IPv6 Security

Different, but almost the same

Carsten Strotmann

CREATED: 2025-01-30 THU 09:47

Agenda

- IPv6 Security Issues
- Tools

IPv6 Security Issues

Security and IPv6

- IPv6 is now over 25 years old
    - It inherits many design decisions from IPv4
    - It also inherits the security shortcomings from IPv4
    - Most IPv6 security issues are also available on IPv4
    - Some IPv4 security issues don't exist on IPv6
    - Some new security issues have been introduced by IPv6

- ↪ISOC IPv6 Security FAQ (PDF)
- ↪RFC 9099 "Operational Security Considerations for IPv6 Networks"

ICMPv6 neighbor solicitation/advertisement spoofing

- Neighborhood Discovery is un-authenticated
  - An "on-link" attacker can spoof or alter ND messages
  - DoS attacks (e.g. Duplicate Address Detection DoS)
  - MITM attacks
    - spoofed Address Resolution Responses
    - Router Redirection spoofing
- ↪RFC 3756 "IPv6 Neighbor Discovery (ND) Trust Models and Threats"

ICMPv6 neighbor solicitation/advertisement spoofing

- Possible mitigation
    - Secure Neighborhood Discovery (SeND) ↪RFC 3971 "SEcure Neighbor Discovery (SEND)"
        - Unfortunately, SeND is not well supported by current Operating Systems and difficult to deploy

- Host isolation - assigning a /64 prefix per node
    - all communication must pass though a router (that should be a filtering device), no direct node-to-node traffic is permitted
    - ↪RFC 8273 "Unique IPv6 Prefix per Host"

Router spoofing

- Attacker (for example via malware/trojan software) can activate a "fake" router in the network
    - Denial-Of-Service attack
    - Men-in-the-Middle (MITM) attack

- ↪RFC 6104 "Rogue IPv6 Router Advertisement Problem Statement"

Router spoofing

- Possible mitigation
  - Secure Neighborhood Discovery (SeND) ↪RFC 3971 "SEcure Neighbor Discovery (SEND)"
    - Unfortunately, SeND is not well supported by current Operating Systems and difficult to deploy
  - ↪RFC 6105 "IPv6 Router Advertisement Guard"

DHCP spoofing

- Attacker can launch malicious DHCPv6 server (via malware/trojan software)
    - Distribute wrong network configuration
    - Distribute wrong IPv6 addresses
    - Creates MITM and DoS attack possibilities
- Mitigation
    - "*DHCP Shield*" in Layer 2 devices
    - ↪RFC 7610 "DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers"

Spoofed DNS Resolver in Router Advertisements

- Router Advertisements (RA) messages are not authenticated
    - Attacker can spoof this messages with any content
    - The RA can contain the IP-Addresses of DNS resolver to be used
    - By changing the DNS resolver of clients, an attacker can redirect or manipulate network traffic

Spoofed DNS Resolver in Router Advertisements

- Mitigation
  - Use of DNSSEC for security critical domains (e.g. internal Active Directory)
  - Use of authenticated DNS-over-TLS/DNS-over-HTTPS (using x509 certificates)
  - Distribute manual configured DNS resolver addresses (through configuration management systems)
  - Use of manual configured site-local multicast addresses for DNS resolver

Router/Neighborhood Advertisements Flooding (DoS)

- Attackers can trigger a high number of Neighborhood-Discovery (ND) events from a Router or from network devices, for example through a network scan
  - The high number of events can create a denial-of-service attack onto the router infrastructure

- Mitigation strategies
  - Rate-Limiting of ND events
  - Filter (parts of) the unused address space
  - For Router-to-Router connections, use a /127 network prefix
  - Using only link-local addresses on links where there are only routers

- ↪RFC 6583 "Operational Neighbor Discovery Problems"

Extension Header attacks

- Creative use of extension headers can create security issues
  - Nested fragmentation
  - Fragmented Extension Headers
  - Overlapping Extension Headers

- Can be used to bypass security appliances and firewalls
- Stealth Data exfiltration via Extension Headers
- ↪IPv6 Extension Headers - New Features, and New Attack Vectors
- ↪RFC 9098 - "Operational Implications of IPv6 Packets with Extension Headers"

Extension Header attacks

- Packets containing wrongly formatted IPv6 extension headers can result in nodes crashing when processing the headers
- A firewall or edge device should be used to enforce the recommended order and the maximum occurrences of extension headers by dropping nonconforming packets
- ↪RFC 9288 - "Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers at Transit Routers"
- Firewalls based on OpenBSD (pf), Linux "nftables" or eBPF, are to be a good choice

Fragmentation Attacks

- Stateless filtering in firewalls can be bypassed by creative use of IPv6 fragmentation headers
- Firewall and security devices should drop first fragments that do not contain the entire IPv6 header chain (including the transport-layer header)
- Destination nodes should discard first fragments that do not contain the entire IPv6 header chain (including the transport-layer header).
- ↪RFC 6980 "Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery"

IPv6 Address Scanning

- it is widely assumed that it would take a huge effort to perform address-scanning attacks against IPv6 networks
    - IPv6 address-scanning attacks have been considered unfeasible

- However based on the "randomness" of the source of IPv6 Interface-IDs, IPv6 address-canning might be possible
    - Manual continuous address assignment
    - IPv6 Interface IDs from "well-known" Hardware-Addresses
    - DHCPv6 Host "reservations"
    - Node-Information-Queries over ICMPv6

IPv6 Address Scanning

- Security should not rely on hiding IPv6 addresses in the vast IPv6 address space (aka "Security by Obscurity")
- See
    - ↪RFC 7707 "Network Reconnaissance in IPv6 Networks"
    - ↪"Mapping the Great Void - Smarter scanning for IPv6", February 2012 (PDF)

Security Implications of Dual-Stack Networks

- Running IPv6 and IPv4 in the same network (aka "Dual-Stack") can create it's own security issues
    - Attacker can choose the weakest protocol
    - Attacker can tunnel one Protocol inside the other to hide

- Security policies need to in sync between IPv6 and IPv4 (Firewall rules, Intrusion Detection systems)
    - Firewalls should allow a common ruleset for IPv6 and IPv4 (use "nftables" not "iptables" on Linux)

Security Implications of Dual-Stack Networks

- Control or block Protocol tunnel technologies (see RFC 9099 for guidance)
- See
  - ↪RFC 4942 "IPv6 Transition/Coexistence Security Considerations"
  - ↪RFC 7123 "Security Implications of IPv6 on IPv4 Networks"
  - ↪RFC 7359 - Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks

Tools

The Hackers Choice IPv6 Toolkit

- The Hackers Choice IPv6 Toolkit is a collection of Linux/Unix command line tools to test the security properties of IPv6 networks
    - "The Hacker's Choice" IPv6 toolkit: ↪https://www.thc.org/
        - Sources: ↪https://github.com/vanhauser-thc/thc-ipv6.git
    - As these tools can also be mis-used for attacks, be careful when using them to test foreign networks

SI6 Toolkit

- A set of IPv6 security assessment and trouble-shooting tools:
  - ↪https://www.si6networks.com/research/tools/ipv6toolk

Chiron

- Chiron is an IPv6 Security Assessment Framework, written in Python and employing Scapy
  - IPv6 Scanner
  - IPv6 Local Link Security Tests
  - IPv4-to-IPv6 Proxy
  - IPv6 Attack Module
  - IPv6 Proxy
- Source: ↪https://github.com/aatlasis/Chiron

Conclusion

Conclusion

- IPv6 is neither more, nor less secure compared to IPv4
- In Dual-Stack networks, Administrators have to deal with security issues of both protocols
    - Attacker have twice the attack space
    - A motivation to move to *IPv6-only* networks sooner (remove IPv4 where possible)

Questions?