Previous Articles

Email This Article | Subscribe To CircleID

Overcoming IPv6 Security Threat

September 12, 2002 | By Joe Baptista | Article Feedback

Technology rags and industry pundits see IPv6 (Internet Protocol version 6) as the future of networking, but Daniel Golding a participant of the North American Network Operators' Group (NANOG) thinks it's a "solution in search of a problem". Many others have argued IPv6 is a problem in itself and it is unlikely the protocol will gain wide acceptance in the short term.

IPv6 does solve many of the problems with the current version of IPv4 (Internet Protocol version 4). Its purpose is to expand address space and fix the IPv4 address depletion problem, which many techies claim, was due to mismanagement. The industry's goal is to use the very large address allocation pool in IPv6 to expand the capabilities of the Internet to enable a variety of peer-to-peer and mobile applications including cellular phone technology and home networking.

IPv6, a suite of protocols for the network layer, uses IPv4 gateways to interconnect IPv6 nodes and comes prepackaged with some popular operating systems. This includes almost all Unix flavors, some Windows versions and Mac OS. Some vendors offer upgrades to older operating systems. Trumpet Software International in Tasmania Australia manufactures a Trumpet Winsock version that upgrades old Windows 95/98 and NT systems to the current IPv6 standard.

IPv6 has suffered bad press over privacy issues. Jim Fleming, the inventor of IPv8, a competing protocol, sees many hazards and privacy flaws in existing IPv6 implementations. IPv6 address space in some cases
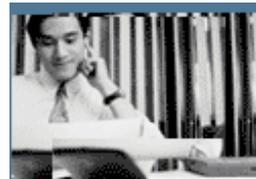
uses an ID (identifier) derived from your hardware or phone "that allows your packets to be traced back to your PC or cell-phone" said Fleming. Potential abuse to user privacy exists as a hardware ID wired into the IPv6 protocol can be used to determine the manufacturer, make and model number, and value of the hardware equipment being used. Fleming warns users to think twice before they buy themselves a used Laptop computer and inherit all the prior surfing history of the previous user!

IPv6 uses 128 bits to provide addressing, routing, and identification information on a computer interface or network card. The 128 bits are divided into the left 64 and the right 64. Some IPv6 systems use the right 64 bits to store an IEEE defined global identifier (EUI64). This identifier is composed of company id value assigned to a manufacturer by the IEEE Registration Authority. The 64-bit identifier is a concatenation of the 24-bit company identification value and a 40-bit extension identifier assigned by the organization with that company identification assignment. The 48-bit MAC address of your network interface card may also be used to make up the EUI64.

In the early stages of IPv6 development, Bill Frezza a General Partner with the venture capital firm, Adams Capital Management warned software developers that if privacy issues are not properly addressed, the migration to IPv6 "will blow up in their face"! Leah Gallegos agrees that while "expanding the address space is necessary the use of the address for ID and tracking is horrific". Gallegos the operator of the top-level domain .BIZ and a Director of the Top Level Domain Association cautions network administrators that they should refuse to implement IPv6 unless these issues are properly addressed.

Privacy concerns prompted the creation of new standards, which provide privacy extensions to IPv6 devices. Thomas Narten and Track Draves of Microsoft Research published a procedure to ensure privacy of IPv6 users. Narten, IBM's technical lead on IPv6 and an Area Director for the Internet Engineering Task Force (IETF), agrees "IPv6 address can, in some cases, include an identifier derived from a hardware address". But Narten points out that a hardware address is not required. "In cases where using a permanent identifier is a problem", said Narten "RFC 3041 addresses should be used".

RFC 3041 titled "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" was published this

past January 2001 by the IETF. It is an algorithm developed jointly by Narten and Draves which generates randomized interface identifiers and temporary addressees during a user session. This would eliminate the concerns privacy advocates have with IPv6.

Unfortunately RFC 3041 is not widely implemented. But Narten expects major vendors to incorporate his privacy standard and offered that Microsoft implemented privacy extensions "and apparently intends to make it part of their standard stuff". Narten also assisted in the drafting of recommendations for some second and third generation cellular phones recently approved for publication by the Internet Engineering Steering Group. That document recommends that RFC 3041 be implemented as part of cellular phone technology but he did not know what direction cell phones manufacturers were taking. "I suspect that client vendors will generally implement it because of the potential bad PR if they don't" said Narten.

Another obstacle raised by NANOG operators is that there is currently no commercial demand for IPv6 at this time. Dave Israel, a Data Network Engineer and regular participant on NANOG lists, sees no immediate demand for IPv6 services. "The only people who ask me about IPv6", said Israel "are people who have heard something about it from some tech-magazine and want the newest thing". Israel says he sees no commercial demand for a v6 backbone.

Daniel Golding, another NANOG participant agrees, "v6 deployment is being encouraged by some countries, and the spread of 3G (cellular technology) is helping things along, but we have yet to see really widespread v6 deployments anywhere". Golding sees major backbone networks deploying IPv6 when it makes economic sense for them to do so. "Right now", said Golding "there is no demand and no revenue upside. I don't expect this to change in the near future".

Most on NANOG agree the roadblock seems to be a lack of ISPs that offer IPv6 services. Stephen Sprunk, a Network Design Consultant with Cisco's Advanced Services group sees the "greater adoption of always-on broadband access will be the necessary push" to get IPv6 off the ground. "Enterprise networks will not be the driver for ISPs to go to IPv6" said Sprunk and "NAT is too entrenched". Network Address Translation (NAT) is a method of connecting multiple computers to the Internet (or any other IP network) using one IPv4

address.

Vint Cerf senior vice president of architecture & technology at WorldCom has been using IPv6 for about four years. IPv6 has been a key element for some of WorldCom's Government customers. Cerf thinks IPv6 supporters have a lot of work ahead to achieve successful deployment of the protocol. He expects "that over the next several years we will see a lot of consumer devices set up to work with IPv6" and "cell phones are likely candidates, as are radio-enabled PDAs".

....

Joe Baptista is a founding member of Planet Communications & Computing Facility, a not for profit provider of network infrastructure, domain name and internet research services. Joe is also involved in internet governance as a member of the General Assembly of the Domain Name Supporting Organization (DNSO) of The Internet Corporation for Assigned Names and Numbers (ICANN). Joe has been interviewed by the leading Canadian newspapers, radio and television on various internet issues.

Interested in submitting your articles? Learn More
Please send us your Feedback & Error Reports. Thank You.