Global Information Assurance Certification Paper

Robert Buckley

Ipv6: Improvements and Security

IPV6 or Ipng (next generation) is the proposed new standard for the Internet Protocol. It is the intention of this research paper to briefly discuss some of the important changes, and security features of IPV6.

History:

Let's take a historical view of the Internet Protocol. In 1969, Arpanet was created. It was a packet switched network built for the U.S Department of Defense. It started as four nodes originally, and by the end of the 1970's had spanned across many systems in the US as well as systems in Europe and Asia as well. The primary use for Arpanet was by R&D and educational facilities. By the 1990's many commercial users discovered the Internet and its usability. By January of 1997 the number of hosts on the Internet was over 16 million, with more than 100,000 networks worldwide. Work started on IPV6 in 1991 and several IPV6 proposals were subsequently drafted. The result of this effort was IP version 6 (Ipv6), described in RFCs 1883-1886; these four RFCs were officially entered into the Internet Standards Track in December 1995. [8]

IPV6 addressing versus IPV4 Limitations

Our current IP version is Ipv4 and uses a 32 bit addressing scheme. As the use of the internet grows exponentially, it is valid to assume that using a 32 bit addressing scheme will not support the demand for address space. Granted there are many possible addresses, but with the partitioning of this address space into A,B,C and D classes we are already falling short of C addresses, which represent the most needed network size. While it is possible to work around this limitation by subnetting larger classes into class C networks, it is not a viable solution to the increasing demand for IP addresses.

In principle it is possible to assign 232 different addresses, i.e., over 4 billion possibilities. However, the inefficient use of the address space by IPV4 is wasting a large number of these addresses. Class networks have fixed boundaries between the identification of each network and the identification of each node. Once a network number is assigned to a network, all of the host addresses for that network are assigned to that network. For example if a network needed 400 addresses it cannot use a class C address which has only 256 addresses, rather it must use a class B address which has 65,536 addresses. Since this network would only use 400 of the 65,536 addresses, the remaining 65,136 addresses are considered wasted since no other network could use these addresses.

The inefficient use of the address space and the rapid increase in IP addresses demand lead some experts to anticipate that the Ipv4 addresses will run out around the year 2010. To ensure the availability of an adequate supply of IP addresses, IPV6 uses a 128-bit address. In theory, it can address 2^128 interfaces. It is assumed that IPV6 could address between 8*10^17 and 2*10^33 nodes. Using the lowest estimation, 1,564 addresses would be available for every square meter of the planet Earth's surface. [6]

Ipv4 Compatibility

Ipv6 has the ability to emulate the packet design of Ipv4. This allows for interoperability between the two designs without causing a multitude of network changes because of a new IP implementation. Both Ipv4 and Ipv6 can co-exist peacefully without additional requirements. Ipv6 also allows its packets to be "tunneled" through existing Ipv4 networks. This feature allows network administrators to phase Ipv6 routing equipment and use today's existing Ipv4 Internet as a routing path to connect their Ipv6 networks.

Ipv6 Security

In the early days of TCP/IP, the ARPANET user community was small and close, and security mechanisms were not of primary concern. As the number of TCP/IP hosts grew, and the user community became one of strangers (some nefarious) rather than friends, security became more important. As critical and sensitive data travels on today's Internet, security is of paramount concern. Although many of today's TCP/IP applications have their own security mechanisms, many would argue that security should be implemented at the lowest possible protocol layer. Ipv4 had few, if any, security mechanisms, and authentication and privacy mechanisms at lower protocol layers is largely absent. Ipv6 builds two security schemes into the basic protocol.

The first mechanism is the IP authentication Header referred to as AH (RFC 1826), an extension header that can provide integrity and authentication for IP packets. The Ipv6 Authentication Header (AH) provides integrity and authentication for Ipv6 datagrams by computing a cryptographic authentication function over the Ipv6 datagram and using a secret authentication key in this computation. The sender computes the authentication data for static fields just prior to sending the authenticated Ipv6 packet and the receiver verifies the correctness of the authentication data upon reception. Non-repudiation might be provided by some (e.g. asymmetric) authentication algorithms used with the Authentication Header. The default authentication algorithm is keyed MD5, which like all symmetric algorithms cannot provide non-repudiation. Confidentiality and traffic analysis protection are not provided by the AH as the IPV6 datagrams are not encrypted. Although many different authentication techniques will be supported, use of the keyed Message Digest 5 (MD5, described in RFC 1321) algorithm is required to ensure interoperability. Use of this option can eliminate a large number of network attacks, such as IP address spoofing. As IP is located at the Internet layer, it helps to provide host authentication. This will also be an important addition to overcoming some of the security weaknesses of IP source routing. In contrast, IPV4 provides no host authentication. All Ipv4 can do is to supply the sending host's address as advertised by the sending host in the IP datagram. Placing host authentication information at the Internet Layer in Ipv6 provides significant protection to higher layer protocols and services that currently lack meaningful authentication processes.

The second mechanism is the IP Encapsulating Security Payload (ESP, described in RFC 1827), an extension header that can provide integrity and confidentiality for IP packets. Like authentication header, ESP is cipher independent. Although the definition is algorithm-independent, the Data Encryption Standard using cipher block chaining mode (DES-CBC) is specified as the standard encryption scheme to ensure interoperability. The Ipv6 Encapsulating Security Payload (ESP) provides integrity, authentication, and confidentiality for Ipv6 datagrams by encapsulating either an entire

Ipv6 datagram or only the upper-layer protocol data inside the ESP, encrypting most of the ESP contents, and finally a new cleartext IPV6 header is appended to the ESP. The recipient of the datagram removes and discards the cleartext Ipv6 header and options, decrypts the ESP, processes and removes the ESP headers, and then processes the data as normal. The ESP mechanism can be used to encrypt an entire IP packet (tunnel-mode ESP) or just the higher layer portion of the payload (transport-mode ESP).
These features will add to the secure nature of IP traffic while actually reducing the security effort; authentication performed on an end-to-end basis during session establishment will provide more secure communications even in the absence of firewall routers. Some have suggested that the need for firewalls will be obviated by widespread use of Ipv6, although there is no evidence to that effect yet. [4]

IPV6 and Keys
"All Ipv6 implementations must support manual key management and should support an Internet standard key management protocol once it is approved. All IPV6 implementations must permit the configuration and use of user-to-user keying for traffic originating at that system and may additionally permit the configuration of host-to-host keying for traffic originating at that system as an added feature to make manual key distribution easier and give the system administrator more flexibility". [1]

"A device that encrypts or authenticates Ipv6 packets originated on other systems, for example a dedicated IP encryptor or an encrypting gateway, cannot generally provide user-to-user keying for traffic originating on other systems. Hence, such systems must implement support for host-to-host keying for traffic originating on other systems and may implement support for user-to-user keying for traffic originating on other systems. The method by which keys are configured on a particular system is implementation-defined". [1]

Summary

The need for change from the Ipv4 implementation is obvious. It is already quickly running out of address spaces and would be virtually dead in the water in the next decade. Ipv4 lacks security methods and it is the intention of the next generation ip to fix both addressing issues and security.

Using a 128 bit addressing scheme and better heirarchy design, it is possible to conceive well over 1000 addresses per every square meter of the Earth's surface.

Using newly designed headers (Authentication Header and Encapsulating Security Payload) will allow for data confidentiality, integrity, harder traffic analyses, encryption, and authentication. Although the common DES cipher doesn't provide a mechanism for non-repudiation, it is there only for interoperability. Other ciphers may be implemented to provide non-repudiation.

Ipv6 is backwards compatible with Ipv4 in the sense that it can operate simultaneously on a system with no intervention needed. Ipv6 networks can use the existing Ipv4 infrastructures to "tunnel" to other Ipv6 networks.

References:

[1] Randall Atkinson. Security Architecture for the Internet Protocol, Internet Draft, RFC 1825, Aug 1995 URL: http://www.faqs.org/rfcs/rfc1825.html
[2] Markku Korhonen Tik- 110.551 Internetworking Seminar Department of Computer Science Helsinki University of Technology URL: http://www.tml.hut.fi/Opinnot/Tik-110.551/1996/keymgmt.html
[3] S. Deering, S. Hinden. Internet Protocol, Version 6 (Ipv6) Specification, RFC 1883, Dec 1995
[4] http://sunsite.auc.dk/RFC/
[5] Reto E Haeni The George Washington University Washington DC January 1997
[6] C. Huitems, The H Ratio for Address Assignment Efficiency, RFC 1715, November 1994 URL http://www.faqs.org/rfcs/rfc1715.html
[7] Jim Bound Ipv6 – The Coming "Big Bang" in Cyberspace URL: http://www.sal.ksu.edu/faculty/fld/ipng.htm
[8] Gary C Kessler – Ipv6 The Next Generation Protocol URL: http://www.vtac.org/Tutorials/ipv6_exp.html

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS