



[CIO/CTO Perspective](#)
[Policy and Regulation](#)
[Defense in Depth Security](#)
[Business Insights](#)
[Voice and Collaboration Solutions](#)
[IP Solutions](#)

[Virtualization & On-Demand](#)

Home » Blogs » lippard's blog

IPv6 Security Considerations



Thu, 06/09/2011 - 14:30 | by [Jim Lippard](#)

Mark Newton of Internode gave an excellent talk on IPv6 transition and security in May at AusCERT 2011, the conference of the Australian Computer Emergency Response

Team. The talk, based on his experience in making a fairly rapid transition to a dual-stack configuration for Internode across its network and services, he recommended planning now and transitioning early if you can, in a piecemeal fashion starting from the perimeter and working in, making sure that you maintain equivalence between IPv4 and IPv6 configurations wherever possible.



Like 7

9

His talk covers IPv6 basics and some of the caveats to watch out for, and also provided a very nice list of security-related issues:

There is no longer RFC 1918 private address space, all hosts have public addresses.

There is no NAT; peer-to-peer reachability is assumed. (Newton rightly said that you should consider what you're trying to achieve with NAT, but I think he dismissed it a bit too glibly as security through obscurity, perhaps a topic for a future blog post.)

Intrusion Detection support for IPv6 is limited; there are no Deep Packet Inspection vendors currently supporting IPv6. [Snort does support IPv6.]

You need to make sure you put IPv6 access lists on your router VTYs when you deploy IPv6.

Vulnerability scanning across your entire network is no longer possible in IPv6. This doesn't make much difference to the bad guys, who have alternative ways of finding hosts to compromise, but means that you also can't rely on scanning IPs in sequence to monitor your own vulnerabilities. (See [RFC 5157](#).) Newton noted that this seems to entail that an IPv6 network cannot be PCI compliant (since requirement 11.2 requires external and internal network scans quarterly and after every significant network change).

The EUI-64-based IPv6 addresses assigned by stateless auto-configuration are effectively a tracking token for systems. This may be a positive thing in a corporate environment, and can be changed either on the network side by using stateful configuration (e.g., with DHCPv6) or on the host side by using [RFC 4941](#) privacy extensions (which are enabled by default on Windows systems, and easily enabled in Mac OS X and Unix-like systems via sysctl). The privacy extensions cause temporary randomly generated interface identifiers to be generated instead of using EUI-64.

It's possible for any host to issue a router announcement (similar to the issues surrounding rogue DHCP announcements), unless your switch is filtering with RA Guard (see [RFC 6105](#)). (More below.)

If you're currently filtering ICMP, you probably need to change how you're doing it. ICMP is much more important in IPv6, with neighbor advertisements and solicitations replacing ARP. See [RFC 4890](#) for filtering considerations for ICMP in IPv6.

Newton also gave two examples of security issues that can arise for you even if you are not currently transitioning to IPv6:

You may already have hosts bypassing firewalls by tunneling IPv6 out of your network using ISATAP, 6in4, 6to4, or Teredo tunnels to IPv6 gateways. (The first three of these use protocol 41, the last uses outbound UDP on port 3544 to set up the tunnel.)

As mentioned above, it is possible for a rogue host to inject fake IPv6 router announcements. Combined with stateless address auto-configuration (SLAAC), this makes possible a [man-in-the-middle "SLAAC attack" on an IPv4-only network using IPv6, which can be introduced into a network with a tiny piece of hardware.](#)

In short, whether you're planning to transition to IPv6 now or not, you need to pay attention to the potential for IPv6 security vulnerabilities now because of these last two points. When you do start your transition to IPv6, you need to account for the differences from IPv4 and make some adjustments to make sure you place equivalent controls in place for IPv6, since failure to maintain equivalence creates a hole.

Follow Global Crossing



Subscribe to our Level 3 Blog



Languages

English

Search

Search

Connect on Facebook

Like

Greg Pendergrast, Montgomery Scott and 1,809 others like this.



Cloud Services Suite

Click Again for Full Screen

User login

Username: *

Password: *

Log in

[Log in using OpenID](#)

[Create new account](#)

Newton's talk goes into more detail than I've given here and is well worth a listen. Check it out [here](#) and let me know what you think in the comments.

(Also see Karl Kasarda's blog post on "5 Things to Consider When Migrating Your Web Presence to IPv6.")

Additional Resources:

Rob Rachwald, "IPv6 Security: Should We Be Concerned?", Imperva Security Blog (Spanish & English posts)

Danny McPherson, "8 Security Considerations for IPv6 Deployment," CircleID blog

"Some talks about IPv6 security," Fernando Gont's blog

Joe St. Sauver, "If We Deploy IPv6, Will It Help or Hurt Our Security?"

Like  and 1 other liked this.

Add New Comment

[Login](#)



Type your comment here.

Showing 2 comments

Sort by oldest first



MatthewRay

Testing



MatthewRay

test
2

[M](#) [Subscribe by email](#) [S](#) [RSS](#)

Trackback URL

[Jim Lippard's blog](#)

Tags: [Defense in Depth Security](#) [concerns](#) [IPv4](#) [IPv6](#) [IPv6 Security](#) [Security](#) [SLACC](#) [Vulnerability](#) [World IPv6 day](#)

[Request new password](#)

Recent blog posts

[Global Crossing Genesis Solutions International Events Part 2 of 2 - "Operationalizing the deal"](#)
[Global Crossing Genesis Solutions International Events Part 1 of 2 "Winning the deal"](#)
[IPv4 Addresses for Sale? Recap at IBC 2011 - Global Crossing Genesis Solutions Regional and global bandwidth expansion boom](#)
[Tips to prevent voice communications systems fraud](#)
[PSN Cost Savings in the UK Government Sector](#)
[Advanced Cyber Attacks Require Sophisticated Technology](#)
[Application management on Data Center critical environments](#)
[Crowning glory for Global Crossing \(UK\) Telecommunications Limited](#)

[more](#)



Legal Disclaimer

Disclaimer: Opinions expressed here and in any corresponding comments are the personal opinions of the original authors, and do not necessarily reflect the views of Global Crossing. The content is provided for informational purposes only and is not meant to be an endorsement or representation by Global Crossing or any other party. This site is available to the public. No information you consider confidential should be posted to this site. By posting you agree to be solely responsible for the content of all information you contribute, link to, or otherwise upload to the Website and release Global Crossing from any liability related to your use of the Website.