IPv6 Security Threats and Mitigations
Agenda

- Debunking IPv6 Myths
- Shared Issues by IPv4 and IPv6
- Specific Issues for IPv6
  - Extension headers, IPsec everywhere, transition techniques
- Enforcing a Security Policy in IPv6
IPv6 Security Myths…
Is IPv6 (a teenager) really ‘better and more secure’?
The Absence of Reconnaissance Myth

- Default subnets in IPv6 have $2^{64}$ addresses
  - 10 Mpps = more than 50,000 years
Reconnaissance in IPv6
Scanning Methods Are Likely to Change

- Public servers will still need to be DNS reachable
  ⇒ More information collected by Google...

- Increased deployment/reliance on dynamic DNS
  ⇒ More information will be in DNS

- Using peer-to-peer clients gives IPv6 addresses of peers

- Administrators may adopt easy-to-remember addresses (::{10},::{20},::{F00D},::{C5C0},::{ABBA:BABE} or simply IPv4 last octet for dual stack)

- By compromising hosts in a network, an attacker can learn new addresses to scan
Viruses and Worms in IPv6

- Viruses and email, IM worms: IPv6 brings no change
- Other worms:
  - IPv4: reliance on network scanning
  - IPv6: not so easy (see reconnaissance) => will use alternative techniques

- Worm developers will adapt to IPv6
- IPv4 best practices around worm detection and mitigation remain valid
Scanning Made Bad for CPU
Remote Neighbor Cache Exhaustion

- Potential router CPU/memory attacks if aggressive scanning
  - Router will do Neighbor Discovery... And waste CPU and memory

```
2001:db8::/64
NS: 2001:db8::1
NS: 2001:db8::2
NS: 2001:db8::3
NS: 2001:db8::1
NS: 2001:db8::2
NS: 2001:db8::3
```

2001:db8::1
2001:db8::2
2001:db8::3

2001:db8::/64
Mitigating Remote Neighbor Cache Exhaustion

- Built-in rate limiter but no option to tune it
  - Since 15.1(3)T: `ipv6 nd cache interface-limit`
  - Or IOS-XE 2.6: `ipv6 nd resolution data limit`
  - Destination-guard is coming with First Hop Security phase 3

- Using a /64 on **point-to-point links** => a lot of addresses to scan!
  - Using /127 could help (RFC 6164)

- **Internet edge/presence**: a target of choice
  - Ingress ACL permitting traffic to specific statically configured (virtual) IPv6 addresses only

- Using infrastructure ACL prevents this scanning
  - iACL: edge ACL denying packets addressed to your routers
  - Easy with IPv6 because new addressing scheme can be done 😊
Reconnaissance in IPv6? Easy with Multicast!

- No need for reconnaissance anymore
- 3 site-local multicast addresses (not enabled by default)
  - FF05::2 all-routers, FF05::FB mDNSv6, FF05::1:3 all DHCP servers
- Several link-local multicast addresses (enabled by default)
  - FF02::1 all nodes, FF02::2 all routers, FF02::F all UPnP, …

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacker</td>
<td>FF05::1:3</td>
<td>DHCP Attack</td>
</tr>
</tbody>
</table>

http://www.iana.org/assignments/ipv6-multicast-addresses/

BRKSEC-2003 © 2012 Cisco and/or its affiliates. All rights reserved. Cisco Public
The IPsec Myth: IPsec End-to-End will Save the World

- “IPv6 mandates the implementation of IPsec”
- Some organizations believe that IPsec should be used to secure all flows…

“We’ve devised a new security encryption code. Each digit is printed upside down.”
The IPsec Myth:
IPsec End-to-End will Save the World

- IPv6 originally mandated the implementation of IPsec (but not its use)
- Now, RFC 6434 “IPsec SHOULD be supported by all IPv6 nodes”
- Some organizations still believe that IPsec should be used to secure all flows...
  - Interesting scalability issue (n^2 issue with IPsec)
  - Need to trust endpoints and end-users because the network cannot secure the traffic: no IPS, no ACL, no firewall
  - IOS 12.4(20)T can parse the AH
  - Network telemetry is blinded: NetFlow of little use
  - Network services hindered: what about QoS?

**Recommendation:** do not use IPsec end to end within an administrative domain.

**Suggestion:** Reserve IPsec for residential or hostile environment or high profile targets EXACTLY as for IPv4
The No Amplification Attack Myth
IPv6 and Broadcasts

- There are no broadcast addresses in IPv6
- Broadcast address functionality is replaced with appropriate link local multicast addresses
  - Link Local All Nodes Multicast—FF02::1
  - Link Local All Routers Multicast—FF02::2
  - Link Local All mDNS Multicast—FF02::FB

- **Note:** anti-spoofing also blocks amplification attacks because a remote attacker cannot masquerade as his victim

http://iana.org/assignments/ipv6-multicast-addresses/
Shared Issues
IPv6 Bogon and Anti-Spoofing Filtering

- Anti-spoofing = uRPF

IPv6 Unallocated Source Address

IPv6 Intranet

Inter-Networking Device with uRPF Enabled

IPv6 Intranet/Internet

No Route to SrcAddr => Drop
Neighbor Discovery Issue#1
Stateless Autoconfiguration

**Router Solicitations** Are Sent by Booting Nodes to Request Router Advertisements for Stateless Address Auto-Configuring

1. **RS:**
   - **Src** = ::
   - **Dst** = All-Routers multicast Address
   - **ICMP Type** = 133
   - **Data** = Query: please send RA

2. **RA:**
   - **Src** = Router Link-local Address
   - **Dst** = All-nodes multicast address
   - **ICMP Type** = 134
   - **Data** = options, prefix, lifetime, **autoconfig** flag

**RA/RS w/o Any Authentication**
Gives Exactly Same Level of Security as ARP for IPv4 (None)

**Attack Tool:**
fake_router6

Can Make Any IPv6 Address the Default Router
Neighbor Discovery Issue#2
Neighbor Solicitation

Src = A
Dst = Solicited-node multicast of B
ICMP type = 135
Data = link-layer address of A
Query: what is your link address?

Src = B
Dst = A
ICMP type = 136
Data = link-layer address of B

A and B Can Now Exchange Packets on This Link

Security Mechanisms Built into Discovery Protocol = None
=> Very similar to ARP

Attack Tool: Parasite6
Answer to all NS, Claiming to Be All Systems in the LAN...
ARP Spoofing is now NDP Spoofing: Mitigation

- **SEMI-BAD NEWS**: nothing yet like dynamic ARP inspection for IPv6
  - First phase (Port ACL & RA Guard) available since Summer 2010
  - Second phase (NDP & DHCP snooping) starting to be available since Summer 2011

- **GOOD NEWS**: Secure Neighbor Discovery
  - SeND = NDP + crypto
  - IOS 12.4(24)T
  - But not in Windows Vista, 2008 and 7, Mac OS/X, iOS, Android
  - Crypto means slower...

- Other **GOOD NEWS**:
  - Private VLAN works with IPv6
  - Port security works with IPv6
  - IEEE 802.1X works with IPv6 (except downloadable ACL)
RA-Guard

Goal: mitigate against rogue RA

- Switch selectively accepts or rejects RAs based on various criteria's
- Can be ACL based, learning based or challenge (SeND) based.
- Hosts see only allowed RAs, and RAs with allowed content

Configuration-based
- Learning-based
- Challenge-based

Verification succeeded?

Router Advertisement Option: prefix(s)

“I am the default gateway”
ICMPv4 vs. ICMPv6

- Significant changes
- More relied upon

<table>
<thead>
<tr>
<th>ICMP Message Type</th>
<th>ICMPv4</th>
<th>ICMPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity Checks</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Informational/Error Messaging</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Fragmentation Needed Notification</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Address Assignment</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Address Resolution</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Router Discovery</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Multicast Group Management</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Mobile IPv6 Support</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

=> ICMP policy on firewalls needs to change
Information Leak with Hop-Limit

- IPv6 hop-limit has identical semantics as IPv4 time-to-live
- Can be leveraged by design
  - To ensure packet is local iff hop-limit = 255
  - Notably used by Neighbor Discovery
- Can be leveraged by malevolent people
  - Guess the remote OS: Mac OS/X always set it to 64
  - Evade inspection: hackers send some IPv6 packets analyzed by the IPS but further dropped by the network before reaching destination… Could evade some IPS
  - Threat: low and identical to IPv4
Quick Reminder
IPv4 Broadcast Amplification: Smurf

160.154.5.0

ICMP REQ D=160.154.5.255 S=172.18.1.2

ICMP REPLY D=172.18.1.2 S=160.154.5.14
ICMP REPLY D=172.18.1.2 S=160.154.5.15
ICMP REPLY D=172.18.1.2 S=160.154.5.16
ICMP REPLY D=172.18.1.2 S=160.154.5.17
ICMP REPLY D=172.18.1.2 S=160.154.5.18
ICMP REPLY D=172.18.1.2 S=160.154.5.19

Attempt to Overwhelm Destination

172.18.1.2

Belgian Schtroumpf
IPv6 Attacks with Strong IPv4 Similarities

- **Sniffing**
  - IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

- **Application layer attacks**
  - The majority of vulnerabilities on the Internet today are at the application layer, something that IPSec will do nothing to prevent

- **Rogue devices**
  - Rogue devices will be as easy to insert into an IPv6 network as in IPv4

- **Man-in-the-Middle Attacks (MITM)**
  - Without strong mutual authentication, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4

- **Flooding**
  - Flooding attacks are identical between IPv4 and IPv6
Specific IPv6 Issues
IPv6 Privacy Extensions (RFC 3041)

- Temporary addresses for IPv6 host client application, e.g. web browser
  - Inhibit device/user tracking
  - Random 64 bit interface ID, then run Duplicate Address Detection before using it
  - Rate of change based on local policy
- Enabled by default in Windows, Android, iOS

Recommendation: Use Privacy Extensions for External Communication but not for Internal Networks (Troubleshooting and Attack Trace Back)
IPv4 to IPv6 Transition Challenges

- 16+ methods, possibly in combination

- Dual stack
  - Consider security for both protocols
  - Cross v4/v6 abuse
  - Resiliency (shared resources)

- Tunnels
  - Bypass firewalls (protocol 41 or UDP)
  - Can cause asymmetric traffic (hence breaking stateful firewalls)
Dual Stack with Enabled IPv6 by Default

- Your host:
  - IPv4 is protected by your favorite personal firewall...
  - IPv6 is enabled by default (Vista, Linux, Mac OS/X, ...)
- Your network:
  - Does not run IPv6
- Your assumption:
  - I’m safe
- Reality
  - You are not safe
  - Attacker sends Router Advertisements
  - Your host configures silently to IPv6
  - You are now under IPv6 attack
- => Probably time to think about IPv6 in your network
Dual Stack Host Considerations

- Host security on a dual-stack device
  - Applications can be subject to attack on both IPv6 and IPv4
  - **Fate sharing**: as secure as the least secure stack...

- Host security controls should block and inspect traffic from both IP versions
  - Host intrusion prevention, personal firewalls, VPN clients, etc.

Dual Stack VPN Client

IPv4 IPsecVPN with No Split Tunneling

IPv6 HDR IPv6 Exploit

Does the IPsec Client Stop an Inbound IPv6 Exploit?
Bored at BRU Airport on a Sunday at 22:00

$ ifconfig en1
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
ether 00:26:bb:xx:xx:xx
inet6 fe80::226:bbff:fexx:xxxx%en1 prefixlen 64 scopeid 0x6
inet 10.19.19.118 netmask 0xfffffe00 broadcast 10.19.19.255
media: autoselect status: active

$ ping6 -I en1 ff02::1%en1
PING6(56=40+8+8 bytes) fe80::226:bbff:fexx:xxxx%en1, 40 bytes from fe80::226:bbff:fexx:xxxx%en1, icmp_seq=0 hlim=64 time=0.140 ms
. . .
16 bytes from fe80::cabc:c8ff:fec3:fdef%en1, icmp_seq=3 hlim=64 time=402.112 ms
^C
--- ff02::1%en1 ping6 statistics ---
4 packets transmitted, 4 packets received, +142 duplicates, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.140/316.721/2791.178/412.276 ms

$ ndp -an
Neighbor
---

Humm... Is there an IPv6 Network?
Humm... Are there any IPv6 peers?

Let's have some fun here... Configure a tunnel, enable forwarding and transmit RA
Enabling IPv6 in the IPv4 Data Center
The Fool’s Way

1) I want IPv6, send RA

2) Sending RA with prefix for auto-configuration

3) Yahoo! IPv6

IPv4 protection:
iptables

IPv4 Protection:
Security center

IPv6 Protection:
No ip6tables
IPv6 Protection:
No ip6fw
IPv6 Protection:
Security center

4) Default protection…
Enabling IPv6 in the IPv4 Data Center
The Right Way

1) I want IPv6, send RA

2) Sending RA with “no auto-config”

3) Yahoo! Static IPv6 address

IPv4 protection: iptables

3) No IPv6 SLAAC

IPv4 protection: ipfw

3) No IPv6 SLAAC

IPv4 Protection: Security center
L3-L4 Spoofing in IPv6 When Using IPv6 over IPv4 Tunnels

- Most IPv4/IPv6 transition mechanisms have no authentication built in
- => an IPv4 attacker can inject traffic if spoofing on IPv4 and IPv6 addresses

IPv6 ACLs Are Ineffective Since IPv4 & IPv6 Is Spoofed

Tunnel Termination Forwards the Inner IPv6 Packet
Enforcing a Security Policy
IPv6 ACL Implicit Rules
RFC 4890

- Implicit entries exist at the end of each IPv6 ACL to allow neighbor discovery:

```plaintext
permit icmp any any any nd-na
permit icmp any any any nd-ns
deny ipv6 any any any
```

- Nexus 7000 also allows RS & RA
IPv6 ACL Implicit Rules – Cont.
Adding a deny-log

- The beginner’s mistake is to add a deny log at the end of IPv6 ACL

```
... 
! Now log all denied packets
deny ipv6 any any log
! Heu ... I forget about these implicit lines
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

- Solution, explicitly add the implicit ACE

```
... 
! Now log all denied packets
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any log
```
Example: Rogue RA & DHCP Port ACL

```plaintext
ipv6 access-list ACCESS_PORT
  remark for paranoid, block 1st fragment w/o L4 info
  deny ipv6 any any undetermined-transport
  remark Block all traffic DHCP server -> client
  deny udp any eq 547 any eq 546
  remark Block Router Advertisements
  deny icmp any any router-advertisement
  permit ipv6 any any

Interface gigabitethernet 1/0/1
  switchport
  ipv6 traffic-filter ACCESS_PORT in
```

*Note: PACL replaces RACL for the interface (or is merged with RACL ‘access-group mode prefer port’)*

*In August 2010, Nexus-7000, Cat 3750 12.2(46)SE, Cat 4500 12.2(54)SG and Cat 6500 12.2(33)SXl4*
IPv6 ACL to Protect VTY

```
ipv6 access-list VTY
  permit ipv6 2001:db8:0:1::/64 any

line vty 0 4
  ipv6 access-class VTY in
```

**MUST BE DONE** before `ipv6 enable` on any interface!
Summary
Key Take Away

- So, nothing really new in IPv6
  - Reconnaissance: address enumeration replaced by DNS enumeration
  - Spoofing & bogons: uRPF is our IP-agnostic friend
  - NDP spoofing: RA guard and more feature coming
  - ICMPv6 firewalls need to change policy to allow NDP
  - Extension headers: firewall & ACL can process them
  - Amplification attacks by multicast mostly impossible
  - Potential loops between tunnel endpoints: ACL must be used

- Lack of operation experience may hinder security for a while: **training is required**

- Security enforcement is possible
  - Control your IPv6 traffic as you do for IPv4

- Leverage IPsec to secure IPv6 when suitable
Is IPv6 in My Network?

- Easy to check!
- Look inside NetFlow records
  - Protocol 41: IPv6 over IPv4 or 6to4 tunnels
  - IPv4 address: 192.88.99.1 (6to4 anycast server)
  - UDP 3544, the public part of Teredo, yet another tunnel
- Look into DNS server log for resolution of ISATAP
- Beware of the IPv6 latent threat: your IPv4-only network may be vulnerable to IPv6 attacks NOW
Questions and Answers?
Thank you.