Security Assessment and Troubleshooting with SI6 IPv6 Toolkit v2.0 (Guille)

Fernando Gont
(as Guillermo Gont)

SI6 NETWORKS

FLIP6 2015
Lima, Peru. Mayo 18-22, 2015

About...

- Security Researcher and Consultant at SI6 Networks
- Published:
  - 20 IETF RFCs (9 on IPv6)
  - 10+ active IETF Internet-Drafts
- Author of the SI6 Networks' IPv6 toolkit
  - http://www.si6networks.com/tools/ipv6toolkit
- Admin of the IPv6 Hackers mailing-list
  - ipv6hackers@lists.si6networks.com
- More information at: http://www.gont.com.ar

Agenda

"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 new features in the

SI6 Network's IPv6 Toolkit

Introduction

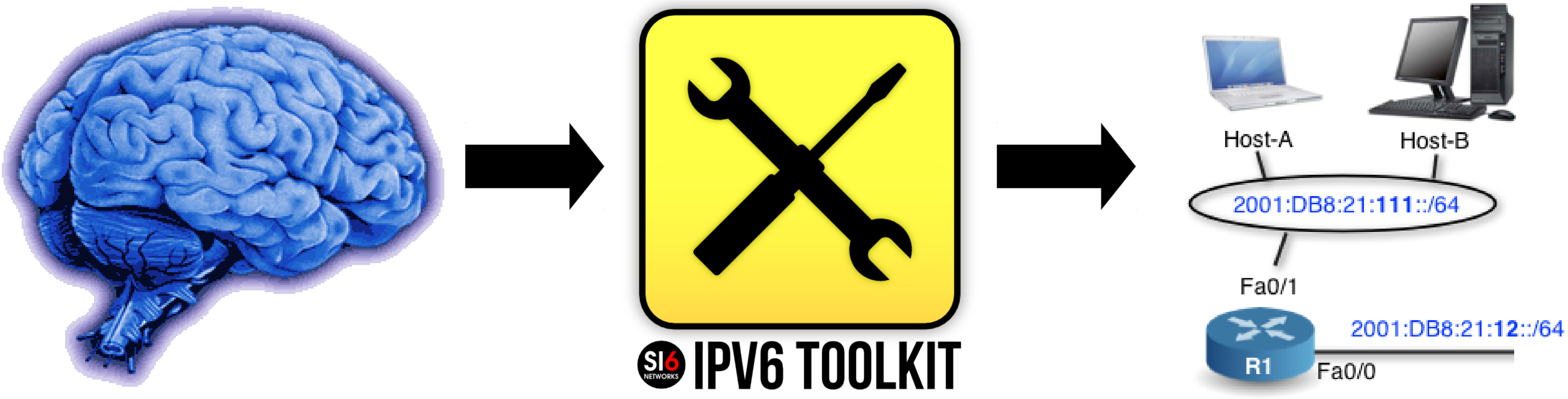
SI6 Networks' IPv6 Toolkit: Intro

- 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, Mac OS, and OpenSolaris
- License:
  - GPL (free software)
- Home:
  - http://www.si6networks.com/tools/ipv6toolkit
- Collaborative development:
  - 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”

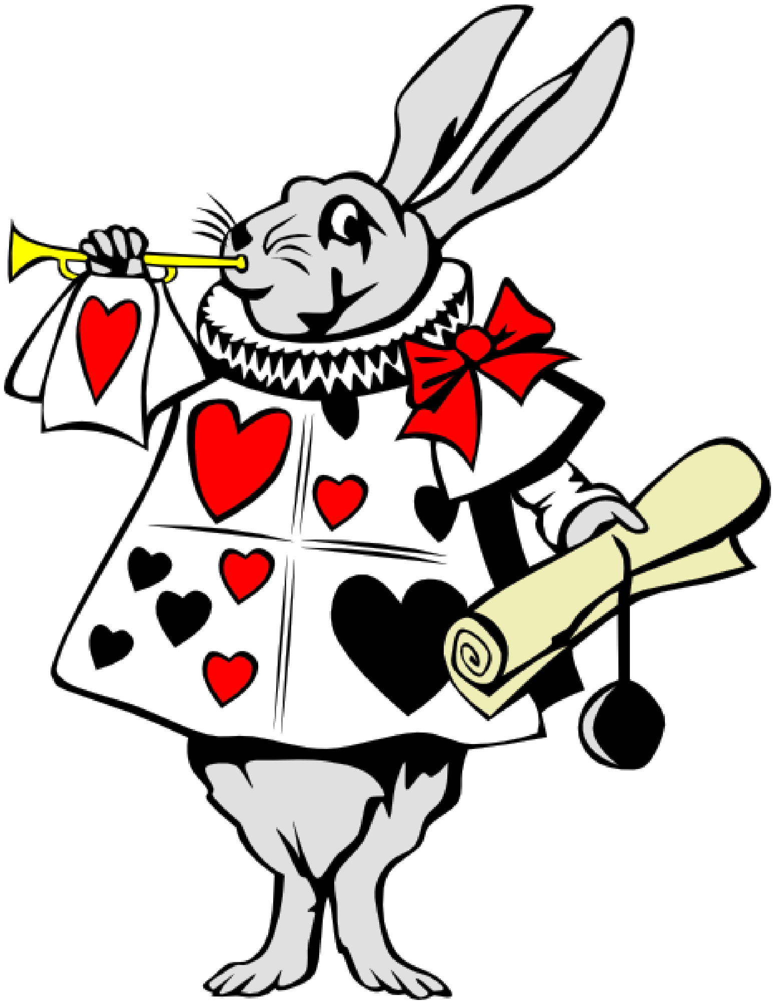
Some find this is NOT a useful approach, though! ☺

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
- udp6: Play with UDP datagrams
- ns6: Play with Neighbor Solicitation messages
- na6: Play with Neighbor Advertisement messages
- script6: Rather complex tasks made easy

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



IPv6 Toolkit v2.0!

Overview

What's new in SI6 IPv6 v2.0 (Guille)

- Lots of bug fixes!
- An additional supported platform
  - OpenSolaris
- New tools:
  - **`blackhole6`**
  - **`script6`**
  - **`path6`**
  - **`udp6`**
- New features:
  - **`tcp6`**'s --close-mode, --data, etc.
  - **`scan6`**'s automatic smart scanning

Address Scanning

Address Scanning

- scan6 is **the most comprehensive IPv6 address scanner**
- It now supports heuristic address scanning:
  - It automatically detects address patterns
  - Then automatically targets such address patterns
- Employing heuristic scanning:

```
scan6 -d DOMAIN/64

scan6 -d IPV6ADDR/64
```

Host Scanning
Demo

IPv6-based TCP/UDP port scanning

- scan6 incorporates all known TCP and UDP port-scanning techniques
- Specifying a protocol and port range:

```
--port-scan {tcp,udp}:port_low[-port_hi]
```

- Specifying a TCP scan type:

```
--tcp-scan-type {syn,fin,null,xmas,ack}
```

- Example:

```
--port-scan tcp:1-1024 --tcp-scan-type syn
```

Port Scanning
Demo

Tracing IPv6 Routes

path6 tool

- No existing traceroute tool supported IPv6 extension headers
  - e.g., How far do your IPv6 EH-enabled packets get?
- Hence we produced our path6 tool
  - Supports IPv6 Extension Headers
  - Can employ TCP, UDP, or ICMPv6 probes
  - It's faster ;-)
- Example:

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

Dst Opt Hdr

Tracing IPv6 Routes
Demo

Finding IPv6 blackholes

blackhole6: Finding IPv6 blackholes

- It is useful to find out who is dropping specific packets:
  - Troubleshooting
  - Network reconnaissance
  - ... or just checking if you EH-enabled attacks would work
- blackhole6 does this (and more) auto-magically:

```
blackhole6 DESTINATION [EHTYPE[EHSIZE]]
[PROTOCOL [PORT]]]
```

blackhole6: Methodology

1) Run “normal” path6 to target (D), and save route (ROUTE)
2) Check that last “hop” in route is D
3) Run EH-enabled path6, and find last responding address (M)
4) Find “M” in “ROUTE” -> dropping system is next in ROUTE (M+1)
5) Compare AS(M) with AS(M+1), and produce other stats

blackhole6: Methodology (II)

- Given the output of path6 for no-EH and EHs:

No EHs

1. fc00:1:1:1000::1
2. fc00:1:1:2000::4
3. fc00:1:2:4000::1
4. fc00:2:1:4000::1
5. fc00:a:2:1000::1
6. fc00:a:4:4000::1
7. fc00:b:1:1000::1
8. fc00:b:2:5000::1
9. fc00:b:4:5000::1
10. fc00:d::1

DROP

With EHs

1. fc00:1:1:1000::1
2. fc00:1:1:2000::4
3. fc00:1:2:4000::1
4. fc00:2:1:4000::1
5. fc00:a:2:1000::1
6. fc00:a:4:4000::1

blackhole6: Methodology (III)

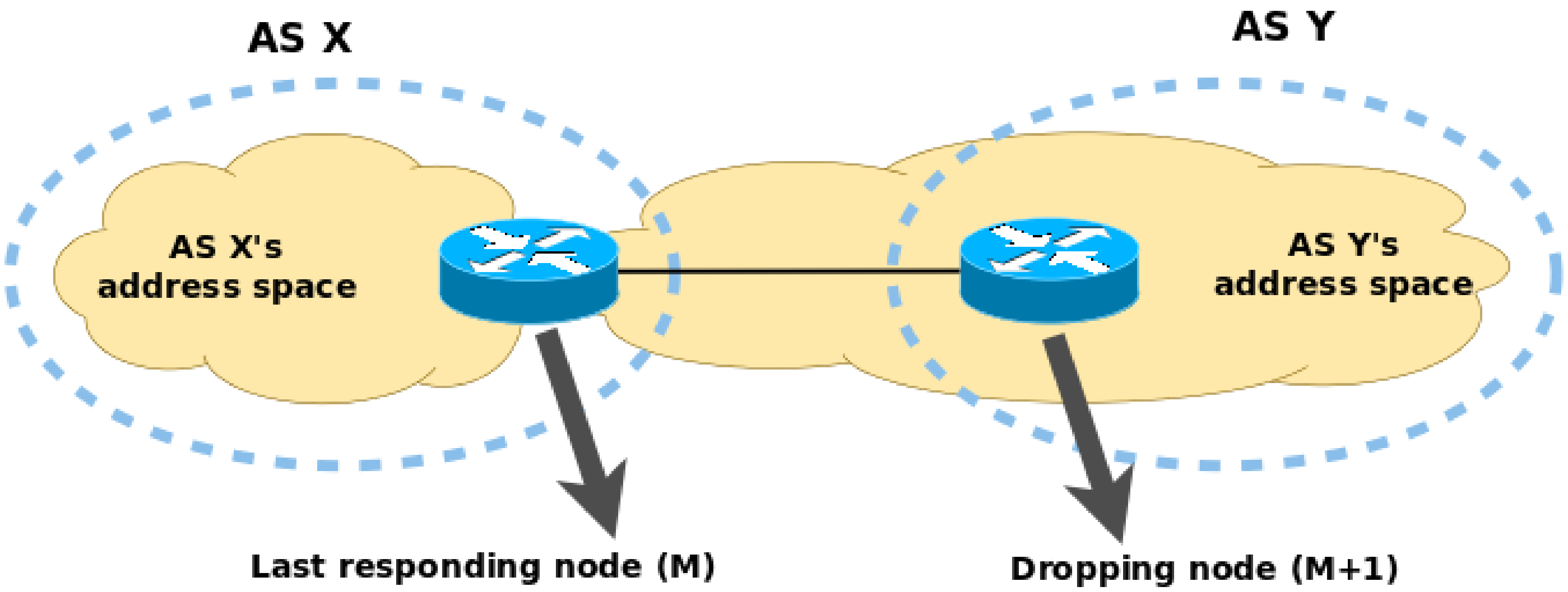
- We assume ingress filtering...
- Otherwise dropping node actually is M rather than M+1

blackhole6: ASes

- Lookup ASN of dropping node, but...
- There may be ambiguity when finding the AS of the dropping node:
  - who provides the address space for the peering?

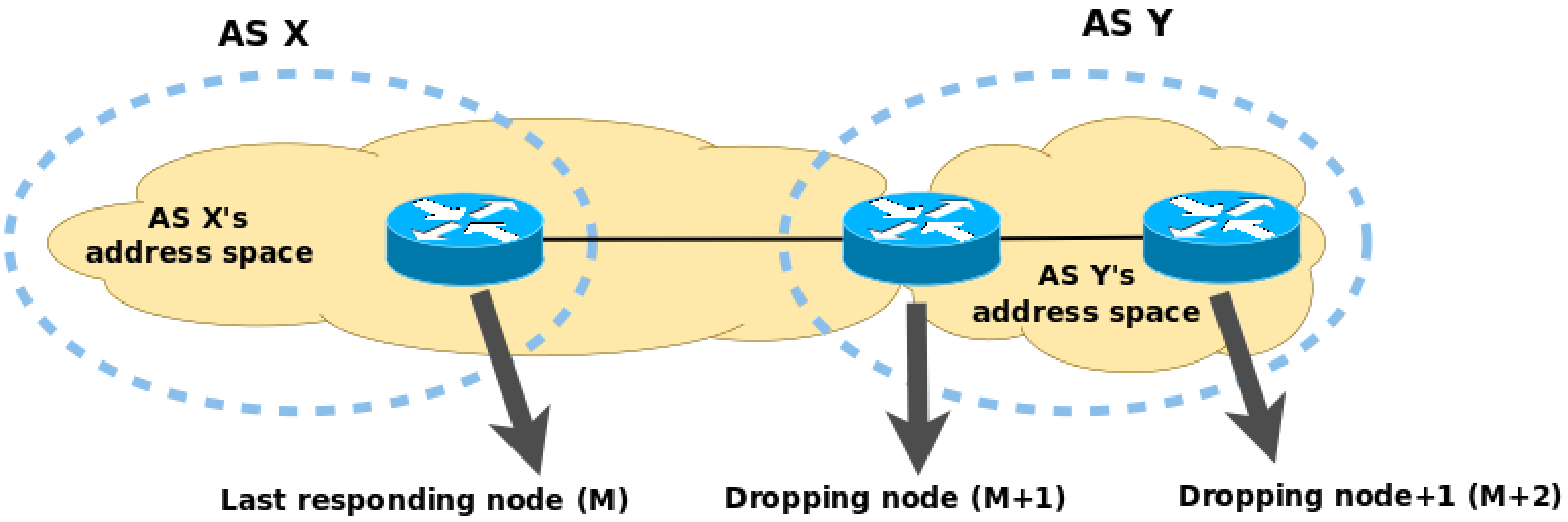
blackhole6: ASes (II)

- Case 1: Address space provided by AS Y



blackhole6: ASes (III)

- Case 2: Address space provided by AS X



Finding IPv6 blackholes Demo

Some conclusions

Some conclusions

- Coding IPv6 tools:
  - Portability harder than expected (harder than it “should”)
  - Increased usage -> increased code quality
- Using IPv6 tools
  - There is a lot to learn through practice
- **Please use the toolkit and report back to us**

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com