



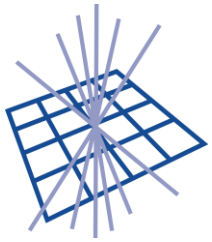
Science & Technology Facilities Council

# IPv6 Security

David Kelsey (STFC-RAL)

IPv6 workshop pre-GDB, CERN

7 June 2016



GridPP

UK Computing for Particle Physics

WLCG

# Outline

MORE MATERIAL HERE THAN TIME TO PRESENT & DISCUSS

(BUT SLIDES AVAILABLE FOR LATER REFERENCE)

- IPv6 security & threats
- IPv6 protocol attacks
- Issues for site network & security teams
- Issues for sys admins
- Where to find more information
- Summary and outlook

*With MANY thanks to my colleagues in the HEPiX IPv6 Working Group and EGI CSIRT*

# New features of IPv6 (1998)

https://tools.ietf.org/html/rfc2460

- Larger address space
- Streamlined protocol headers
- Stateless auto-configuration
- Privacy
- Multicast
- Jumbograms
- Network layer security
- Quality of Service
- Anycast
- Mobility


# IPv6 security and threats

# IPv6 security pros/cons

- Advantages of a new design
  - Security: important part of the IPv6 initial design
- Down-sides
  - Lack of maturity
  - New vulnerabilities and attack vectors
  - Need IPv6-compliant monitoring and tools
  - Lack of education and experience
  - Problems of transition – dual-stack, tunnels
- BUT - Many threats/attacks happen at layers above/below the network layer
  - And are therefore exactly the same as in IPv4
  - Malware, phishing, buffer overflows, cross-site scripting, DDoS etc etc

# Immediate IPv6 concerns

- IPv6 may be on by default (and not controlled or monitored)
- End systems have multiple addresses (and changing)
- Searching logs will not always work
  - Formatting when writing the logs is still broken
  - Same address but different formats (drop zero or not)
- What is wrong with tunnels?
  - Site may not be in control
  - Tunnels traverse the IPv4 perimeter firewall and NAT gateways
- Reputation-based (IP address) web protection does not fully exist for IPv6

# IPv6 deployment risks

- The attacker community can make good use of IPv6
  - They are IPv6 experts
  - E.g. for tunneling leaked info out from compromised systems
- Vulnerabilities present in IPv6, including day zero issues inherent in any new or revised system
  - 242 CVE entries with keyword “IPv6” since 2002
  - 44 in 2015
- Lack of vendor support

- 2001:0DB8:0000:0000:0008:8000:0000:417A
- 2001:DB8:0:0:8:8000:0:417A
- 2001:DB8::8:8000:0:417A
- 2001:DB8:0:0:8:8000::417A
- 2001:db8::8:8000:417A

# IPv6 security myths

- Internet Society has published 10 myths of IPv6 security
- https://www.internetsociety.org/deploy360/blog/tag/ipv6-security-myths/
- **Myth 2: IPv6 has security designed In**
- **Reality: IPv6 was designed 15-20 years ago**

# Network scanning

- **IPv6 Security Myth #4 – IPv6 Networks are Too Big to Scan (Internet Society)**
- **Myth: IPv6 networks are too big to scan**
  **Reality: Many addressing techniques reduce the search space**
- Scanning an IPv4 /24 subnet (256 addresses) is trivial
- An IPv6 /64 subnet has $1.8 * 10^{19}$ addresses
- BUT - SLAAC, DHCPv6 and manual configuration all tend to introduce order into the sparse address space
- For LANs, can use one compromised host to scan via use of Neighbor Discovery

# Some IPv6 protocol attacks

# Some IPv6 protocol attacks

- Extension Headers
- Neighbor Discovery
- Rogue RA
- Duplicate Address Detection
- ICMPv6
- *see backup slides for more details*

# Draft guidance from HEPiX IPv6 working group

## Issues for Sites

# IPv6 issues for security/network teams

- Control IPv6 if not using it
- Use Dual-stack and avoid use of tunnels wherever possible
- Drop packets containing RH Type 0 and unknown option headers
- Deny packets that do not follow rules for extension headers
- Filter IPv6 packets that enter and leave your network
- Restrict who can send messages to multicast group addresses
- Create an Address management plan
- Create a Security Policy for IPv6 (same as IPv4)
- Block unnecessary ICMPv6
- Protect against LAN RA, ND and DHCP attacks
  - NDPMON and RAFIXD on critical segments
- Check/modify all security monitoring, logging and parsing tools

# Draft guidance from HEPiX IPv6 working group

## Issues for Sys Admins

# IPv6 issues for sys admins

- Follow best practice security guidance
  - System hardening as in IPv4, see for example
  - *https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf*
  - Specific advice on IPv6 hardening, see for example
  - *https://www.ernw.de/download/ERNW_Guide_to_Securely_Configure_Linux_Servers_For_IPv6_v1_0.pdf*
- Check for processes listening on open ports
  - # netstat, lsof
- Review neighbour cache for unauthorised systems
  - # ip -6 neigh show
- Check for undesired tunnel interfaces
  - # ip -6 tunnel show, # route –A inet6

# IPv6 for Sys admins (2)

- Ensure not unintentionally forwarding IPv6 packets
  - /proc/sys/net/ipv6/conf/*/forwarding files
  - Or net.ipv6.conf.*.forwarding sysctl
- Use OS embedded IPv6 capable stateful firewall
  - filter based on EH and ICMPv6 message type
- Manage ip6tables
- IPv6 aware intrusion detection
  - E.g. Snort, Suricata, Bro
  - *https://www.sans.org/reading-room/whitepapers/detection/ipv6-open-source-ids-35957*
- IPv6 penetration testing
  - *http://tools.kali.org/information-gathering/thc-ipv6*

# More Information?

# More information

- Many IETF RFC documents on IPv6!
  - *https://tools.ietf.org/wg/opsec/*
- *IPv6 Security – Protection measures for the next Internet Protocol*, Scott Hogg and Eric Vyncke, Cisco Press (2009)
- NIST *Guidelines for the Security Deployment of IPv6* (NIST SP800-119)
  *http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf*
- Internet Society – top 10 IPv6 security myths
  *https://www.internetsociety.org/deploy360/blog/tag/ipv6-security-myths/*

# Summary and Outlook

- In many ways IPv6 security is similar to IPv4
  - But with new twists and new vulnerabilities
- It has taken ~ 30 years to learn how to cope with IPv4 security
- There will be lots of fun ahead with IPv6
- Enjoy the next 20-30 years!

# Questions?

# Backup slides

# IPsec

- Was first developed in 1995 for IPv4 internet layer
  - SSL and TLS operate at Application Layer
- A framework of standards
  - End to end authentication, data integrity and privacy (encryption)
- Can be used site to site (gateway to gateway)
  - As a Virtual Private Network (VPN)
- Or host to host
- All major aspects are same in IPv6 as IPv4
- Does not fully support protection for multicast traffic
  - Key management is one-to-one
- **No longer mandatory** (rfc6434 – MUST -> SHOULD)

# Extension Header vulnerabilities

- Routing Header Type 0
  - Source Routing
  - Lots of security issues with RH0
  - Destination address in packet is replaced at every Layer 3 hop
  - Difficult for firewalls to determine the actual destination and compare with policy
  - Can be used for DoS traffic amplification
  - RH0 deprecated (rfc5095)
- Fragmentation issues
  - Upper-layer info may be in second packet (and not inspected by firewall)
  - IPv6 standard defines every link to have MTU of at least 1280 bytes
    - Smaller fragments should be suspicious
- Hop-by-hop extension header also dangerous
- Solutions include
  - Filter on allowed and expected EH

# IPv6 Neighbor Discovery

## NDP

**NDP** specifies 5 types of ICMP packets:

- **Router Advertisement (RA)**: periodic advertisement of the availability of a router
- **Router Solicitation (RS)**: the host needs RA immediately (at boot time)
- **Neighbor Solicitation (NS)**: to determine the link-layer address of a neighbor (equivalent to ARP request)
- **Neighbor Advertisement (NA)**: answer to a NS packet (equivalent to ARP reply)
- **Redirect**: Used by a router to inform a host of a better route to a given destination

[http://tools.ietf.org/html/rfc4861]

Edoardo Martelli (CERN)

# Neighbor Discovery Protocol

- NDP authenticates neither the requestor or responder
  - Spoofing is possible
- SLAAC, NDP and DAD include protection mechanisms
  - Source address for RA and NS messages must be unspecified (::)
  - Hop limit must be 255 (the maximum)
  - RA and NA messages must be rejected if hop limit is not 255
  - This prevents a remote attacker sending forged RA or NA messages
    - scope is always local
- Secure Neighbor Discovery (SEND) (rfc3971)
  - Uses Cryptographically Generated Addresses (rfc3972)
  - BUT – problems managing the keys

# Rogue RA

- No authentication mechanism built into SLAAC
- Malicious host can send rogue RA and pretend to be a router
  - Can capture or drop packets
- Badly configured systems too

# Detecting rogue RA messages

- Use generic IDS with customised signatures
  - RA whose source MAC or IP is not in a configured list
    - Lots of manual configuration!
- Use tool NDPMon
  - And check against XML config file
  - also monitor all NS and NA
  - To check when NA contradicts a previous one
- Intelligent switches – known RA source
- Cisco RA Guard
- Rafixd (and ramond)
  - Detect all rogue RA messages and immediately transmit another forged RA with lifetime 0 seconds (to clear the rogue info on all nodes)

# DAD

- Duplicate Address Detection
  - Host checks whether its address is already in use
  - Sends NS asking for resolution of its own address
  - An attacker can launch a DoS attack by pretending to own all IPv6 addresses on the LAN

# ICMPv6

- Internet Control Message Protocol (rfc4443)
- An important component of IPv6
- Redefines ICMPv4 with additions and changes
  - Ping, destination unreachable, neighbor discovery, path MTU discovery
  - Error messages (message number 1 to 127)
  - Informational messages (128 to 255)
- Essential to establish strict ICMP filtering policies
  - Define ICMPv6 messages that can/cannot pass between the site and the internet
    - E.g. PMTU and ND
- Rfc4890 “Recommendation for Filtering ICMPv6 Messages in Firewalls”
  - Each site needs to consider carefully!