



SEAPORT WORLD TRADE CENTER
BOSTON, MA, USA
MAY 4-7, 2009
SESSION ID: S27



IPV6 SECURITY

Scott Hogg

GTRI - Director of Advanced Technology Services

CCIE #5133, CISSP #4610



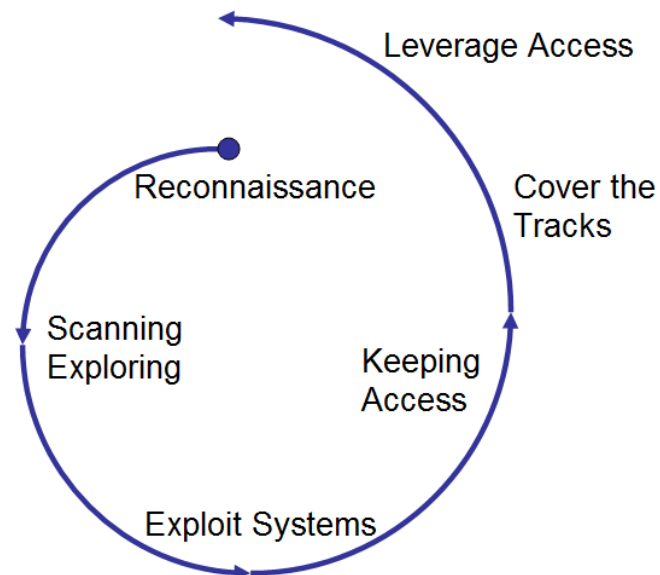
IPv6 SECURITY



- We will all migrate to IPv6 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





IPv6 ATTACK TOOLS

- **THC IPv6 Attack Toolkit**
 - parasite6, alive6, fake_router6, redir6, toobig6, detect-new-ip6, dos-new-ip6, fake_mld6, fake_mipv6, fake_advertiser6, smurf6, rsmurf6
- **Scanners**
 - Nmap, halfscan6
- **Packet forgery**
 - Scapy6, SendIP, Packit, Spak6
- **DoS Tools**
 - 6tunneldos, 4to6ddos, Imps6-tools



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 may 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

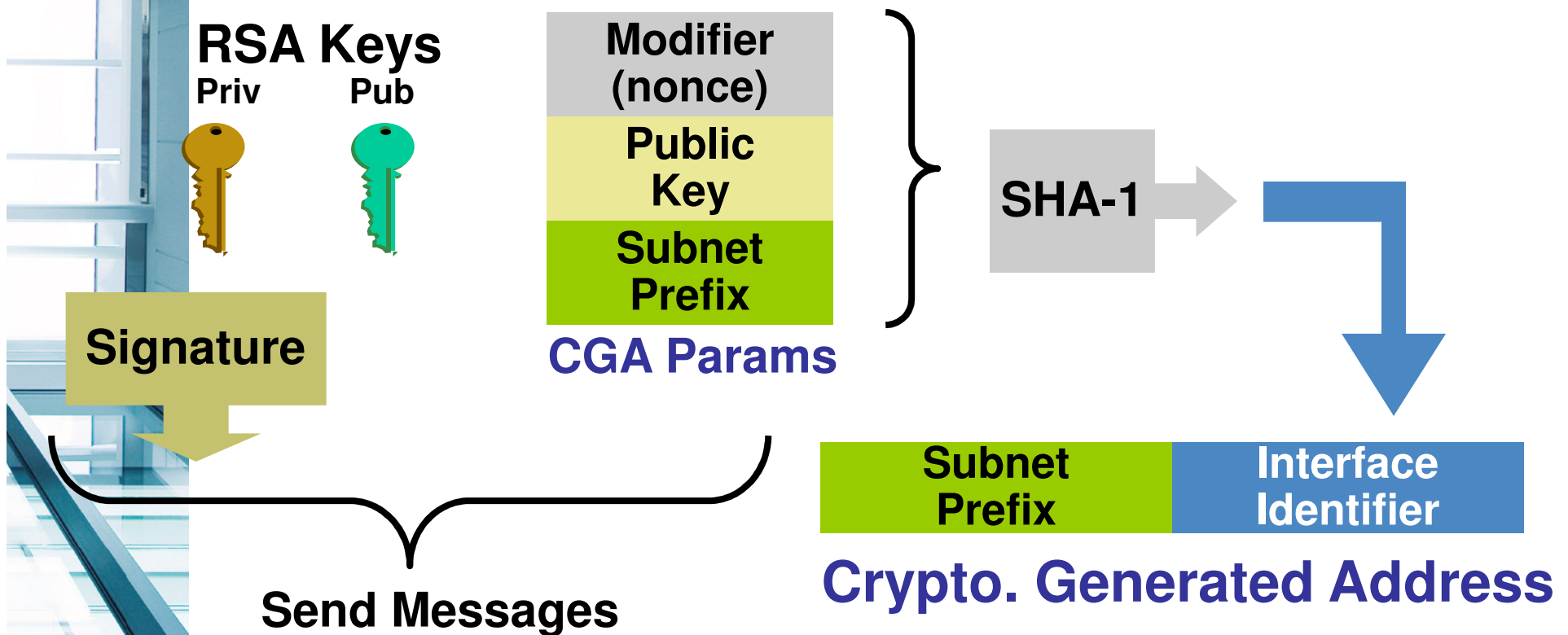


SECURE NEIGHBOR DISCOVERY (SEND)

- 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
 - Cisco 12.4T and 12.2SR

CRYPTOGRAPHICALLY GENERATED ADDRESSES (CGA)

- Each devices has a RSA key pair (no need for cert)
- Ultra light check for validity
- Prevent spoofing a valid CGA address

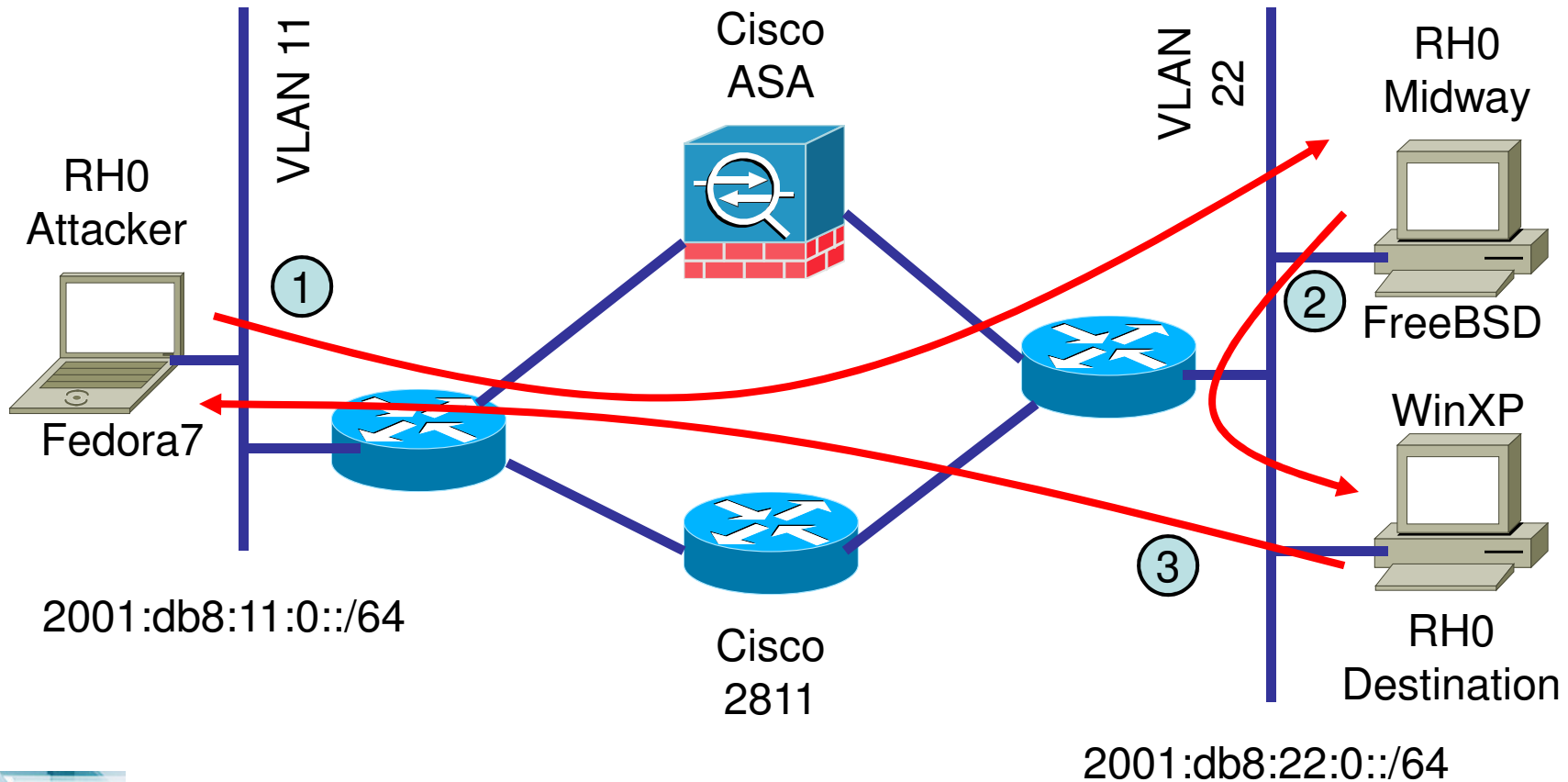


EXTENSION HEADERS (EHs)

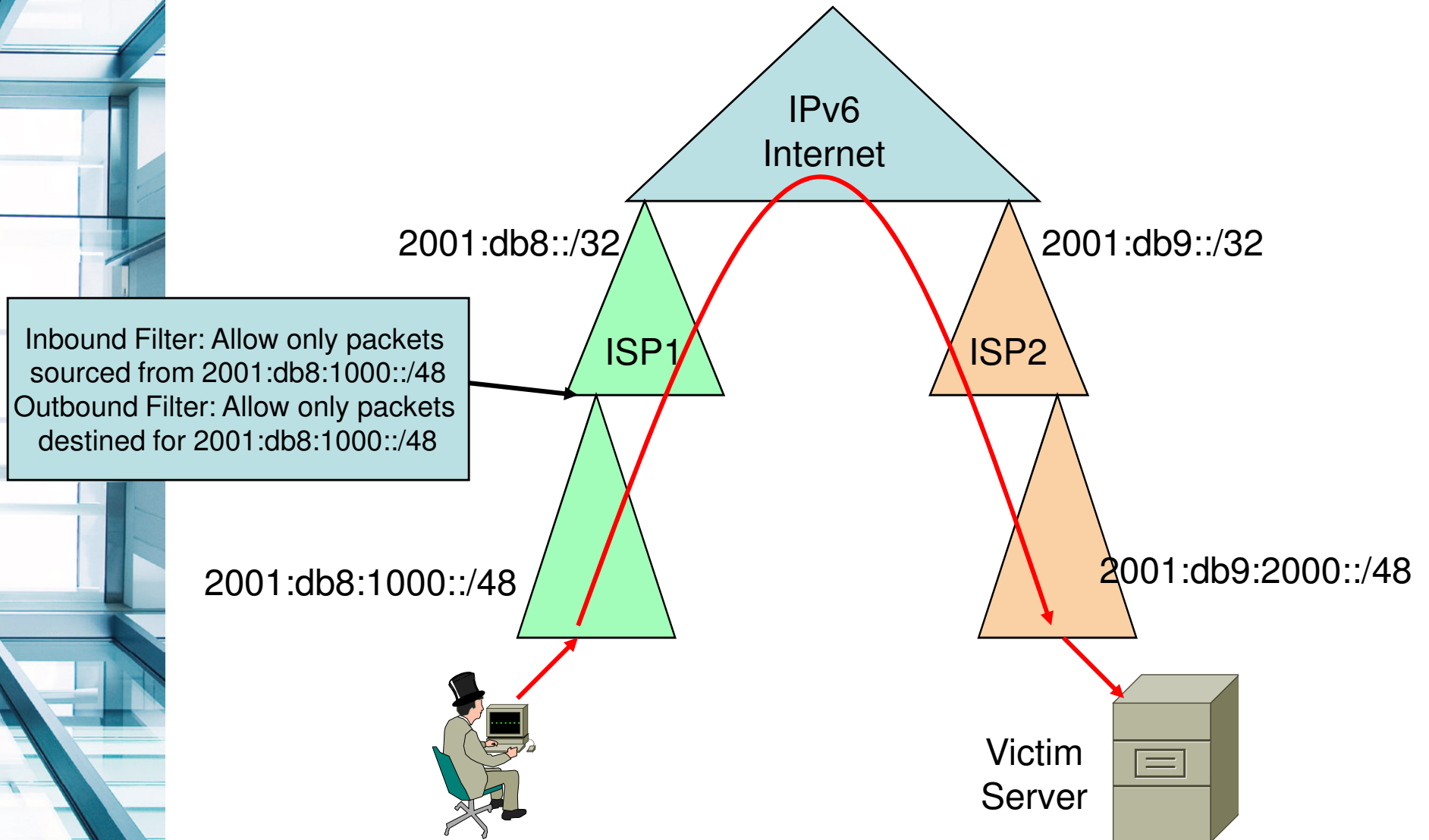
- Extension Headers
 - Each header should not appear more than once with the exception of the Destination Options header
 - Hop-by-Hop extension header should only appear once.
 - Hop-by-Hop extension header should be the first header in the list because it is examined by every node along the path.
 - 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



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





MOBILE IPv6 SECURITY

- Mobility changes the perimeter model
- Layer-3 devices need to enable MIPv6 to all hosts on the subnet
- You must allow Type 2 Routing Header for CN to MN
- Attacker could be a fake MN or a rogue Home Agent
- If you don't use MIPv6 then filter it
 - Home Agent Address Discovery Request - Type 144
 - Home Agent Address Discovery Reply - Type 145
 - Mobile Prefix Solicitation - Type 146
 - Mobile Prefix Advertisement - Type 147
- Firewalls don't have state information on who is roaming and who isn't
- Binding Update, Binding Ack filtering on the Layer-3 HAs
- IPSec can be used with MIPv6 but some mobile devices don't have the resources

IPv6 PRIVACY ADDRESSING



- Privacy of addresses is 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 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 (v6.1)
 - Juniper/NetScreen ScreenOS
 - IBM/ISS Proventia/RealSecure



SUMMARY OF BCPs



- Remember physical security
- Use a NAC/802.1X solution, disable unused switch ports, Ethernet port security
- 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
- 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
- Leverage IPSec for everything possible
- Try to achieve equal protections for IPv6 as with IPv4

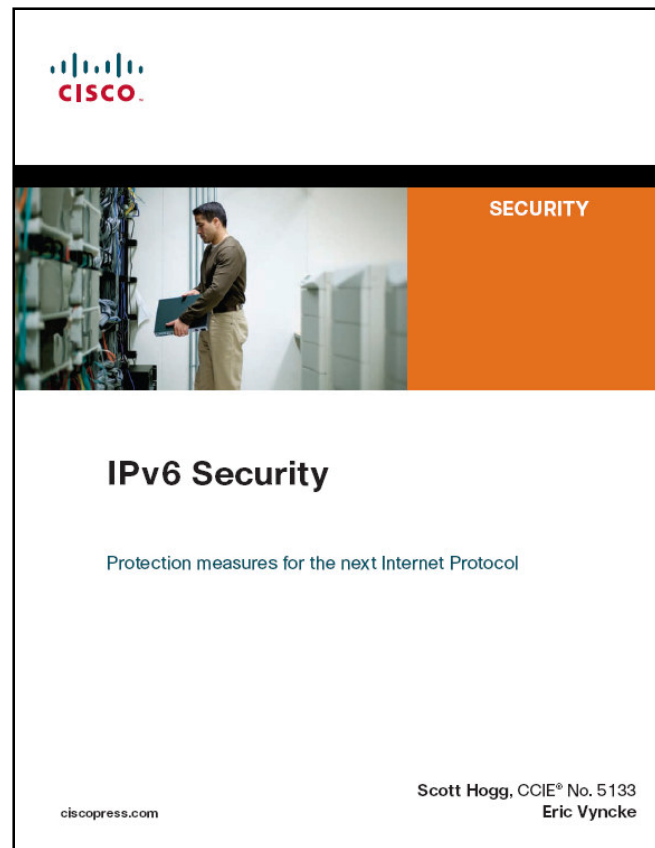


IPv6 SECURITY SUMMARY

- IPv6 is no more or less secure than IPv4
 - Lack of IPv6 knowledge and experience is a serious 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

YET ANOTHER IPv6 BOOK

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





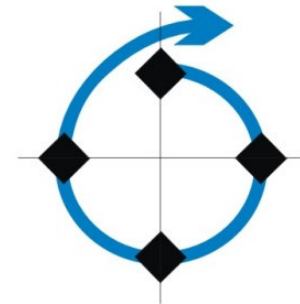
ROCKY MOUNTAIN IPv6 TASK FORCE



- Regional “chapter” of North American IPv6 Task Force and, therefore, the IPv6 Forum
- Our Charter
 - Provide Education on IPv6 and its benefits
 - Promotion of IPv6 technology
 - Research and Development and showcase IPv6 technology and services
 - Put on local IPv6-focused events
 - Work to further the use of IPv6 with a regional focus
- Get involved in your regional/national IPv6 organizations
 - www.RMv6TF.org
 - www.MidAtlanticv6tf.org
 - www.cav6tf.org

GTRI's IPv6 Transition Services

- **IPv6 Inventory**
 - Documentation of your current inventory and determination of IPv6 compatibility
 - Data gathering expertise (manual, data calls, automated utilities)
 - Cisco and GTRI automated tools
 - Inventory data aggregation and review
- **IPv6 Training**
 - Education for your teams to help them learn IPv6 technologies
 - Classroom and hands-on training
- **IPv6 Impact Analysis**
 - IPv6 Risk Assessment using OMB's own Risk Analysis Methodology
 - Custom-tailored transition planning for your IPv6 migration, tied to your enterprise architecture
- **IPv6 Application Assessment**
 - Software assessments leveraging COTS tools and our extensive experience
 - Review of your operating system constraints for IPv6 adoption
- **IPv6 Experimentation and Testing**
 - Systems testing in our IPv6 lab (DNS, routing, security, applications)
- **IPv6 Deployment**
 - Deployment of dual-stack and other IPv6 transition techniques
 - Dual Stack DNS servers and IPv6 security deployment



QUESTION AND ANSWER

Q:

&

A:

SHogg@GTRI.com
Scott@HoggNet.com

Mobile: 303-949-4865