NIST SP 800-119 Guidelines for the Secure Deployment of IPV6

Recommendations and Updates

Sheila Frankel

Computer Security Division

NIST

sheila.frankel@nist.gov

SP 800-119 Goals

- To educate the reader about IPv6 features and their security impacts
- To provide a comprehensive survey of IPv6 deployment mechanisms
- To provide a suggested deployment strategy for secure IPv6 deployment

IPv6 Security Challenges

- Active, experienced attacker community
- Unknown/unauthorized IPv6 assets on existing IPv4 networks
- Complexity/unexpected interactions between IPv4 and IPv6
- IPv6 protocols' continued development, immaturity
- Proliferation of transition-driven tunnels
  - Complicate network boundary defense
  - Penetrate Network

Terminology

- Transition
- Adoption
- Deployment

Addressing

- Assign random subnet and interface IDs
- Apply different types of IPv6 addressing (privacy, unique local, sparse allocation)
- Use automated tool
- DHCPv6 is now widely implemented
- FISMA system boundaries
  - "Be aware that switching from a NATted address environment to unique global IPv6 addresses **could** trigger a change in the FISMA system boundaries."

DNS

- Different names for IPv6-enabled hosts
  - Address selection issues
  - Application failure
- Premature AAAA record insertion

IPsec

- “Use IPsec to authenticate and provide confidentiality to assets that can be tied to a scalable trust model”
- Added new RFCs
- AES-XCBC
- IP compression

Network Protection Devices (NPDs)

- "Enable controls that might not have been used in IPv4 due to a lower threat level during initial deployment (implementing default deny access control policies, implementing routing protocol security, etc)."
- Granular ICMPv6 filtering policy
  - Required by USGv6 Profile (NIST SP 500-267)
  - Not currently available in all devices

ICMP firewall filtering (Table 3-7)

- Allow non-local associated with allowed connections
  - Maintenance of communications
  - Error messages
- Allow/disallow non-local based on topology/information concealment policy
  - Echo request/response

ICMP firewall filtering (Table 3-7) (cont'd)

- Allow in link-local traffic only
  - Address configuration and router selection
  - Link-local multicast receiver notification
  - SEND messages
  - Multicast router discovery (MLD)
- Allow non-local for predefined endpoints
  - Mobile IPv6 (MIPv6)
- Removed Table 3-8
  - Experimental/unallocated messages

Further Information

- Website:
  - http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf
  - Contact: sheila.frankel@nist.gov