IPV6 key exchange provide for denial-of-service defeats in key exchange, they

do not do anything about other IP denial-of-service attacks nor do they help with generalized packet 'clogging' attack techniques.

- Stateful attacks. There are still methods to attack a session in a stateful manner if the AH facilities are not used in conjunction with ESP or other solutions.

- Logging and accounting. These facilities are critical to evidence gathering and information analysis of potential attacks. None of the IPV6 facilities provide for logging of activities and accounting of user, session, component, application or other traffic generating or receiving facilities.

Of course, there are other methods to attack the facilities as well as other manners in which to use IPV6 facilities to defeat attacks. The illustration above serves, however, to show that there is not an all-encompassing approach in the offerings in IPV6 and customers should be careful to temper their enthusiasm with the reality of what the facilities can and cannot accomplish (properly implemented, of course).

Overall, IPV6 security facilities dramatically improve connection security, but the main items to remember are that they are not all-encompassing and lack many specific security facilities and logging facilities critical to overall security management. And, while many vendors are offering the facilities retrofitted to IPV4, they still require many other security technologies to properly secure network connectivity and session connections.

Meta-Firewall: A Sixth Generation Firewall — Part 1

Oliver Lau

Terminology in the firewall area is still confusing. Proxies, packet filters, 'stateful' filters, hybrid approaches, fifth generation firewalls and many more rule the market, and thus rule the user's mind of what is good and what is bad. But few people (1) have thought about the relationships between all those technologies, how they can interact, and how they can be integrated to increase security on a perimeter network to a maximum. Let us call this approach a 'meta-firewall', designed to provide maximum security for dedicated purposes. All of the issues involved in planning for a solution for any network cannot be discussed, but it is an approach to a new way of thinking what can be done with firewalls and the like. The first part of this two-part article begins to build the layers of security in a firewall for an imaginary company.

What exactly is a firewall?

A firewall is any component that is capable of controlling and filtering traffic between at least two networks. As such, a firewall is both ingress and egress, depending on the side you are looking at it. When the term 'firewall' is addressed throughout this article it is in the sense of a dual-homed gateway (i.e. the firewall could be attached to only two networks) controlling traffic between a trusted and an untrusted network, where the trusted network mostly is the corporate network or a local area network, and the Internet mostly belongs to the untrusted side.

Although arguing based on an analogy could be dangerous, because it could lessen the accuracy of the real situation, here is a trial on firewall concepts: firewalls are the doors between networks, meticulously controlled by doorkeepers (the filtering engines), who look at you, inspecting your ID card, asking you where you want to go, where you come from and whom do you want to talk to, and either say, "Ok, you may pass!" or, "Stop, access prohibited!".

Some of the doorkeepers are really dumb, they can't remember if you have already entered or not. Others are 'stateful', e.g. when they see you twice attempting entrance without exiting, this is not allowed and you are refused. A third group of doorkeepers would never let you pass, instead they ask you for your message and whom it should be delivered to,