Security Implications of IPv6 on IPv4 Networks

(draft-gont-opsec-ipv6-implications-on-ipv4-nets)

Fernando Gont

SI6
NETWORKS

IETF 84
Vancouver, Canada. July 29-August 3, 2012

Overview

- Common claim/assumption:

  “*I don't need to worry about IPv6 security – my network is IPv4 only!*”

- Truth is:
  - Most networks have **at least partial deployment of IPv6**
  - Hence, **one does need to worry about IPv6 security for “IPv4-only” networks**

Common/general issues

- IPv6-specific vulnerabilities might be exploited
- IPv6 could be leveraged to circumvent security controls
- Transition technologies might increase host exposure

*-opsec-ipv6-implications-on-ipv4-nets

- Raises awareness about the security implications of IPv6 on “IPv4-only” networks
- Provides concrete advice to mitigate them

Security Implications of Native IPv6 Support

Overview

- Even with no infrastructure support, local hosts may communicate with IPv6 link-local addresses
  - This may allow attackers to circumvent controls
  - May enable exploitation of IPv6-specific vulnerabilities
- Global connectivity might be enabled with rogue routers
  - And then leveraged for the same purpose

Possible mitigations

- Filter IPv6 packets at layer-2 (Ethernet Protocol 0x86dd)
- Mitigate SLAAC, DCHPv6, and ND attacks with:
  - RA-Guard
  - DHCPv6-Shield
  - ND-Shield
- Enforce IPv6 controls on your “IPv4” network
- In specific environments (e.g. military) you may want to completely disable IPv6 support in communicating devices

Security Implications of Tunneling Mechanisms

Overview

- They might introduce tunnel-specific vulnerabiities
  - e.g. think about Nakibly et al's “automatic-tunnel loops”
- They might be leveraged to circumvent security controls
- Some (notably Teredo) might inadvertently increase host exposure
  - e.g. allow incoming connections through a NAT-PT

Mitigations

- Enforce a “default deny” policy for tunnels
  - Most can be blocked by filtering IP Proto 41
  - Others can be trickier (e.g. TSP and Teredo)
- Enforce tunnel-aware security controls (NIDS, firewalling, etc.)

Moving forward

- Adopt as wg item?

Thanks!

Fernando Gont

fgont@si6networks.com

www.si6networks.com