GTRI
GLOBAL TECHNOLOGY RESOURCES INC.

IPv6 Security

DREN Networking and Security Conference 2011

August 16, 2011

Scott Hogg

GTRI - Director of Technology Solutions

CCIE #5133, CISSP #4610

IPv6 Security – Latent Threat

- Even if you haven't started using IPv6 yet, you probably have some IPv6 running on your networks already and didn't know it
- Do you use Linux, Mac OS X, BSD, or Microsoft Vista/Windows 7 systems in your environment?
  - They all come with IPv6 capability, some even have IPv6 enabled by default (IPv6 preferred)
  - They may try to use IPv6 first and then fall-back to IPv4
  - Or they may create IPv6-in-IPv4 tunnels to Internet resources to reach IPv6 content
  - Some of these techniques take place regardless of user input or configuration
- If you are not protecting your IPv6 nodes then you have just allowed a huge back-door to exist

IPv6 Security Threats

- There isn't a large hacker community focusing on IPv6 today but it is starting to gain the attacker's attention
- THC IPv6 Attack Toolkit, IPv6 port scan tools, IPv6 packet forgery tools and IPv6 DoS tools all exist and continue to evolve
- Many major vendors and open-source software have already published IPv6 bugs/vulnerabilities
- Attacks at the layers below and above the network layer are unaffected by the security of IPv6
  - Buffer overflows, SQL Injection, cross-site scripting will all remain valid attacks on IPv6 servers
  - E-mail/SPAM is still a problem in IPv6 nets

Reconnaissance

- Ping sweeps, port scans, application vulnerability scans are problematic with IPv6's large address space - brute-force scanning a /64 is not practical
- There are methods of speeding up reconnaissance
  - ping6 -I eth0 ff02::1
  - [root@hat ~]# ./alive6 eth0 ff02::1
  - Node Information Queries (RFC 4620) in BSD
  - Scanning for specific EUI-64 addresses using specific OUIs
  - Scanning IPv4 and getting IPv6 info
    - Metasploit Framework "ipv6_neighbor" auxiliary module can leverage IPv4 to find IPv6 hosts
  - Scanning 6to4, ISATAP, Teredo addresses
  - Attackers may find one node and leverage the neighbor cache to find other nodes
  - DHCPv6 logs, DNS servers, server logs, NMSs, Google

IPv6 Privacy Addressing

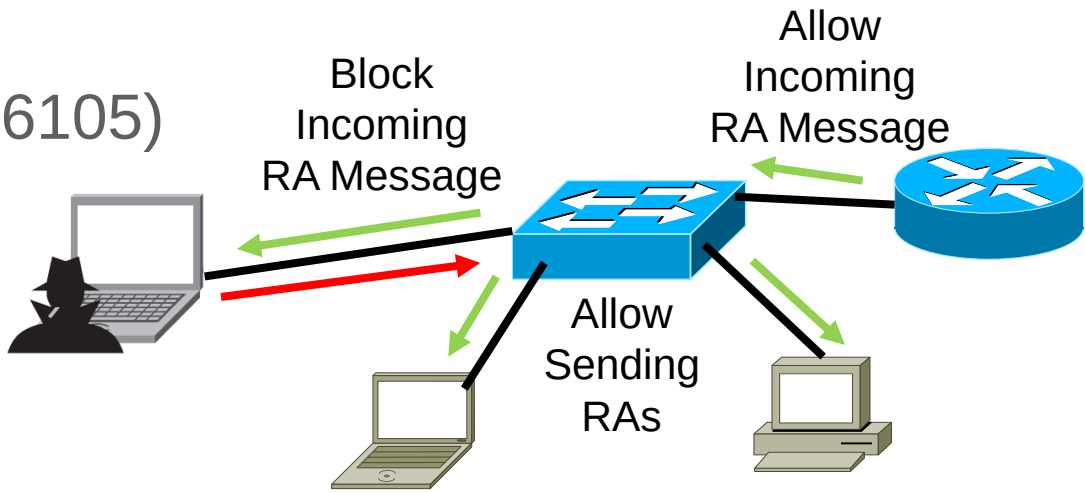
- Privacy of addresses in an issue with IPv6
  - EUI-64 addresses are derived from the host's MAC
  - That could be used to track user's activity and thus identity
- Temporary and Privacy IPv6 address intended to protect the identity of the end-user
  - MD5 hash of the EUI-64 concatenated with a random number that can change over time
  - Different implementations rotate the address at different frequencies – can be disabled
- Forensics and troubleshooting are difficult with privacy addresses – Who had what address when?
- Dynamic DNS and firewall state updates
- Difficulty creating granular firewall policy when IP addresses change often
- Better to use DHCPv6 with randomized IIDs

LAN Threats

- IPv6 uses ICMPv6 for many LAN operations
  - Stateless auto-configuration
  - Neighbor Discovery Protocol (NDP)
  - IPv6 equivalent of IPv4 ARP – same attack types
- Spoofed RAs can renumber hosts or launch a MITM attack
- Forged NA/NS messages to confuse NDP
- Redirects – same as ICMPv4 redirects
- Forcing nodes to believe all addresses are on-link
- These attacks presume the attacker is on-net or has compromised a local computer

Methods of Preventing Rogue RAs

- Prevent unauthorized LAN access
- Disable unused switch ports
- Network Access Control (NAC), Network Admission Control (NAC)
- IEEE 802.1AE (MACsec), Cisco TrustSec
- IEEE 802.1X
- RA Guard (RFC 6105)
- NDPMon
- Ramond
- Kame rafixd
- Port Security
- Cisco Port-based ACL (PACL)



Extension Headers

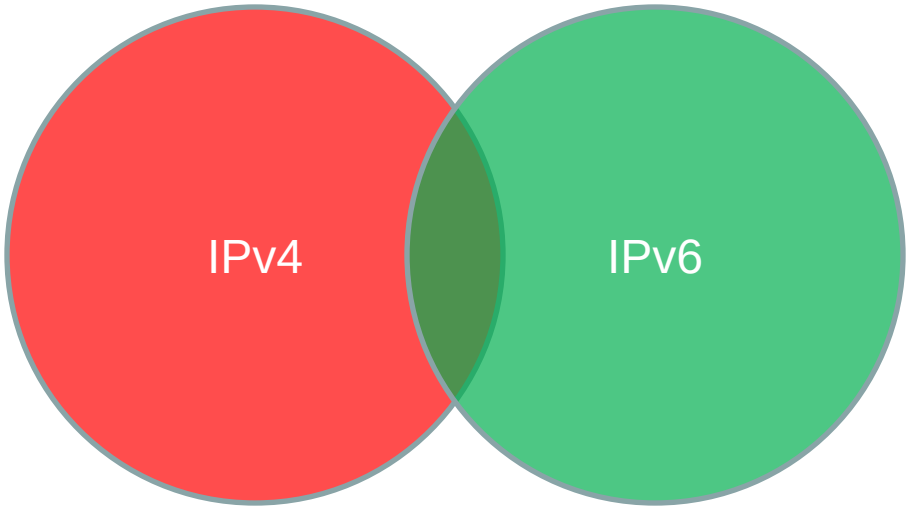
- There are rules for the frequency and order of various extension headers
  - Hop-by-Hop and Destination Options
- Header Manipulation – Crafted Packets
  - Large chains of extension headers
  - Separate payload into second fragment
  - Consume resources - DoS
  - Invalid Extension Headers – DoS
- Routing Headers Type 0 – source routing
  - Routers can be configured to block RH0
  - This is now the default on newer routers
  - Firewalls, Windows, Linux and MacOS all block RH0 by default

Layer-3/4 Spoofing

- Spoofing of IPv6 packets is possible
- IPv6 BOGON (Martians) Filtering is required
  - Filter traffic from unallocated space and filter router advertisements of bogus prefixes
  - Permit Legitimate Global Unicast Addresses
  - Don’t block FF00::/8 and FE80::/10 – these will block NDP
- Hierarchical addressing and ingress/egress filtering can catch packets with forged source addresses
- Tracebacks may prove to be easier with IPv6
- You can use inbound Infrastructure ACLs (iACLs) that deny packets sent to infrastructure IPv6 addresses

Transition Mechanism Threats

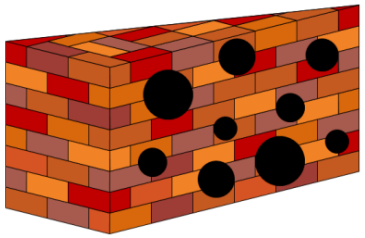
- Dual Stack is the preferred transition method
- You are only as strong as the weakest of the two stacks
- Running dual stack will give you at least twice the number of vulnerabilities and require almost twice the work to secure



Threats Against Translation

- Manual Tunnels
  - Preferred over dynamic tunnels
  - Filter tunnel source/destination and use IPsec
  - If spoofing, return traffic is not sent to attacker
- Dynamic Tunnels
  - 6to4 Relay routers are “open relays”
  - Attackers can guess 6to4 addresses easily
  - ISATAP can have potential MITM attacks
  - Attackers can spoof source/dest IPv4/v6 addresses
- Translation techniques are susceptible to DoS attacks
  - NAT prevents IPsec, DNSSEC, Geolocation and other applications from working
  - Consuming connection state (CPU resource consumption attack on ALG)
  - Consuming public IPv4 pool and port numbers (pool depletion attack)

IPv6 Firewalls



- Don’t just use your IPv4 policy for your IPv6 policy
- Don’t blindly allow IPsec or IPv4 Protocol 41 (6in4 tunneled traffic) through the firewall unless you know the tunnel endpoints
- Firewalls have improved their IPv6 capabilities, IPv6 addresses in the GUI, some logs, ability to filter on Extension Headers, Fragmentation, PMTUD, and granular filtering of ICMPv6 and multicast
- IPv6 firewalls may not have all the same full features as IPv4 firewalls
  - UTM/DPI/IPS/WAF/content filtering features may only work for IPv4

IPv6 Intrusion Prevention

- Few signatures exist for IPv6 packets or you have to build your own using cryptic regular expressions or byte-offset values
- IPSs should send out notifications when non-conforming IPv6 packets are observed having faulty parameters, bad extension headers, source address is a multicast address
- Many IPSs don’t inspect packets that are encapsulated (6in4, 6to4, 6in6, ISATAP, Teredo, 6rd, DS-Lite)
- IPv6 support varies greatly in modern IPS systems
- Talk with your vendor about what you need

Host-Based Firewalls and AV

- There are many IPv6-capable host-based firewalls available depending on the OS you prefer
  - Linux: ip6tables (NetFilter), ipf
  - Windows Firewall with Advanced Security
  - BSD: pf, ipfw, ipf
  - Mac: ipfw, ipf
  - Solaris, HP-UX : ipf
- Few Host-based IPS systems support IPv6
- Desktop AntiVirus software has gotten better at allowing ICMPv6 (RA/RS/NA/NS) packets through
- However, there are still a handful of popular AV suites that don't support IPv6

IPv6 Security Policies

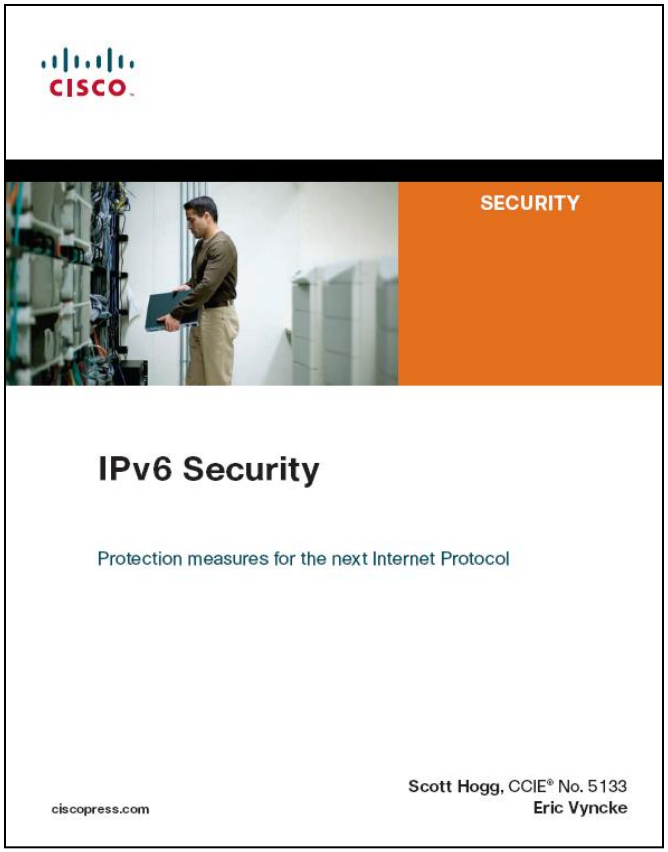
- Many security standards don't discuss IPv6. However, any guideline related to IP may apply to both versions – many policies are higher level
- NIST SP 800-119: Guidelines for the Secure Deployment of IPv6, December 2010
  - http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf
- NIST Special Publication (SP) 500-267: A Profile for IPv6 in the U.S. Government – V1, USGv6-V2 comments due June 10, 2011, results Sept. 2011
  - USGv6 Profile tests for granular filtering of IPv6 and ICMPv6 messages
    - http://www.antd.nist.gov/usgv6/cfp.html

Summary of BCPs

- Perform IPv6 filtering at the perimeter
- Use RFC2827 filtering and Unicast RPF checks throughout the network
- Use manual tunnels (with IPsec whenever possible) instead of dynamic tunnels and deny packets for transition techniques not used
- Use common access-network security measures (NAC/802.1X, disable unused switch ports, Ethernet port security, MACSec/TrustSec) because SEND won't be available any time soon
- Strive to achieve equal protections for IPv6 as with IPv4
- Continue to let vendors know what you expect in terms of IPv6 security features

Yet another IPv6 Book

- *IPv6 Security*, By Scott Hogg and Eric Vyncke, Cisco Press, 2009.



ISBN-10: 1-58705-594-5
ISBN-13: 978-1-58705-594-2