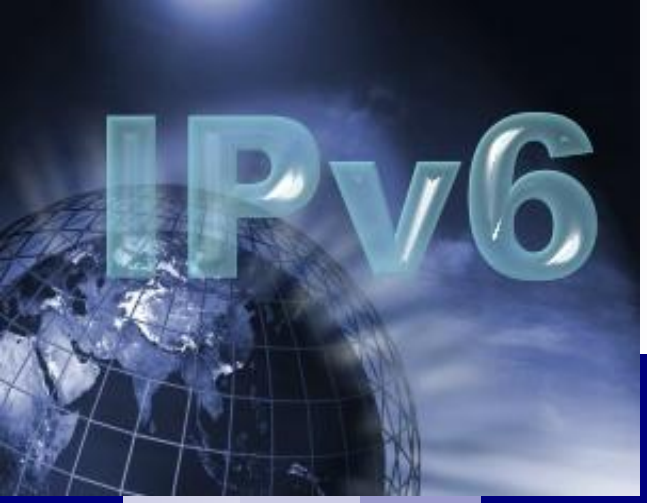

Secure Deployment of IPv6

Sheila Frankel

Computer Security Division

NIST

sheila.frankel@nist.gov

Background

- Defined by the Internet Engineering Task Force (IETF: www.ietf.org)
- Internet Drafts (IDs)
- Requests for Comment (RFCs)

Background (cont'd)

- Current working groups
  - IPv6 Maintenance (6man): 7 RFCs, 13 IDs
  - IPv6 Operations (v6ops): 36 RFCs, 11 IDs
  - Mobility Extensions for IPv6 (mext): 8 RFCs, 3 IDs
  - IPv6 over Low power WPAN (6lowpan): 2 RFCs, 4 IDs
  - Site Multihoming by IPv6 Intermediation (shim6): 3 RFCs, 2 IDs
  - Behavior Engineering for Hindrance Avoidance (behave): 13 RFCs, 10 IDs
  - IP Security Maintenance and Extensions (IPsecME): 10 RFCs, 2 IDs

Background (cont'd)

- Concluded working groups
  - IP version 6 (IPv6): 83 RFCs, 2 IDs
  - Mobility for IPv6 (MIP6): 16 RFCs, 10 IDs
  - MIPv6 Signaling and Handoff Optimization (mipshop): 14 RFCs, 3 IDs
  - Mobile Nodes and Multiple Interfaces in IPv6 (monami6): 3 IDs
  - Site Multihoming in IPv6 (multi6): 5 RFCs
  - Next generation transition (ngtrans): 15 RFCs
  - IPv6 Backbone (6bone)
  - IPv6 MIB (ipv6mib)
  - IP Security (IPsec): 43 RFCs, 3 IDs

Advantages

- Longer addresses
- Better address management (assignment, renumbering)
- Extensibility
- Flexible extension headers
- Device mobility
- Quality of service (QoS)
- IPv4 operational experience/new technology
- Increased security: IP security (IPsec)

US Government IPv6 Directives:

Office of Management and Budget (OMB)

- OMB Memo, August 2005
  - Agencies: “backbone” using IPv6 by June 2008
  - NIST: develop standard for USGv6 compliance
- OMB Memo, September 2010
  - External servers: native IPv6 by September 2012
  - Internal applications that communicate with public servers and their supporting enterprise networks: native IPv6 by September 2014

US Government IPv6 Directives:

General Services Administration (GSA)

- IPv6 Federal Acquisition Regulation (FAR)
- Published in Federal Register, July 2010
  - *Unless the agency Chief Information Officer waives the requirement, when acquiring information technology using Internet protocol, the requirements documents must include reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST Special Publication 500–267) and the corresponding declarations of conformance defined in the USGv6 Test Program.*

NIST's IPv6 Program: Components

- USGv6 (U.S. Government IPv6) Profile
- USGv6 Test Program
- Guidance document

NIST IPv6 Guidance

- SP 800-119:

  Guidelines for the Secure Deployment of IPv6
  - Published December 2010
  - IPv6 Protocols and Features
    - General Description
    - Differences from IPv4
    - Security Ramifications
    - Unknown Aspects
  - Recommends stages/activities for deployment
  - http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

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, including SLAAC (Stateless Autoconfiguration)
  - Routing
  - DNS

SP 800-119 Topics
(cont'd)

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

SP 800-119 Topics
(cont'd)

- IPv6 Security Advanced Topics
  - Privacy Addresses
  - Cryptographically Generated Addresses (CGAs)
  - IPsec
  - Securing SLAAC
  - 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
  - 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

Terminology

- Transition
- Adoption
- Deployment

Transition

- Dual stack
- Tunneling
  - Manual or static
  - Automatic
  - IPv6-over-IPv4
  - IPv4-over-IPv6
- Translation
- Security/complexity challenges

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

Advantages of IPsec

- Implement once, in a consistent manner, for multiple applications
- Centrally-controlled access/security policies
- Enable multi-level, layered approach to security

Types of Security Provided by IPsec

- Data origin authentication
- Connectionless integrity
- Replay protection
- Confidentiality (encryption)
- Traffic flow confidentiality
- Access control

Types of Attacks Prevented by IPsec

- Address spoofing
- Replayed packets
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)
- Traffic analysis

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
- Lack of operational experience
- Proliferation of transition-driven tunnels
  - Complicate network boundary defense
  - Penetrate Network

Agencies not yet Deploying IPv6

- Block all IPv6 traffic
  - Native and tunneled
  - Inbound and outbound
- Disable IPv6 ports/protocols/services
  - Software and hardware
- Acquire IPv6 expertise
- Set up IPv6-accessible web servers outside organizational firewall

Addressing

- Address management
  - Develop strategy
  - Diverse address types: autoconfiguration, privacy, unique local, etc.
  - Use automated tool
- Address scanning no longer practical
  - Assign random subnet and interface IDs
- 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”
- Only use FIPS-approved cryptographic algorithms
- IP compression

Network Protection Devices (NPDs)

- Ensure parity of network protection devices
  - Deep packet inspection
  - Multicast scope boundaries
- “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)
- Block experimental/unallocated messages

IPv6 Myths (or partial truths)

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

NIST's USGv6 Profile and Testing Program

IPv6 Standards Profile

- NIST Special Publication (SP) 500-267:
  A Profile for IPv6 in the U.S. Government – Version 1.0
  - Published July 2008
  - Took effect 24 months after publication
  - http://www.antd.nist.gov/usgv6/usgv6-v1.pdf
- Basic functional requirements for IPv6 devices
  - Inventory of required standards (RFCs) and features
  - List of required features
  - Minimal operational requirements
- Descriptive Text and Table
  - Profiles general-purpose devices
  - Can be modified to satisfy specific requirements/constraints

IPv6 Standards Profile:

Device Categories

- Hosts
  - Any node that is not a Router.
- Routers
  - a Node that interconnects subnetworks by packet forwarding.
- Network Protection Devices (NPDs)
  - A device such as a Firewall or Intrusion Detection device that selectively blocks packet traffic based on configurable and emergent criteria.

IPv6 Standards Profile:

Functional Categories

- Basic Requirements (ICMP, PMTU, ND, Autoconfig)
- Addressing
- Routing (BGP, OSPF)
- Quality of Service (QoS)
- Transition Mechanisms (Dual Stack, Tunnels, GRE)
- Link Specific Capabilities
- IP Security (IPsec, IKE, Crypto Algorithms)

IPv6 Standards Profile:

Functional Categories (cont'd)

- Network Management (SNMP, MIB)
- Multicast (MLD, SSM, PIM)
- Mobility (MIPv6)
- Quality of Service (QoS)
- Application Requirements (DNS, URI, Socket API)
- Network Protection Device (NPD) Requirements

Sample Table Specification

		IP Security Requirements							
		IPsec-v3							
RFC4301		**Security Architecture for the IP**	PS	2005		M	M		2010/03
	4.1	Support of Transport Mode SAs			IPv4	M	c(M)		2010/03
	4.5.1	Manual SA and Key Management				M	M		2010/03
	4.5.2	Automated SA and Key Management				M	M		2010/03
RFC4303		Encapsulating Security Payload (ESP)	PS	2005	IPsec-v3	M	M		2010/03
RFC4302		Authentication Header (AH)	PS	2005	IPsec-v3	O	O		
RFC3948		UDP Encapsulation of ESP Packets	PS	2005	IPsec-v3	O	O		

Sample NPD Requirements

- IPsec Traffic Handling
  - Firewalls MUST either be capable of terminating IPsec connections (security gateways), or be capable of selectively blocking IPsec traffic.
- Tunneled Traffic Detection
  - Intrusion detection systems MUST be able to detect threat patterns even for tunneled traffic, when packet data contents may be embedded with multiple IP (v6/v4) headers. For tunneling methods for which content examination is not supported, it is sufficient merely to flag all such tunneled packets.

IPv6 Product Testing Program

- Open Process
  - Documents published for comment
  - Meetings with stakeholders
- NIST SP 500-273:
  USGv6 Test Methods: General Description and Validation
  - Guidance for Labs
  - Published November 2009
  - http://www.antd.nist.gov/usgv6/docs/NIST-SP-500-273.v2.0.pdf
- NIST SP 500-281:
  USGv6 Testing Program User's Guide
  - Guidance for vendors and purchasers
  - Published August 2010
  - http://www.antd.nist.gov/usgv6/docs/NIST-SP-500-281-v1.3.pdf

IPv6 Product Testing Program (cont'd)

- Initially sets "low bar"
  - Only test MUSTs
- Expected to "sunset" at some point

Types of Testing

- Conformance
- Interoperability
- (Security)
  - FIPS 140

Types of Labs

- 1st Party (Vendor)
- 2nd Party (Purchaser)
- 3rd Party (Independent fee-for-service)

Laboratory Accreditation

- Licensed Accreditor(s)
  - ISO/IEC 17011
  - International Laboratory Accreditation Cooperation (ILAC)
- Accredited Laboratories
  - ISO/IEC 17025
  - Develop testing, quality management procedures and documentation
- National Voluntary Laboratory Accreditation Program (NVLAP)

Test Methods

- Abstract Test Suite
- Based on IPv6 Forum test methods
- Used by accreditor to certify labs that will perform the testing
- Public and Open
  - NIST publishes test suites for public comment

Test Suites

- Developed or Acquired by Laboratories
- Bit-level compatability of tests across laboratories
- Resolution process

Conforming Products

- No Centralized Qualified Product List (QPL)
- Suppliers Declaration of Conformity (ISO/IEC 17050)
  - Identifies Testing Lab
  - Lists Optional Capabilities
- Rules for “derived products,” families of products
- Rules for “aging,” expiration of listing
  - Goal: to maximize interoperability

Further Information

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