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

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


# SP 800-119 Topics

- Introduction
  - IPv4 Limitations
  - IPv4 and IPv6 Threat Comparison
  - IPv6 Benefits/Advances
- IPv6 Overview
  - Addressing/Address Allocation
  - Headers/Extension Headers
  - ICMP
  - Routing
  - DNS


# SP 800-119 Topics
(cont'd)

- IPv6 Advanced Topics
  - Multihoming
  - Multicast
  - Quality of Service (QoS)
  - Mobile IPv6 (MIPv6)
  - Jumbograms
  - DHCP
  - Renumbering


# SP 800-119 Topics
(cont'd)

- IPv6 Security Advanced Topics
  - Privacy Addresses
  - Cryptographically Generated Addresses (CGAs)
  - Secure Neighbor Discovery (SeND)


# SP 800-119 Topics
(cont'd)

- IPv6 Deployment: Select Topics
  - Security Risks
  - Secure Address Management
  - Transition Mechanisms
  - Dual Stack
  - Tunneling
  - Translation
  - Other Transition Mechanisms
  - Security-Related Planning


# SP 800-119 Topics
(cont'd)

- IPv6 Deployment Process/Phases
  - Initiation Phase
  - Acquisition/Development Phase
  - Implementation Phase
  - Operations/Maintenance Phase
  - Disposition Phase


# 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


# Agencies not yet Deploying IPv6

- Block all IPv6 traffic
  - Native and tunneled
  - Inbound and outbound
- Acquire IPv6 expertise
- Set up IPv6-accessible web servers outside organizational firewall


# Agencies Beginning IPv6 Deployment

- Address Management
  - Develop strategy
  - Use automated tool
- Ensure parity of network protection devices
  - ICMP filtering
  - Deep packet inspection
  - Multicast scope boundaries


# What is IPsec?

- Security provided at the Internet layer of communications
- Provided by security headers
  - Encapsulating Security Payload (ESP)
  - Authentication Header (AH)
- Dynamic negotiation, update and management of symmetric secret keys
  - Internet Key Exchange (IKE)
- Optional for IPv4, mandatory for IPv6


# IPv6 Myths (or partial truths)

- Restoration of end-to-end communications
  - Topology-defined network
  - Policy-defined network
- The end of NAT (Network Address Translation) boxes
- IPsec is the “silver bullet”


# Further Information

- Website:
  - http://www.antd.nist.gov/usgv6/
- Contact:
  - sheila.frankel@nist.gov