Top IPv6 Security Issues Today

And what you can do to mitigate them
Bottom Line Up Front (BLUF)

- Security issues surrounding IPv6 is getting better
- There still remains a lot of work to do
- With the right tools and smart engineering you can mitigate them
Top IPv6 Security Issues

• Issue #1: Accidental IPv6 deployment in an unmanaged IPv4 enterprise
• Issue #2: Malicious IPv6 Deployment
• Issue #3: Security Tools are not capable to protect basic threats
• Issue #4: Mis-configured IPv6 Deployments
• Issue #5: Growing IPv6 Exploitation Tools
• Issue #6: Lack of IPv6 Trained Security Engineers
Issue 1 - Accidental IPv6 Deployment

• All operating systems now include IPv6 on by default – including IPv6 tunnel mechanisms
  – Windows Server 2008 + includes native IPv6, 6to4 and ISATAP
  – Windows Vista+ includes native IPv6, 6to4 and ISATAP (and Teredo when not domain joined)
    • Except when you type: “netsh int teredo set state enterpriseclient”
  – Apple Mac includes native IPv6 (no tunneling by default)
  – Linux (RHEL, SuSE, Ubtuntu) includes native IPv6 (no tunneling by default)
Issue 1 - Accidental IPv6 Deployment

• When these tunnel adapters are enabled they try to “call home”
  – Teredo will attempt IPv6 bubble packets for Teredo relays when an address is received
    • These relays could exist anywhere in the world (use of Anycast, can go up and down)
  – 6to4 will try to access IPv6 internet if protocol 41 is allowed
    • These 6to4 tunnel brokers exist all around the world as well
Issue 1 - Accidental IPv6 Deployment

• These IPv6-enabled nodes are listening for ANYONE to talk to without authentication:
  – Routers, other nodes, etc

Who has fe80:1:2:3:4?
Ooo! Ooo! That’s me!
My IPv6: fe80:1:2:3:4
Issue 2 – Malicious IPv6 Deployment

• Tech-savvy users are learning about ways to avoid detection on un-managed IPv4 networks
  – Bypass firewalls by using IPv6 UDP-based tunnels over non-standard ports for:
    • Bit torrent
    • Data Exfiltration through public cloud services (Google Drive)
  – Accessing IPv6-IPv4 Proxy service from SixXS to reach IPv6-only content: https://www.sixxs.net/tools/gateway/

• Cause havoc on enterprise LANs with internal DoS with expanding tool sets
  – THC-IPv6, Scapy, etc
IPv6 Attacks on the Local Segment

- Man-in-the-Middle Attacks during neighbor advertisement/solicitation
  - Parasite6 – THC-IPv6
  - Spoofs every NS sent out by any host

Who has fe80:1:2:3:4?

Ooo! Ooo! That’s me!

My IPv6: fe80:1:2:3:4
IPv6 Attacks on the Local Segment, cont

• Denial of Service (DoS) or Session Hijacking using a Rogue Router
  – Fake_router6 and/or flood_router6 – THC-IPv6
  – Acts like a router with highest priority
  – Floods route tables and interface address config

Is there an IPv6 router?

DoS!

Oh, and here’s a million RAs!

Me! I am, use me! <pwnd>
IPv6 Attacks on the Local Segment, cont

- **Denial of Service (DoS) with IP conflicts**
  - Dos-new-ip6– THC-IPv6
  - Always responds to a Duplicate Address Detection (DAD) with a positive
  - Hosts will never be able to address their link-local or Global address

Hey, anyone have this address?

Yes, I own that one, try again!

OK, what about this one?

Yep, got that one too! <pwnd>
IPv6 Attacks on the Local Segment, cont

- Denial of Service (DoS) with Neighbor floods
  - `Flood_advertise6` – THC-IPv6
  - Floods all hosts on a network with bogus neighbor advertisements
  - Performance on host IPv6 neighbor tables will degrade and cause a DoS

I feel bloated

- NA for fe80::2
- NA for fe80::3
- NA for fe80::4 <pwnd>
IPv6 Attacks on the Local Segment, cont

- IPv6 Exploitation and Fuzzing attacks
  - fuzz6, exploit6, denial6 – THC-IPv6
  - Runs a series of fuzzing and link-local exploitation attacks on hosts
Issue 3 – Security Tools Lacking

• Every commercial and enterprise-grade firewall and IPS/IDS lack broad threat awareness
  – Native IPv6 with obfuscating Extension Headers
  – Full IPv6 tunnel detection (most only provide basic Teredo and 6to4)
  – Application firewall rules for anything but HTTP/HTTPS and SSH (everything else is wide open)
  – Providing basic SEIM awareness in alerting (most use a modified IPv4 address (e.g. 255.255.2.1 instead of ff02::1)
Issue 3 – Security Tools Lacking

– Most provide basic TCP SYN flood and SMURF attack capability
– No local network awareness on Rogue Router Advertisements, Neighbor Discovery Floods, etc (anything done by THC-IPv6)
– Popular Host-Based IDS tools either break valid IPv6 traffic or provide useless false-positives (need heavy tuning)
Issue 4 – Mis-Configured IPv6

• Not securing IPv6 routing protocols using IPsec
  – OSPFv3 uses IPsec SPIs instead of MD5/SHA
• Switch interfaces not using RA Guard or NDP Guard ACLs/VACLs
• Not auditing IPv6 firewall rules to ensure they match 100% of the IPv4 rules (if you can)
• Not doing X-Forward-For for NAT64/CGN to DMZ servers
  – XFF provides real IPv6 address to translated IPv4 address
Issue 4 – Mis-Configured IPv6

• Perimeter router ACLs:
  – Neighbor Discovery on routed interfaces (DISA STIG issue) \(\rightarrow\) permit this
  – Path MTU Discovery blocked \(\rightarrow\) permit this
  – Allowing Protocol 41 and UDP tunnel ports:
    • 3544, 3545, 5072, 3874, 3740, 3653 \(\rightarrow\) block this

• Not having IPv6 ACLs at all!

• Windows Servers not set with 0x1 DisableComponents
  – Disallow all tunnels
  – Keeping 2002::/16 6to4 prefixes (will break Windows AD)
Issue 4 – Mis-Configured IPv6

• Improperly configuring Windows Direct Access Firewalls
  – Required for DA to function but not allowing ICMPv6 type/codes

• Too reliant on Static IPv6 addressing for servers
  – Use DHCPv6 with static reservations
  – Do not use Stateless Address Autoconfiguration
Issue 5 – Expansion of Exploitation Tools

• More tools are coming out each year built to break IPv6 security:

- THC-IPv6
- IPv6 Toolkit
- Scapy
- Kali Linux
- BackTrack
Issue 6 – Lack of IPv6 Trained Engineers

• Serious implication: Solving IPv6 problems with IPv4 solutions
  – Too different to layer the same broken philosophy

• 28% of survey still thinks NAT is a security “feature”

Mitigating Accidental Deployments

• If you aren’t using it, turn it off with these exceptions:
  – Windows Server and Workstation (set to enable but disable tunneling)
  – Windows Direct Access servers require Teredo and 6to4 to be enabled

• Audit your Security Tools for views into internal IPv6:
  – Ensure SPAN/Taps are configured to see all multicast traffic (this is where NDP lives)

• Lock-Down IPv6 on the end-node (use a host-based IDS/IPS, but spend time testing rules)
Mitigating Malicious Deployments

- Lock-Down IPv6 on the end-node (use a host-based IDS/IPS, but spend time testing rules)
- Monitor SEIM tools for odd behavior over DNS
  - Many UDP-based tunnel tools can use ports allowed on the end nodes like DNS (UDP port 53)
Mitigating Security Tools

• This is a difficult thing to mitigate
• Start by auditing what you have and ask them the tough *and* specific questions about what they can or can’t do
• Get with me after if you want details on your vendors
Mitigating Mid-Configured Deployments

• Follow IPv6 best practices
  – OSPFv3 authentication in Cisco: [OSPFv3 Cisco](#)
  – OSPFv3 authentication (address families) in Cisco: [OSPFv3 AF in Cisco](#)
  – EIGRP IPv6 Authentication: [EIGRP Authentication](#)
  – Cisco Implementing First-Hop Security
  – Microsoft IPv6 DisableComponents key settings: [http://support.microsoft.com/kb/929852](http://support.microsoft.com/kb/929852)
Mitigating IPv6 Training

• Training for security personnel should never be a “nice-to-have”
  – They are the first to spot attacks (or not spot)
• There are many good IPv6 training programs out there
• Get started with these:
Summary

• There are six very important security issues
• Lack of IPv6 training is the most important
• Follow good security practice and industry recommendations
• Audit your security vendors now
• Be very intentional about your IPv6 deployment
Questions?
Backup Slides
What an IPv6 Extension Header Looks Like


Version: 6

[0110 .... = This field makes the filter "ip.version == 6" possible: 6]

[0110 .... = This field makes the filter "ip.version == 6" possible: 6]

[0110 .... = This field makes the filter "ip-version == 6" possible: 6]

Header: IPv6 Extension Header

Next header: IPv6 extension header (0x2c)
Hop limit: 64


Fragmentation Header

Next header: IPv6 extension header (0x2c)
Offset: 0 (0x0000)
More Fragment: 0
Identification: 0x00000000

Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: http (80), Seq: 0, Len: 0


Version: 6

[0110 .... = This field makes the filter "ip-version == 6" possible: 6]

[0110 .... = This field makes the filter "ip-version == 6" possible: 6]

[0110 .... = This field makes the filter "ip-version == 6" possible: 6]

Header: IPv6 Extension Header

Next header: TCP (0x06)


Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: http (80), Seq: 0, Len: 0


Version: 6

[0110 .... = This field makes the filter "ip.version == 6" possible: 6]

[0110 .... = This field makes the filter "ip-version == 6" possible: 6]

[0110 .... = This field makes the filter "ip-version == 6" possible: 6]

Header: IPv6 Extension Header

Next header: TCP (0x06)


Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: http (80), Seq: 0, Len: 0

Encapsulating Security Payload

ESP SPI: 0x00140050
ESP Sequence: 0
RH0 Extension Header Attack

ICMPv6 Probe to Salient’s router w/ source routing..

Unknown UDP data sent (source port 80, destination port 36666)

Because Salient Router was not online
If Salient router had been online…

ICMPv6 Probe to Salient’s router w/ source routing.

Malicious traffic from authorized network (using Salient as friendly network to attack from)
Tunnels Need to be Protected

ACLs can protect against Protocol 41, 47, IPSec and port specific UDP traffic

What if you don’t know the Port?

Miredo: Teredo configured to run on any port
GoGoNet6: TSP can listen on any UDP port (i.e. 53, 80, 443, etc)
Typically Undetectable UDP Tunnel
uTorrent – Teredo Peers

- uTorrent runs well over Teredo
- BitTorrent community is discovering IPv6
Vuze – IPv6 Peers

• Vuze (formerly Azureus) is another fully IPv6-enabled bit torrent client

• See how easy it is to “prefer” IPv6!

<table>
<thead>
<tr>
<th>System</th>
<th>Address</th>
<th>μTorrent 1.8.3</th>
<th>L</th>
<th>Azureus 4.4.0.4</th>
<th>R</th>
<th>μTorrent Mac 1.0</th>
<th>R</th>
<th>Download Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>ubuntu-10.04-desktop</td>
<td>89.133.83.39</td>
<td>100.0%</td>
<td></td>
<td>99.2%</td>
<td></td>
<td>100.0%</td>
<td></td>
<td>146 B/s</td>
</tr>
<tr>
<td>ubuntu-10.04-desktop</td>
<td>62.83.35.208</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0 B/s</td>
</tr>
<tr>
<td>ubuntu-10.04-desktop</td>
<td>2607:f2c0:f00e:5b00:217:f2ff:fee7:6a4c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6.8 kB/s</td>
</tr>
</tbody>
</table>
IPv4 “AAAA” DNS Queries Broadcast IPv6

- Microsoft Dual Stack enabled on ALL Windows 7/8/Server 2008 systems
- AAAA Queries present on every network we monitored.
- Considered ‘harmless’ by many mainstream security and network engineers
- Must be disabled by DoD MO2 guidelines (section 3.3.6.1)
  - “AAAA records may not transit beyond the intra-enclave security zone”
IPv4 “AAAA” DNS—The Loaded Gun

- Remote Hacker sees an organization sending 100,000+ AAAA queries a day
- Hacker Floods an organization’s mail servers with SPAM
  - It only takes one user with elevated privileges to open one SPAM message to execute the encapsulated malware
  - Consider MS 10-009, “New Ping of Death,” and MS10-029 as examples
- Malware establishes an IPv6 in UDP tunnel through an organization’s firewall to Remote Hacker on UDP port 53
  - Such as Miredo or GoGoNet6
- Remote Hacker exfiltrates sensitive data from an organization’s enterprise network
  - Health record data/confidential patient records
ICMPv6 is Required for IPv6

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Destination Unreachable</td>
</tr>
<tr>
<td>2</td>
<td>Packet to Big</td>
</tr>
<tr>
<td>3</td>
<td>Time exceeded</td>
</tr>
<tr>
<td>4</td>
<td>Parameter problem</td>
</tr>
<tr>
<td>128</td>
<td>Echo Request</td>
</tr>
<tr>
<td>129</td>
<td>Echo Reply</td>
</tr>
<tr>
<td>130</td>
<td>Multicast Listener Query – sent to ff02::1 (all nodes)</td>
</tr>
<tr>
<td>131</td>
<td>Multicast Listener Report</td>
</tr>
<tr>
<td>132</td>
<td>Multicast Listener Done – sent to ff02::2 (all routers)</td>
</tr>
<tr>
<td>133</td>
<td>Router Solicitation (RS) – sent to ff01::2 (all routers)</td>
</tr>
<tr>
<td>134</td>
<td>Router Advertisement (RA) – sent to ff01::1 (all nodes)</td>
</tr>
<tr>
<td>135</td>
<td>Neighbor Solicitation (NS) – sent to ff02:0:0:0:0:1:ff00::/104</td>
</tr>
<tr>
<td>136</td>
<td>Neighbor Advertisement (NA)</td>
</tr>
<tr>
<td>137</td>
<td>Redirect message</td>
</tr>
</tbody>
</table>
Rogue RAs: the threat inside

- IPv6-enabled workstations (untouched Vista, 7/8, Server 2008/2012, Linux, Mac, etc) *always* listen for Router Advertisements
- User A downloads some pesky malware
  - Sets up tunnel like the non-standard UDP port example (or port 53)
  - Installs basic router advertisement daemon & IPv6 forwarding
- It sends RAs out to those IPv6-enabled machines with User A as it’s default gateway for IPv6
- Now there is active IPv6 malware on an enterprise that can’t be detected