GTRI
GLOBAL TECHNOLOGY RESOURCES INC.

Rocky Mountain IPv6 Summit

April 9, 2008

Rocky Mountain IPv6 Task Force

RMv6TF

IPv6 Security

Scott Hogg

GTRI - Director of Advanced Technology Services

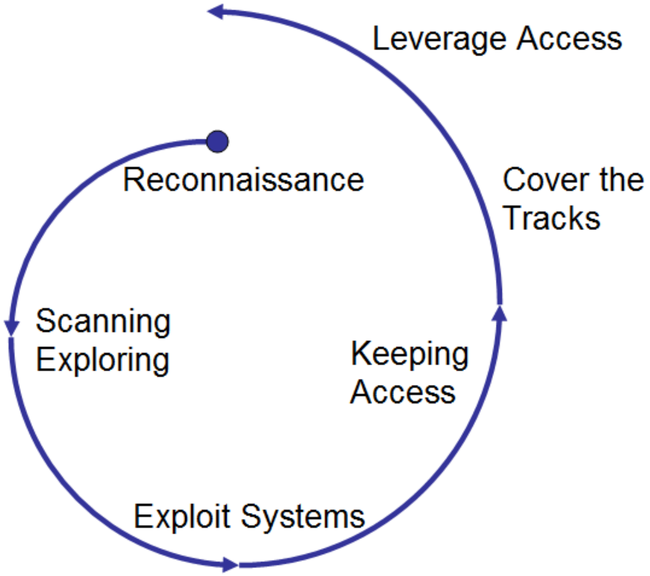
CCIE #5133, CISSP

IPv6 Security

- We will all migrate eventually, but when and how remain to be seen
- I bet you have some IPv6 running on your networks already
- Do you use Linux, MacOS X, BSD, or MS Vista?
  - 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 much of a hacker community focusing on IPv6 today but that is likely to change as IPv6 becomes more popular – IPv6 will gain the hacker's attention
- Many vendors (Cisco, Juniper, Microsoft, Sun, Open Source) have already published IPv6 bugs/vulnerabilities
- Attacks at the layers below and above the network layer are unaffected by the security of IPv6



Reconnaissance

- First step of an attack
- Checking registries (whois), DNS (nslookup, dig, etc.), Google
- Ping sweeps, port scans, application vulnerability scans
- IPv6 makes the ping sweeps problematic
  - The address space is too large to scan
- Ping FF02::1 will give results
- Node Information Queries (RFC 4620)
- Attackers may find one host and leverage the neighbor cache

LAN Threats

- IPv6 uses ICMPv6 for many LAN operations
  - Stateless auto-configuration
  - IPv6 equivalent of IPv4 ARP
- Spoofed RAs can renumber hosts or launch a MITM attack
- NA/NS – same attacks as with ARP
- DHCPv6 spoofing
- Redirects – same as ICMPv4 redirects
- Forcing nodes to believe all addresses are on-link

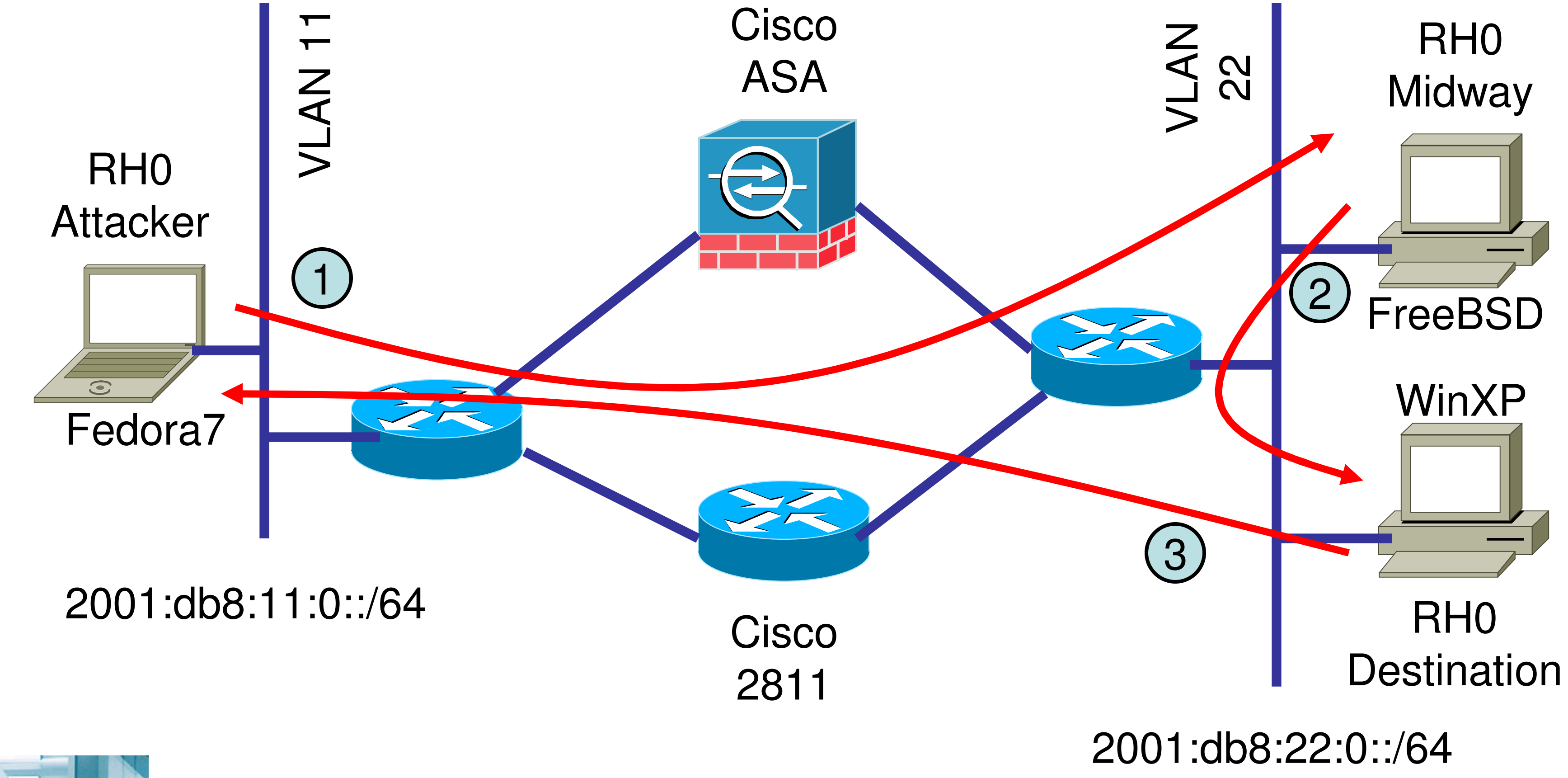
Secure Neighbor Discovery (SEND)

- IPSec is not usable to secure NDP
- SEND (RFC 3971) defines the trust model for nodes communicating on a LAN
- Nodes use public/private key pair to create Cryptographically Generated Addresses (CGA – RFC 3972) which is the last 64 bits of address (interface ID)
- Improvements on standard neighbor discovery:
  - Neighbor Discovery Protocol messages use RSA-based cryptography to protect their integrity
  - Signed ND messages protect message integrity and authenticate the sender.
  - Trust anchors may certify the authority of routers.
- Current Deployment
  - DoCoMo USA Labs - OpenSource SEND Project

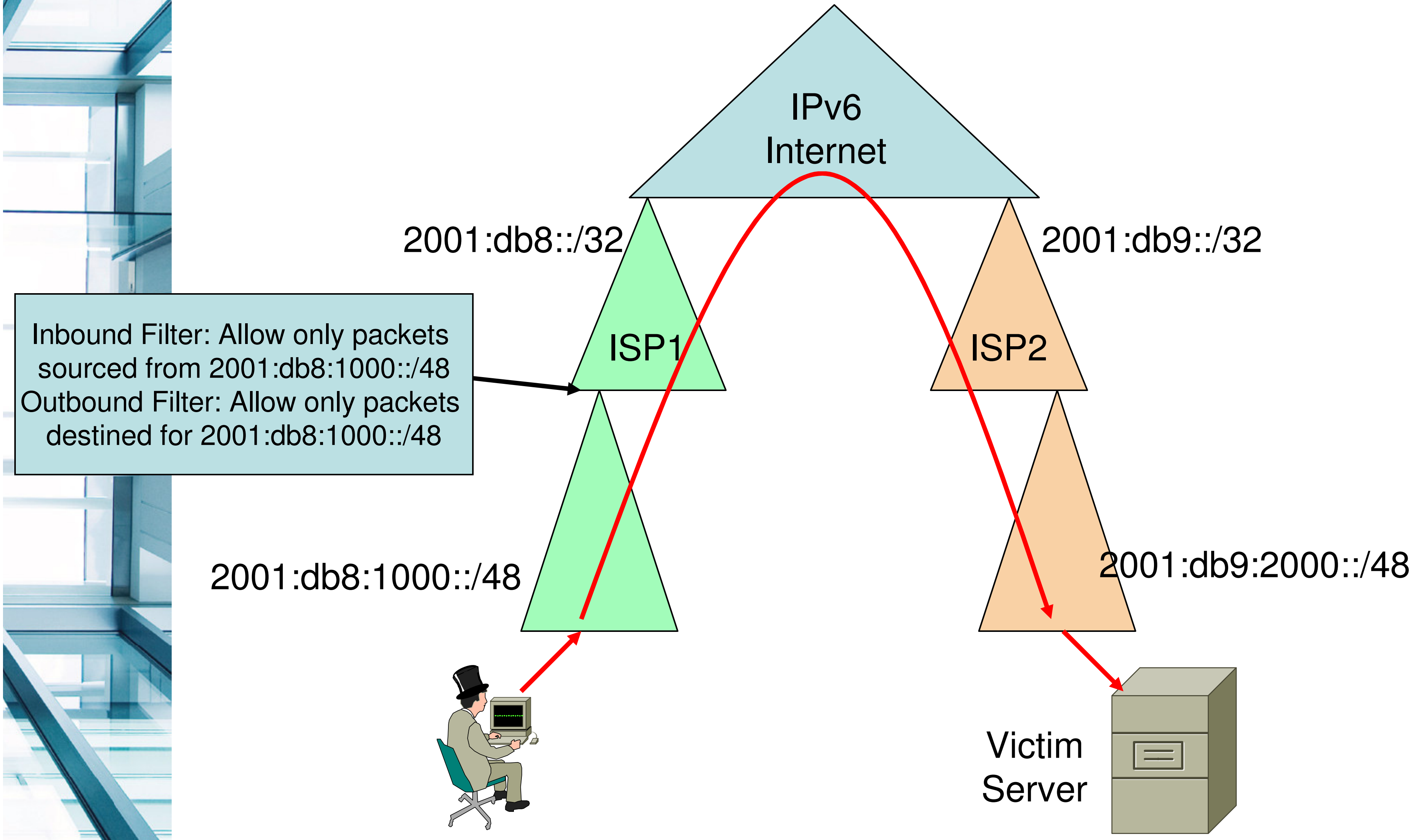
Extension Headers (EHs)

- Extension Headers
  - Each header should not appear more than once with the exception of the Destination Options header
  - Hop-by-Hop extension header should only appear once.
  - Hop-by-Hop extension header should be the first header in the list because it is examined by every node along the path.
  - Destination Options header should appear at most twice (before a Routing header and before the upper-layer header).
  - Destination Options header should be the last header in the list if it is used at all.
- 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

Routing Header 0 Attack



Hierarchy and Traceback

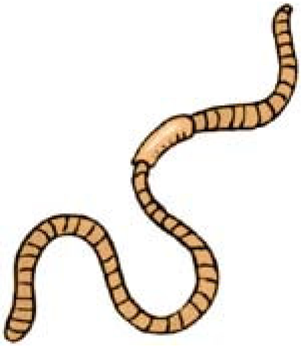


Inbound Filter: Allow only packets sourced from 2001:db8:1000::/48
Outbound Filter: Allow only packets destined for 2001:db8:1000::/48

Transition Mechanism Threats

- Dual Stack - Preferred
  - 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
- Manual Tunnels - Preferred
  - Filter tunnel source/destination and use IPSec
  - If spoofing, return traffic is not sent to attacker
- Dynamic Tunnels
  - 6to4 Relay routers are “open relays”
  - ISATAP – potential MITM attacks
  - Attackers can spoof source/dest IPv4/v6 addresses
- Protocol Translation – Not recommended
- Deny packets for transition techniques not in use
  - Deny IPv4 protocol 41 forwarding unless that is exactly what is intended – unless using 6to4 tunneling
  - Deny UDP 3544 forwarding unless you are using Teredo-based tunneling

Viruses and Worms



- Viruses will be the same with IPv6
- Worms like Sapphire/SQL Slammer won’t spread nearly as quickly (100s of years)
- “At one million packets per second on a IPv6 subnet with 10,000 hosts it would take over 28 years to find the first host to infect”
- IPv6 Worm – Slapper
- Scanning worms may use IPv4 and then check for IPv6 capabilities on infected host
- Perform ingress/egress filtering and uRPF checks throughout the network and at the perimeter

IPv6 Firewalls

- Don’t just use your IPv4 firewall for IPv6 rules
- Don’t just blindly allow IPSec or IPv4 Protocol 41 through the firewall
- Procure separate firewalls for IPv6 policy
- Look for vendor support of Extension Headers, Fragmentation, PMTUD
- Firewalls should have granular filtering of ICMPv6 and multicast
- Some hosts may have multiple IPv6 addresses so this could make firewall troubleshooting tricky
- Layer-2 firewalls are trickier with IPv6 because of ICMPv6 ND/NS/NUD/RA/RS messages

IPv6-Capable Firewalls

- Many vendors already have IPv6 capabilities
  - Cisco Router ACLs, Reflexive ACLs, IOS-based Firewall, PIX, ASA, FWSM
  - CheckPoint, Juniper, Fortinet, others
  - ip6tables, ip6fw, ipf, pf
  - Windows XP SP2, Vista IPv6 Internet Connection Firewall
- IPv6 firewalls don’t have all the same full features as IPv4 firewalls
  - UTM features may only work for IPv4
  - Vendors are working toward feature parity

IPv6 Intrusion Prevention

- Few signatures exist for IPv6 packets
- IPSs should send out notifications when non-conforming IPv6 packets are observed
- Faulty parameters, bad extension headers, source address is a multicast address
- IPv6-Capable IPSs
  - Snort 2.8 Beta and 3.0 Alpha
  - CheckPoint (NFR) Sentivist
  - Cisco 4200 IDS appliances (v6.0)
  - Juniper/NetScreen ScreenOS
  - IBM/ISS Proventia/RealSecure

IPv6 IPSec Solutions

- IPSec was first designed for IPv6 and then was added to IPv4 where it became widely deployed
- RFC 2401 mandated every IPv6 device support IPSec
- IPv6 will use more AH and ESP transport-mode implementations than IPv4/NAT
- Interoperability, global PKI, and the fact that small devices won’t have the capability have stopped this from being a strict requirement
- IPSec isn’t a protection against application attacks
- You may not want to allow IPSec from any to any through your firewall

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 host portions of an 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
- Dynamic DNS and Firewall state will also need to update
- Difficulty creating granular firewall policy when IP addresses change often

IPv6 BOGON Filtering

- Filter traffic from unallocated space and filter router advertisements of bogus prefixes
- Permit Legitimate Global Unicast Addresses
  - 2001::/16—IPv6 Unicast Addresses
  - 2002::/16 - 6to4
  - 2003::/18 - RIPE NCC
  - 2400::/12 - APNIC
  - 2600::/12 - ARIN(US DoD)
  - 2610::/23 - ARIN
  - 2620::/23 - ARIN
  - 2800::/12 - LACNIC
  - 2A00::/12 - RIPE NCC
  - 2C00::/12 – AfriNIC

Team Cymru

IPv6 BOGON Filtering

- Deny Teredo (or UDP 3544)
  - 2001:0000::/32
- Deny 6Bone
  - 3ffe::/16
- Deny Unspecified and Loopback
  - ::/128 (::/0) , ::1
- Deny Site-local Multicast or Deny All Multicasts
  - ff05::/16 or ff00::/8
- Deny Link Local Addresses
  - fe80::/10
- Deny IETF Reserved Address
  - fec0::/10
- Deny Unique-local Address
  - fc00::/7
- Deny Documentation Address
  - 2001:db8::/32
- Deny IPv4 Mapped Addresses
  - ::ffff:0.0.0.0/96
- Deny IPv4-compatible IPv6 Address
  - ::0.0.0.0/96
- Deny Other Compatible Addresses
  - ::224.0.0.0/100
  - ::127.0.0.0/104
  - ::0.0.0.0/104
  - ::255.0.0.0/104
- Deny False 6to4 Packets
  - 2002:e000::/20
  - 2002:7f00::/24
  - 2002:0000::/24
  - 2002:ff00::/24
  - 2002:0a00::/24
  - 2002:ac10::/28
  - 2002:c0a8::/32

IPv6 Security Summary

- IPv6 is no more or less secure than IPv4
  - Lack of knowledge of IPv6 is an issue
- There aren’t as many security products that support IPv6 yet
- IPv6 will change traffic patterns (p2p, MIPv6)
- IPv6 larger addresses makes worms and scanning less effective but there are still ways to find hosts
- IPv6 hierarchical addressing and no NAT should reduce the anonymity of hackers and allow for full IPSec
- LAN-based attacks exist in IPv6, Physical Security, Ethernet port security, NAC, 802.1X, SEND can help
- Perform IPv6 filtering at the perimeter
- Use RFC2827 filtering and Unicast Reverse Path Forwarding (uRPF) checks throughout the network
- Use manual tunnels instead of dynamic tunnels

Resources

- IETF v6ops Working Group
  - http://www.ietf.org/html.charters/v6ops-charter.html
- Microsoft
  - http://www.microsoft.com/ipv6
- Cisco IPv6 SRND Guides for Branch and WAN
  - http://www.cisco.com/go/srnd
- S. Convery & D. Miller, “IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation”, v1.0, Cisco Systems Technical Report, March 2004
  - http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf
- North American IPv6 Task Force (NAv6TF) Technology Report, “IPv6 Security Technology Paper”, by Merike Kaeo, David Green, Jim Bound, Yanick Pouffary
  - http://www.nav6tf.org/documents/nav6tf.security_report.pdf
- NSA SNAC Guide for IPv6
  - http://www.nsa.gov/snac/downloads_cisco.cfm?MenuID=scg10.3.1

Question and Answer

Q:

&

A:

SHogg@GTRI.com
Scott@HoggNet.com

Mobile: 303-949-4865