Rocky Mountain ISSA Chapter
April 5, 2007

IPv6 Security

2007 Rocky Mountain Information Security Conference

Scott Hogg

Director of Advanced Technology Services - GTRI

CCIE #5133, CISSP #4610

Agenda

- IPv6 Threats
  - Reconnaissance
  - LAN Threats
  - ICMPv6 Threats
  - Extension Headers
  - Fragmentation
  - Transition Mechanism Threats
  - Router Threats
  - Application Threats
  - Man-In-The-Middle Threats
  - Flooding – DoS
  - Viruses and Worms
  - Mobile IPv6 Security
- IPv6 Protection Measures
  - IPv6 Firewalls
  - Intrusion Prevention Systems
  - Hardening IPv6 Network Devices
  - IPSec
  - IPv6 Privacy Addressing
- Questions and Answers

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, MS XP SP2, or MS Vista?
  - They all come with IPv6 capability, some even have IPv6 enabled by default (IPv6 preferred)
  - Vista sends IPv6 NA/NS/RS upon link-up
  - Attempts DHCP for IPv6
  - If no DHCP or local RA received with Global or ULA, then try ISATAP, If no ISATAP, then try Teredo
  - If no Teredo, then use IPv4 – LAST RESORT
- If you are not protecting your IPv6 nodes then you have just allowed a huge back-door to exist

IPv6 Security

- IPv6 Security is being considered up front in its design and deployment
- BCPs for IPv4 apply to IPv6
  - Least Privilege
  - Defense in Depth
  - Diversity of Defense
  - Choke Point
  - Weakest Link
  - Fail-Safe Stance
  - Universal Participation
- Simplicity over Complexity
- Confidentiality, Integrity, Availability (CIA)

IPv6 Threats

- There isn't much of a hacker community focusing on IPv6 today but that is likely to change as IPv6 becomes more popular (e.g. Firefox)
- IP is the most popular network-layer protocol on the planet
  - IPv6 will gain the hacker's attention
- Many vendors (Cisco, Juniper, Microsoft, Sun) have already published IPv6 bugs/vulnerabilities
- Attacks generally fall into one of these three categories.
  - Denial of Service
  - Modification of Information
  - Eavesdropping

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
- Ping FF02::1 will give results
- Node Information Queries (RFC 4620)
- Attackers may find one host and leverage the neighbor cache

LAN Threats

- Rogue Devices – Unauthorized Access
  - If an attacker is on your LAN then you have already lost the battle
  - Physical security
  - Disable unused Ethernet switch ports
  - Enable Switch Port Security
  - Use an 802.1X or NAC technology
- IPv6 uses ICMPv6 for many LAN operations
  - Stateless auto-configuration
  - IPv6 equivalent to IPv4's ARP

ICMPv6

- More powerful than ICMPv4
- ICMPv6 uses IPv6 extension header # 58 (RFC 2463)

	Type	Description
	1	Destination Unreachable
	2	Packet to Big
	3	Time exceeded
	4	Parameter problem
PING	128	Echo Request
PING	129	Echo Reply
	130	Multicast Listener Query – sent to ff02::1 (all nodes)
MLD	131	Multicast Listener Report
	132	Multicast Listener Done – sent to ff02::2 (all routers)
Prefix Advertisement	133	Router Solicitation (RS) – sent to ff01::2 (all routers)
Prefix Advertisement	134	Router Advertisement (RA) – sent to ff01::1 (all nodes)
ARP Replacement DAD	135	Neighbor Solicitation (NS) – sent to ff02:0:0:0:0:1:ff00::/104
ARP Replacement DAD	136	Neighbor Advertisement (NA)
Router Redirection	137	Redirect message

LAN Threats

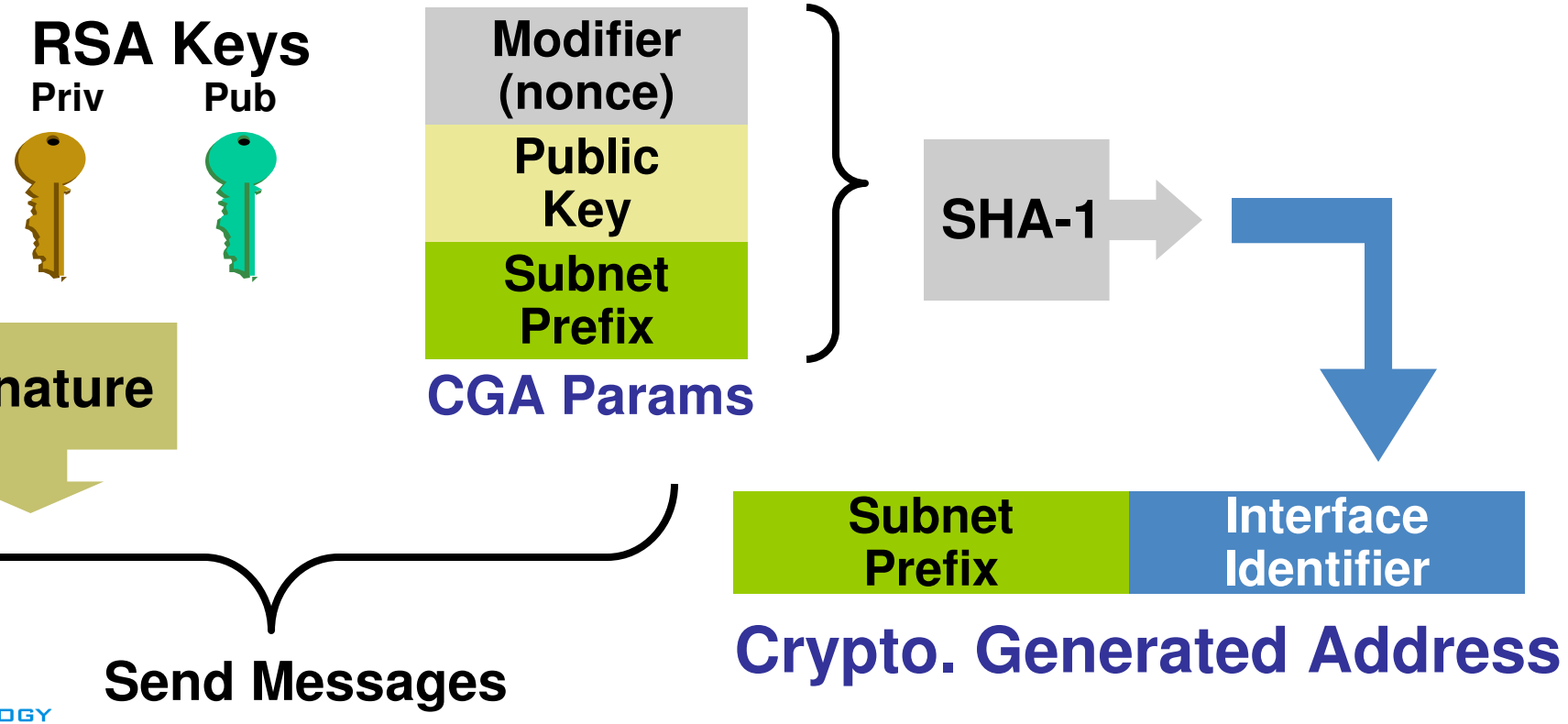
- Spoofed RAs can renumber hosts or launch a MITM attack
- ND/NS – same attacks as with ARP
- DHCPv6 spoofing
- Redirects
- Forcing nodes to believe all addresses are on-link
- Sniffers still work on IPv6 LANs

Secure Neighbor Discovery (SEND)

- Neighbor Discovery is vital for a network to work properly. However, it is not secure.
- Neighbor or router spoofing are possible attacks, along with rogue advertisers, redirect and unreachability attacks.
- IPSec unpractical for securing ND.
- Improvements on standard neighbor discovery:
  - CGAs makes it possible to prove the ownership of a
  - specific address.
  - Signed ND messages protect message integrity and
  - authenticate the sender.
  - Nonce prevent replay attacks.
  - Trust anchors may certify the authority of routers.

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

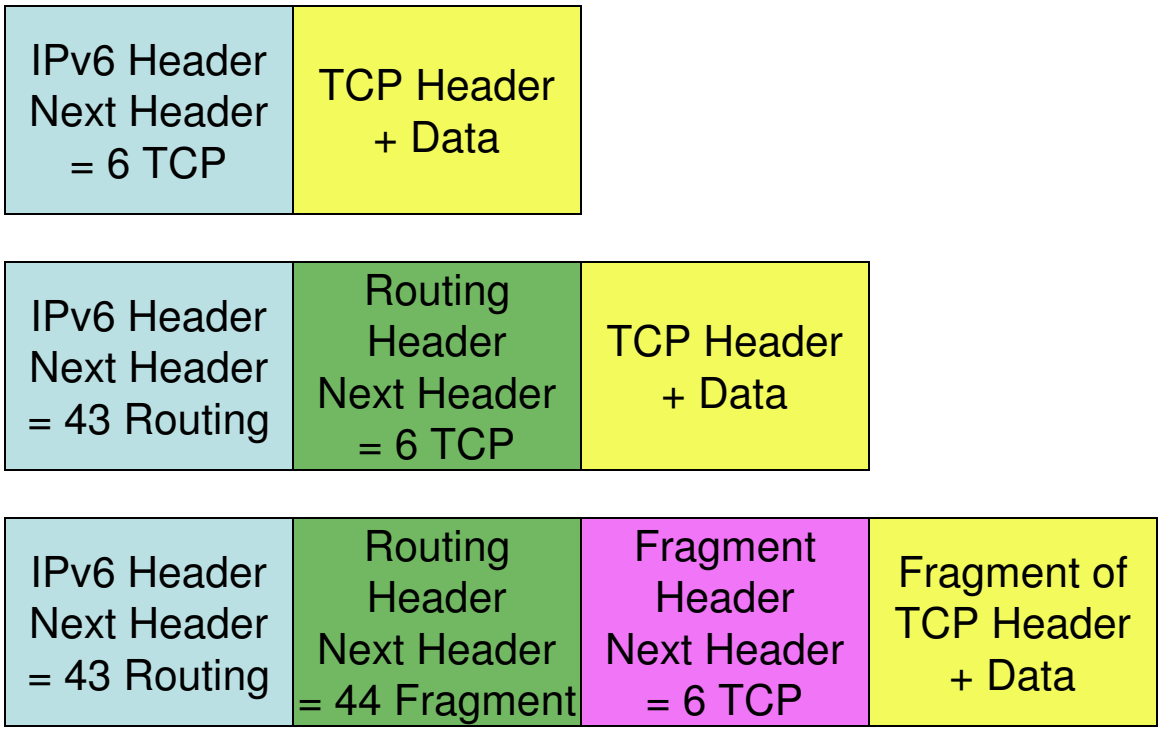


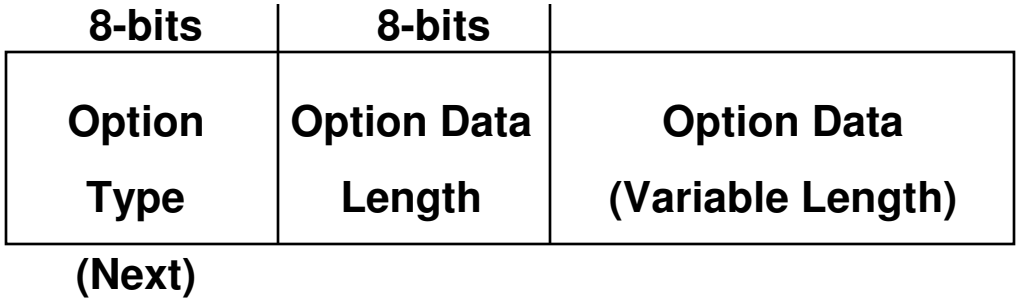
Global Technology Resources, Inc.

ICMPv6 Threats

- Allow the following ICMPv6 packets inbound from the Internet
  - Type 1, Code 0 – No route to destination
  - Type 3 – Time Exceeded
  - Type 128 and Type 129 – Echo request and Echo reply
- Allow the following ICMPv6 packets through the firewall
  - Type 2 – Packet too big – PMTUD
  - Type 4 – Parameter problem
- Allow the following ICMPv6 packets to and from the firewall itself
  - Type 2 – Packet too big – PMTUD
  - Type 4 – Parameter problem
  - Type 130, 131, 132, 143 – Multicast Listener Discovery
  - Type 133 and Type 134 – Router Solicitation and Router Advertisement
  - Type 135 and Type 136 – Neighbor Solicitation and Neighbor Advertisement

IPv6 Extension Headers





Next Header Field:

0 – Hop-by-Hop Options

60 – Destination Options

(If Routing header is used)

43 – Routing

44 – Fragment

46 – RSVP

51 – AH

50 – ESP

88 – EIGRP

89 – OSPF

6 – TCP

17 – UDP

58 – ICMPv6

135 – Mobility Header

59 – None (no next header)

Extension Headers (EHs)

- Header Manipulation – Crafted Packets
- Large chains of extension headers
  - Separate payload into second fragment
  - Consume resources - DoS
- Invalid extension headers – DoS
- Routing headers – source routing
- Cisco ACL Example

```
• no ipv6 source-route
• ipv6 access-list inbound
•  deny ipv6 any any routing
•  deny ipv6 any any undetermined-transport
```

Fragmentation

- In IPv6 routers do not fragment
- IPv6 links must have MTU >=1280
- It is left to the end-systems to perform Path MTU Discovery (PMTUD)
- ICMPv6 – Type 2 - Packet Too Big
- Fragmentation can hide attacks or as an attack itself on the upper layers
  - Overlapping fragments, out of order fragments
- Fragments with less than 1280 bytes should be dropped with the exception of the last fragment
- Fragments destined for network device should be dropped

Layer-3/4 Spoofing

- Spoofing of IPv6 packets
- Hierarchical addressing and ingress/egress filtering
- uRPF Checks (BCP38/RFC 2827)

```
ipv6 access-list RPFACLNAME
 permit IPv6 2001:db8:100:9::/64 any log-input
 deny IPv6 any any log-input
!
interface FastEthernet 0/0
 ipv6 address 2001:db8:100:10::1/64
 ipv6 verify unicast reverse-path RPFACLNAME
```

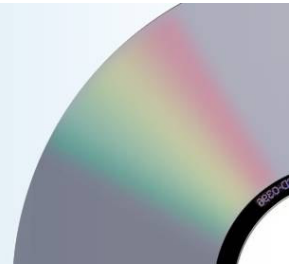
Transition Mechanism Threats

- 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
- 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

Router Threats

- Routing Disruption Attacks
  - Dynamic routing protocols can be exploited
  - Traffic could then be re-routed (Transitive Community Modification)
  - Routing loop, black-hole, gray-hole, detour, asymmetry, partition
- Resource Consumption/Saturation Attacks
  - Injection of extra updates, route requests, or traffic
  - Magnified by the presence of loops or detours
- Buffer Overflow Attacks
- BGP, IS-IS, and EIGRP still use MD5
- OSPFv3 and RIPng use IPSec
- “passive-interfaces” where routing is not needed
- Perform RFC2827 filtering and Unicast Reverse Path Forwarding (uRPF) checks throughout the network and at tunnel endpoints

Application Threats



- Applications for IPv4 and IPv6 are the same
- Buffer overflows, SQL Injection, cross-site scripting will all remain valid attacks on IPv6 servers
- Use of IPSec can prevent many of these attacks that exploit trust between servers
- Completely hierarchal addressing will make trace-back easier but privacy addressing and forged MAC addresses won't
- E-mail/SPAM is still a problem in IPv6 nets
- DNS servers will still be attacked

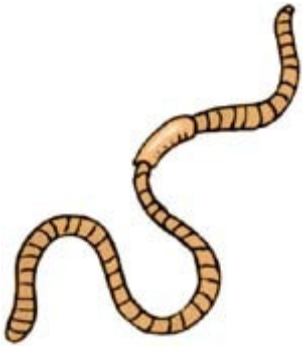
Man-In-The-Middle Threats

- MITM attacks are still possible in IPv6 networks – just like with IPv4
- LAN attacks, sniffing, spoofing the default gateway
- IPSec with both AH and ESP will help immensely
- SeND and CGAs will hopefully make these attacks less common on the LAN

Flooding – DDoS

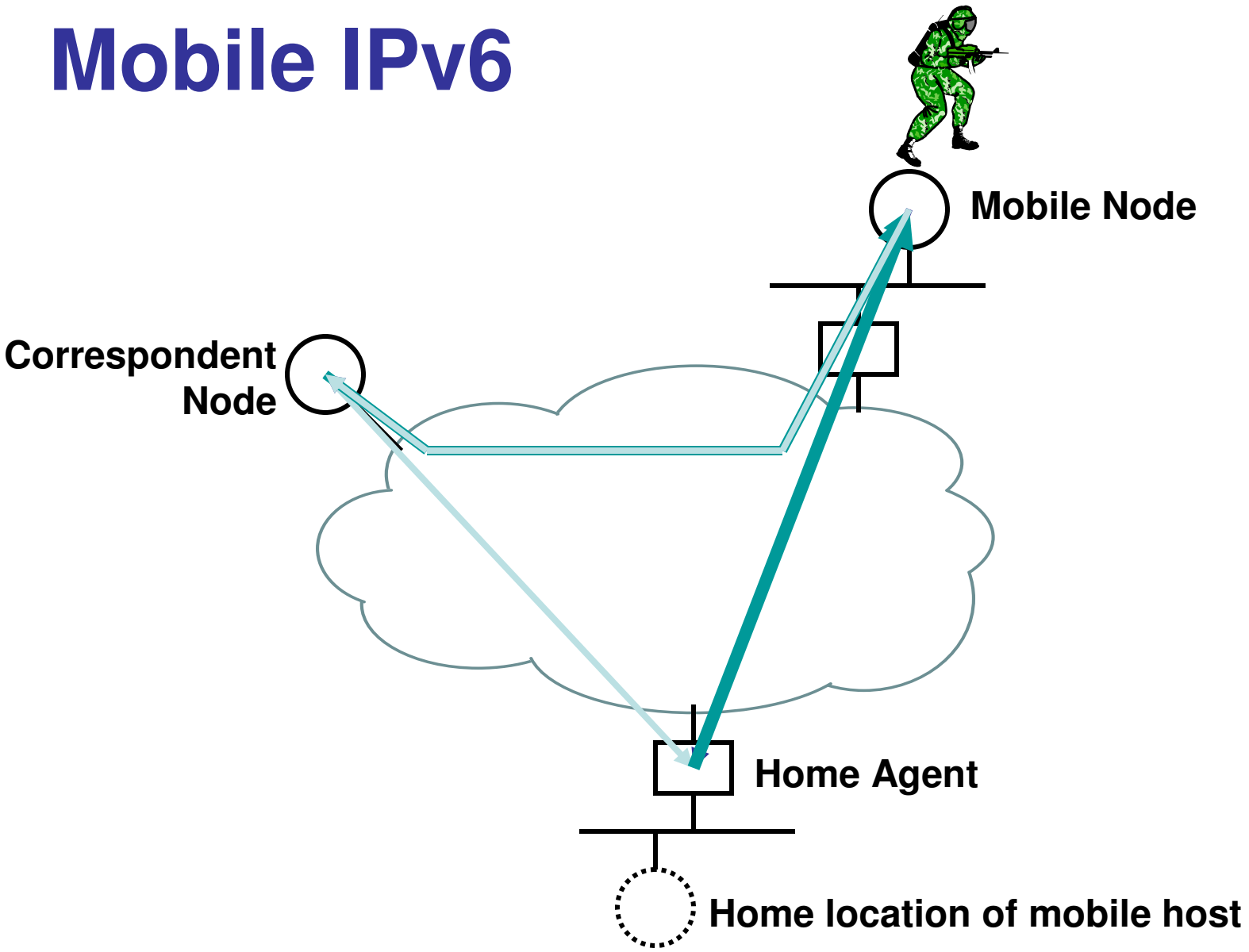
- IPv6 doesn't use broadcast only multicast – Smurf attacks more difficult
  - FF02::1 - All Nodes Address
  - FF02::2 - All Routers Address
  - FF05::1 – All Site Local Nodes
  - FF05::1:3 – All DHCPv6 servers
  - Tightly control who can send to multicast groups
- ICMPv6 error message should not be generated in response to a packet with a multicast destination address
- DDOS attacks can still exist on the IPv6 Internet just like they exist on IPv4 Internet
  - Document your procedures for "last-hop traceback" ahead of time – work with your ISP

Viruses and Worms



- Viruses will be the same with IPv6
- Worms like Sapphire/SQL Slammer won't spread as quickly
- "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
- Perform ingress/egress filtering and uRPF checks throughout the network and at the perimeter

Mobile IPv6



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
- Attacker could be a fake MN or a rogue Home Agent
- If you don't use MIPv6 then filter it
- Firewalls don't have state information on who is roaming and who isn't
- Binding update filtering on the Layer-3 HAs
- IPSec can be used with MIPv6 but some mobile devices don't have the resources
- Return Routability Test

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
- Bogon and anti-spoofing filters are a MUST
- 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 ND/NS/NUD/RA/RS messages

Firewalls with IPv6 Support

- Cisco Router ACLs, Reflexive ACLs, IOS-based Firewall, PIX, ASA
- CheckPoint >R60 (R62 on SplatPro)
- Juniper Screen OS
- Fortinet 3.0 MR5
- ip6tables, ip6fw, ipf, pf
- Windows XP SP2, Vista IPv6 Internet Connection Firewall

IPv6 Intrusion Prevention

- Few signatures for IPv6 exist
- IPSs should send out notifications when non-conforming IPv6 packets are observed
- Faulty parameters, bad extension headers, source address is a multicast address
- Snort 2.0.0 beta – Snort 3.0
- CheckPoint (NFR) Sentivist
- Cisco 4200 IDS appliances
- ISS Proventia/RealSecure

Hardening Network Devices

- “no ipv6 redirect” on interfaces
- Telnet and SSH work over IPv6 so use IPv6 Access-Class
  - **`ipv6 access-list V6ACCESS`**
  - **`  permit ipv6 2001:db8:10:10::1/128 any`**
  - **`line vty 0 4`**
  - **`  ipv6 access-class V6ACCESS in`**
- Use Control Plane Policing for IPv6

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 reality
- 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

- 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
  - EUI-64 addresses are derived from the host's MAC
  - That could be used to track user's activity and thus identity
- 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

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 over dynamic tunnels
- Leverage IPSec for everything possible
- Try to achieve equal protections for IPv6 as with IPv4

Conclusions

- 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 changed traffic patterns (p2p, MIPv6)
- IPv6 larger addresses makes worms less effective
- IPv6 hierarchical addressing should reduce the anonymity of hackers
- IPv6 IPSec will become popular
- LAN-based attacks exist in IPv6
- IPv6 hosts have multiple IPv6 addresses
- Securing IPv6 multicast will be a challenge

Question and Answer

SHogg@GTRI.com
Scott@HoggNet.com

Mobile: 303-949-4865

Global Technology Resources, Inc.