Practical Security Assessment of IPv6 Networks and Devices

Fernando Gont

IPv6 Security Summit, Troopers 14
Heidelberg, Germany. March 17-18, 2014
About

- I have done a fair share of IPv6 standardization work
- I have published and maintain the SI6 Networks IPv6 Toolkit
- I run the IPv6 Hackers mailing-list
- References at: http://www.gont.com.ar
- Everyday work:
  
  ![Diagram showing Security Assessment, Producing fixes, and Tools & Testing]

IPv6 Security Summit, Troopers 14
Heidelberg, Germany. March 17-18, 2014

© 2014 SI6 Networks. All rights reserved
"I’ve never met anybody who really did spend blood on something who wasn’t eager to describe what they’ve done and how they did it and why"

-- Ken Thompson (in "Coders at Work: Reflections on the Craft of Programming")

This talk is about SI6 Network’s IPv6 Toolkit, and how to use it for fun & profit.
Disclaimer

Lots of stuff + 30' talk = Fasten your Seatbelts!
Introduction
IPv6 security tools

• It is hard to assess networks and devices without tools
  • “What would happen if I sent this or that packet to this device?”
• For ages, THC-IPv6 was the only IPv6 security tools publicly available
  • Mostly focused on specific vulnerabilities
• We felt the need for a general IPv6 toolkit
SI6 Networks' IPv6 Toolkit: Intro

• Brief history:
  • Produced as part of a project funded by UK CPNI on IPv6 security
  • Maintenance and extension taken over by SI6 Networks

• Goals:
  • Security analysis and trouble-shooting of IPv6 networks and implementations
  • Clean, portable, and secure code
  • Good documentation
SI6 Networks' IPv6 Toolkit: Intro (II)

- **Supported OSes:**
  - Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS
- **License:**
  - GPL (free software)
- **Home:**
- **Collaborative development:**
  - [https://www.github.com/fgont/ipv6toolkit.git](https://www.github.com/fgont/ipv6toolkit.git)
SI6 Networks' IPv6 Toolkit: Philosophy

IDEAS ➔ TOOLS ➔ IPV6 NETWORK

"an interface between your brain and your IPv6 network"

Some find this is NOT a useful approach, though! ☺
SI6 Networks' IPv6 toolkit: Tools

- addr6: An IPv6 address analysis tool
- scan6: An IPv6 address scanner
- path6: A versatile IPv6-based traceroute
- frag6: Play with IPv6 fragments
- tcp6: Play with IPv6-based TCP segments
- ns6: Play with Neighbor Solicitation messages
- na6: Play with Neighbor Advertisement messages
SI6 Networks' IPv6 toolkit: Tools (II)

- rs6: Play with Router Solicitation messages
- ra6: Play with Router Advertisement messages
- rd6: Play with Redirect messages
- icmp6: Play with ICMPv6 error messages
- ni6: Play with Node Information messages
- flow6: Play with the IPv6 Flow Label
- jumbo6: Play with IPv6 Jumbograms
Some general notes on the tools
Modes of operation

- "Active" mode:
  - Fire packets regardless of what is being received

- "Listening" mode:
  - Listen to packets and respond with crafted packets

- If both modes are selected,
  - Active mode goes first
  - Then the tool enters "listening" mode
More about active mode

- “--loop” specifies that the active attack must be repeated indefinitely
- “--sleep” specifies the amount of time (in secs) to sleep between iterations
- Some tools support a “--rate-limit” option
More about listening mode

- Most tools support filters for the captured packets:
  - Link-layer Address(es)
  - IPv6 Address(es)
  - Tool-specific filters (e.g., ND Target Address)
- Filters can be:
  - “accept filters”: MUST match
  - “block filters”: MUST NOT match
- Example:
  --accept-src fc00::1/64 --block-link-src 00:11:22:33.44:55
Support for Extension Headers

• All tools support use of:
  • Destination Options Header
  • Hop-by-Hop Options Header
  • Fragment Header

• Extension headers can be combined (somewhat) arbitrarily
  • e.g. to make the IPv6 header chain span multiple fragments
Neighbor Discovery tools
Overview

• Tools:
  • ns6
  • na6
  • rs6
  • ra6
  • rd6

• Can perform:
  • Neighbor Cache poisoning attacks
  • a plethora of DoS attacks
Example #1: DAD-based DoS attack

- Example (DAD-based DoS attack)::
  
  ```
  # na6 -i wlan0 -b ::/128 -c -o -L -vv
  ```

  - interface
  - accept
  - filter
  - flags
  - listening
  - mode
  - be very
  - verbose
Example #2: RA-Guard evasion

- Example (DAD-based DoS attack)

```bash
# ra6 -i wlan0 -P fc00:1::/64#LA -u 1000 -u 100
-y 160

interface PIO Dest Opt Hdr Dest Opt Hdr

Frag Hdr
```
Playing with IPv6 fragments
Overview (frag6 tool)

- Can assess IPv6 fragmentation-related issues:
  - Support for IPv6 atomic fragments
  - Assess the Fragment ID generation policy
  - Assess the fragment reassembly policy
  - Stress nodes with fragments
Example #1: Frag. Reassembly policy

- When fragments overlap, a node may:
  - Use the first copy of the data,
  - Use the second copy of the data, or,
  - Discard duplicate fragments

- Example:
  
  ```
  # frag6 -i eth0 -v --frag-reass-policy -d fc00:1::1
  ```
Example #2: Frag ID generation policy

- Nodes typically generate the Frag ID as:
  - a global counter initialized to 0,
  - a per-destination counter initialized to 0,
  - a per-destination counter initialized to a random value, or,
  - a random value

- Predictable Frag IDs have well-known security implications

- Example:
  
  ```
  # frag6 --frag-id-policy -d fc00:1::1 -v
  ```

  3044-7217-4032-5253-7397
Example #3: Flooding with fragments

- Some nodes may have poor management of the fragment reassembly queue

- Example:

  ```
  # frag6 -s ::/0 -F 100 -l -z 5 -d fe00:1::1 -v
  ```

  Rand. Src Addr from 0::/64
  100 Frags at a time
  loop
  Sleep 5 secs.
Playing with ICMPv6 errors
Overview (icmp6 tool)

- Can generate arbitrary ICMPv6 errors:
  - Smart generation based on received packet, or,
  - Generation based on specified parameters
- Example (generate ICMPv6 PTB):

  ```shell
  # icmp6 -i wlan0 -L -p TCP -E -v
  ```

  - `-i wlan0` specifies the interface.
  - `-L` enables listening mode.
  - `-p TCP` captures TCP packets.
  - `-E` indicates that the tool will generate errors.
  - `-v` makes the output more verbose.
Playing with TCP segments
Overview

• For a long time there was not even a IPv6-based SYN flooder
• Even IPv4-based TCP tools were rather scarce and primitive
• tcp6 can:
  • Perform SYN floods
  • Flood with connections in virtually any state
  • Perform TCP probing
  • Perform some smart scans (buffer exhaustion, closed windows, etc.)
Example #1: Buffer/connection DoS

- The effect of this attack is two-fold:
  - Lots of TCP connections with no controlling process
  - Lots of queued data for such connections

- Example:

```bash
# tcp6 -d fc00:1::1 -a 80 -L
-s fc00:1::/112 --flood-ports 10
-1 -r 100pps
--data "GET / HTTP/1.0\r\n\r\n"
--close-mode last-ack
```
Scanning IPv6 networks
Overview

- IPv6 host scanning deemed unfeasible for a long time

  -> But it is not!

- scan6 can leverage IPv6 address patterns:
  - Traditional SLAAC address (embedded MAC address)
  - Port-based addresses
  - Virtual machines
  - Low-byte-addresses
  - etc.

- You should read draft-ietf-opsec-ipv6-host-scanning
Example

- Scan a network for port-based addresses
  
  `# scan6 -d PREFIX/64 --tgt-port`
Analyzing IPv6 addresses
Overview

- There are different address types and scopes
- There are different IID generation schemes
- At times they are not that easy to spot
- Our addr6 tool is your friend here 😊
Example #1: Analyzing IPv6 Addresses

• The addr6 tool can analyze IPv6 addresses

• Example:

  $ addr6 -a ADDRESS

• Format:

  type=subtype=scope=IID_type=IID_subtype

• Example:

  $ addr6 -a fc00::1

  unicast=unique-local=global=low-byte=unspecified
Example #2: IPv6 address stats

$ cat addresses.txt | addr6 -i -s
(Rather uninteresting) tools
(Rather uninteresting) tools

- jumbo6
  - Checks for support of IPv6 jumbogams
- flow6
  - Assesses the Flow Label generation policy
- ni6
  - Same as “ping6 -N” in Linux, but with more options
IPv6 Toolkit v1.6 in Troopers!
A versatile traceroute tool
(new in SI6 IPv6 Toolkit v1.6!)
Overview (path6 tool)

- No existing traceroute tool supports IPv6 extension headers
- We needed to measure packet drops resulting from IPv6 EHs
- Hence we produced our path6 tool
  - Supports IPv6 Extension Headers
  - Can employ TCP, UDP, or ICMPv6 probes
  - It's faster ;-)  

Example:

```bash
# path6 -u 100 -d fc00:1::1
```

Dst Opt Hdr
Questions?
Thank you's

- Troopers 14 crew, for taking care of all details!
Thanks!

Fernando Gont
fgont@si6networks.com
@FernandoGont

SI6 Networks
www.si6networks.com
@SI6Networks