IPv6 Threats

Nathaniel Richmond

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0644

Agenda

Overview and Context

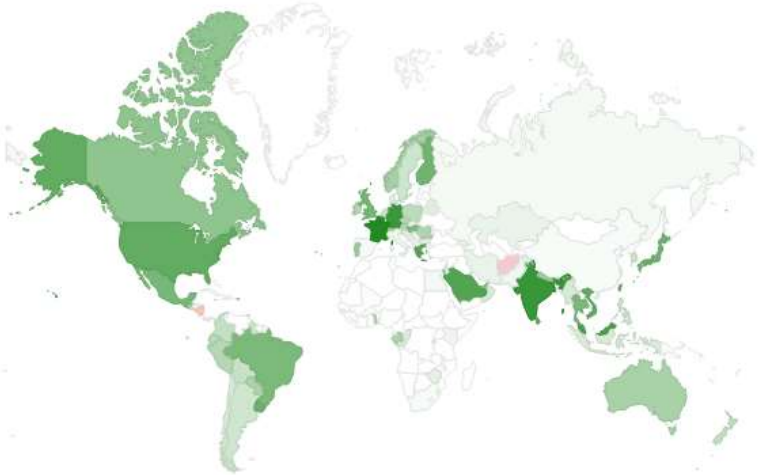
IPv6 and IPv4 Threat Comparison

IPv6 Attacks

Resources

Key Context for Threat Vectors

Per-Country IPv6 adoption



World | Africa | Asia | Europe | Oceania | North America | Central America | Caribbean | South America

The chart above shows the availability of IPv6 connectivity around the world.

- Regions where IPv6 is more widely deployed (the darker the green, the greater the deployment) and users experience infrequent issues connecting to IPv6-enabled websites.
- Regions where IPv6 is more widely deployed but users still experience significant reliability or latency issues connecting to IPv6-enabled websites.
- Regions where IPv6 is not widely deployed and users experience significant reliability or latency issues connecting to IPv6-enabled websites.

https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption

Additional Context for Threat Vectors

Mobile

- IPv6 support varies by carrier
- Most modern phones are capable of IPv6

Cloud

- The big cloud vendors support IPv6, but not universally on all their products and services
- Makes determination of what uses IPv6 and where difficult, plus it can change as support is added or modified

Transition Points

- Translation of IPv4 to IPv6 and vice versa
- Tunneling of various types

Additional Context for Threat Vectors

Experience and Implementation

- IPv6 policies and IPv4 policies may have similar goals but different implementations at Policy Enforcement Points (PEP).
  - Example: DNS traffic detection and response
  - Example: Firewall and router rules/ACLs
- Do operators and analysts have the experience with IPv6 that they have with IPv4?

IPv6 and IPv4 Similarities

Sniffing

Application Layer

Rogue Devices (Physical Layer)

Attacker-in-the-Middle

Flooding

Do you see a lot of IPv6 oddities? Will it be harder to baseline normal traffic?

https://www.hpc.mil/images/hpcdocs/ipv6/cisco_ipv6_and_ipv4_threat_comparison_and_best_practice_0304.pdf

IPv6 Attacks

Reconnaissance

- Huge number of addresses makes host and service discovery much different
- Attackers can use multicasts if not filtered at security boundaries
- Many IPv4 recommended practices like default deny, IP filtering, and more will still apply to IPv6

IPv6 Attacks

Unauthorized Access

- Site-to-site traffic may be direct instead of via VPN, resulting in potential eavesdropping or injection.
- Disparities between IPv4 PEPs (mature) and IPv6 PEPs (less mature) are likely to create issues.
- Temporary addresses can make ACLs and other controls more difficult to define and manage.
- Router advertisements can also be vulnerable without router advertisement guard (RA guard).

IPv6 Attacks

Header Manipulation and Fragmentation

- Header manipulation could potentially cause the default ”accept” of IPv6 packets to also process headers and forward the packet(s).
- RFC 2460 dictates that fragments should not overlap (different from IPv4), so they can be dropped if they do overlap.
- Out-of-order packets could still be potentially used to bypass detection, similar to IPv4 and old IDS evasions.

IPv6 Attacks

Spoofing Layer 3 and Layer 4

- Can use similar address filtering in IPv6 compared to IPv4 to prevent spoofing outside the source network range.
- The huge size of network ranges means attackers have lots of addresses to choose from even with address filtering in place.

IPv6 Attacks

ARP and DHCP attacks compared to IPv6

- Stateless configuration for IPv6 means DHCP does not have to be ubiquitous, but can still be an attack vector
- Neighbor Discovery Protocol (NDP) replaces ARP
- NDP can use Securing Neighbor Discovery (SEND) as a security extension – RFC 3971 and RFC 6494

IPv6 Attacks

Routing and Router Protocol Attacks

- Mismatched vendor implementations could cause issues.
- Routing protocols are spotty in terms of how they handle IPv6
  - BGP and Intermediate System to Intermediate System (IS-IS) both extended to support IPv6 to some degree.
  - OSPF and RIP need IPsec
- Example: CVE-2020-16898 “Bad Neighbor” attack allows remote code execution on Windows because of improperly handled ICMPv6 Router Advertisement packets

IPv6 Attacks

Translation, Transition, and Tunneling

- Tunneling can be used for evasion of detection rules or protection rules (e.g. firewall rules)
- Translation can also make it more difficult to trace attacks for cyber threat intelligence purposes
- Automatic tunneling may not be secure (packet forgery, DoS?)
- Example: Windows IPv6 or 6to4 tunnel for Windows SMB to bypass firewall IPv4 firewall rules. See “Exfiltration with IPv6 tunnels on Windows” at https://insights.sei.cmu.edu/blog/exfiltration-with-ipv6-tunnels-on-windows/
- Other examples?

Other Concerns

Automatic addressing (SLAAC) and other options for IPv6 introduce a lot of flexibility, which in turn makes asset management, ACLs, and understanding topology more difficult.

NDP can be susceptible to Denial-of-Service (accidentally or on purpose) through cache exhaustion.

Resources

CISA's "Internet Protocol Version 6 Considerations for Trusted Internet Connections 3.0"

- https://www.cisa.gov/sites/default/files/publications/CISA%20IPv6%20Considerations%20for%20TIC%203.0.pdf

Cisco's "IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation"

- https://www.hpc.mil/images/hpcdocs/ipv6/cisco_ipv6_and_ipv4_threat_comparison_and_best_practice_0304.pdf

RFC 3971 and RFC 6494 (and more)

- https://www.rfc-editor.org/rfc/rfc3971.html
- https://www.rfc-editor.org/rfc/rfc6494