IPv6 Security Tools

Fernando Gont

SI6 NETWORKS

UK IPv6 Council Security Workshop
London, UK. July 12, 2017

About...

- Security Researcher and Consultant at SI6 Networks
- Published 30 IETF RFCs (15+ on IPv6)
- Contributor to TechTarget.com on IPv6
  - http://www.techtarget.com/contributor/Fernando-Gont
- Author of the SI6 Networks' IPv6 toolkit
  - https://www.si6networks.com/tools/ipv6toolkit
- IPv6 Hackers Mailing List admin
- More information at: https://www.gont.com.ar

IPv6 tools

THC-IPv6 Toolkit: Introduction

- First and only IPv6 attack toolkit for many years
- Easy to use
  - Only minimal IPv6 knowledge required
- Features:
  - Only runs on Linux with Ethernet
  - Free software
- Available at: http://www.thc.org/thc-ipv6

SI6 Networks' IPv6 Toolkit

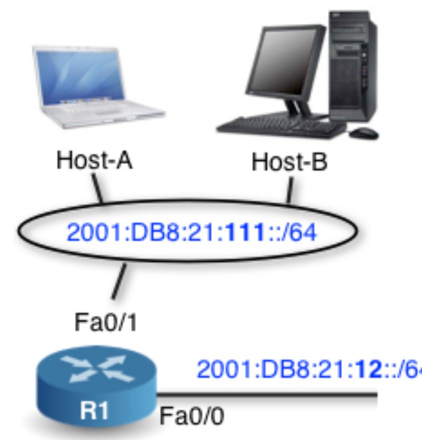
- Brief history:
  - Originally produced as part of a governmental project on IPv6 security
  - Maintenance and extension taken over by SI6 Networks
- Goals:
  - Security assessment and trouble-shooting of IPv6 networks and implementations
  - Clean, portable, and secure code
  - Good documentation

SI6 Networks' IPv6 Toolkit (II)

- Supported OSes:
  - Linux, FreeBSD, NetBSD, OpenBSD, OpenSolaris, and Mac OS
- License:
  - GPL (free software)
- Home:
  - https://www.si6networks.com/tools/ipv6toolkit
- Collaborative development:
  - https://www.github.com/fgont/ipv6toolkit.git

SI6 Networks' IPv6 Toolkit: Philosophy

IPV6 TOOLKIT



IDEAS → TOOLS → IPV6 NETWORK

"an interface between your ideas and an IPv6 network"

IPv6 Addressing

Address Scanning

Introduction

- Address scanning in IPv4 is typically “brute force”
  - search space is so small we can get away with such a loosy job!
- Bruteforce approach simply unfeasible for IPv6
  - search space would be too big (2^{64} addresses)

Approaching IPv6 address scanning

- Two (totally-different) problem areas:
  - Local-network scans
  - Remote-network scans
- Local-network scans rather easy
- Remote-network scans more challenging
- It is key to understant the IPv6 Addressing Architeture

IPv6 addressing

Implications on address scanning of local networks

Overview

- Leverage IPv6 all-nodes link-local multicast address
- Employ multiple probe types:
  - Normal multicasted ICMPv6 echo requests (don't work for Windows)
  - Unrecognized options of type 10xxxxxx
- Combine learned IIDs with known prefixes to learn all addresses
- Example:

```
# scan6 -i eth0 -L
```

IPv6 Addressing

Implications on address scanning of remote networks

IPv6 host scanning attacks

"Thanks to the increased IPv6 address space, IPv6 host scanning attacks are unfeasible. Scanning a /64 would take 500.000.000 years"

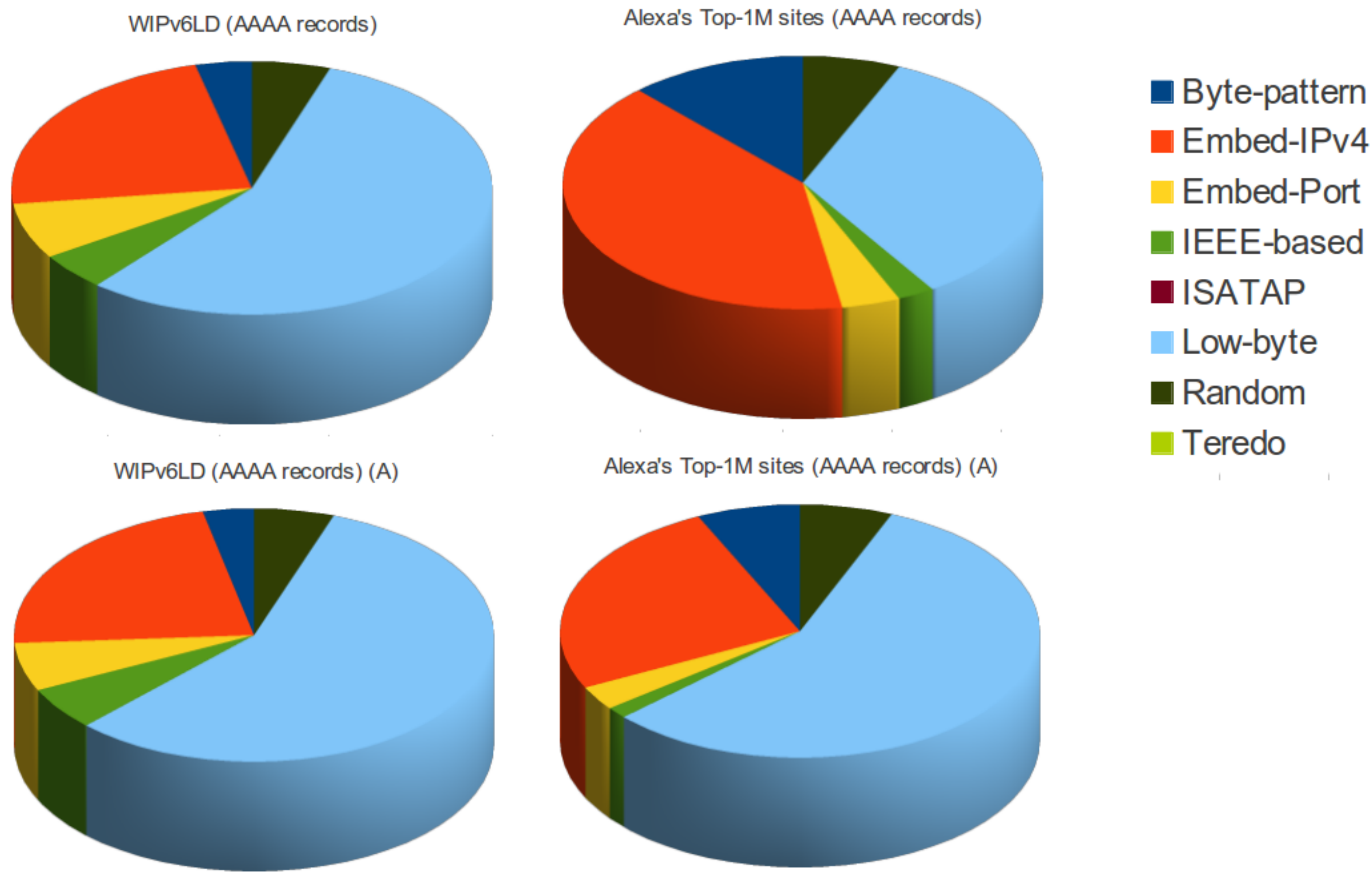
– Urban legend

Is the search space for a /64 really 2^{64} addresses?

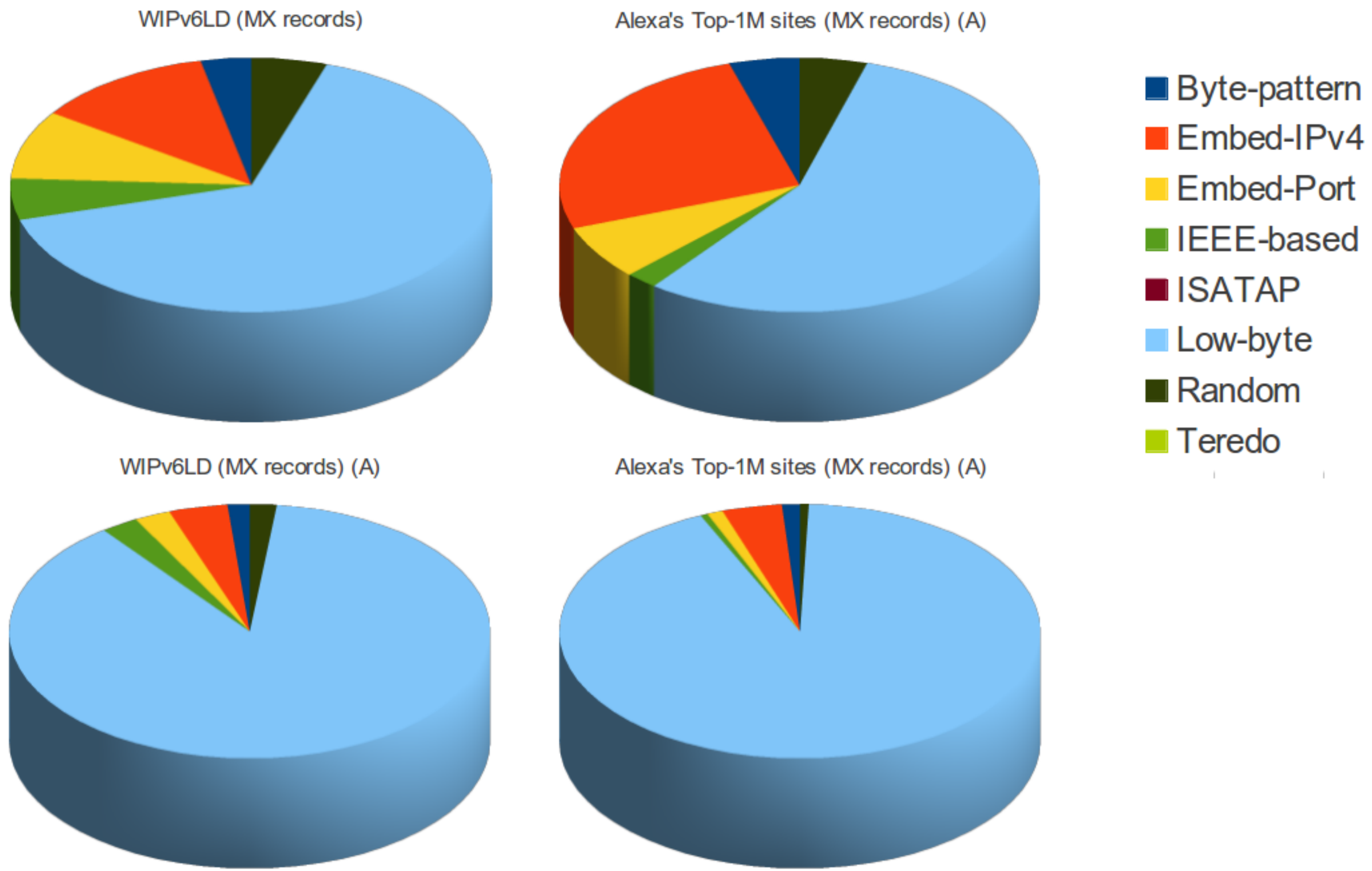
Our experiment

- Find “a considerable number of IPv6 nodes” for address analysis:
  - Alexa Top-1M sites + perl script + dig
  - World IPv6 Launch Day site + perl script + dig
- For each domain:
  - AAAA records
  - NS records -> AAAA records
  - MX records -> AAAA records
- What did we find?

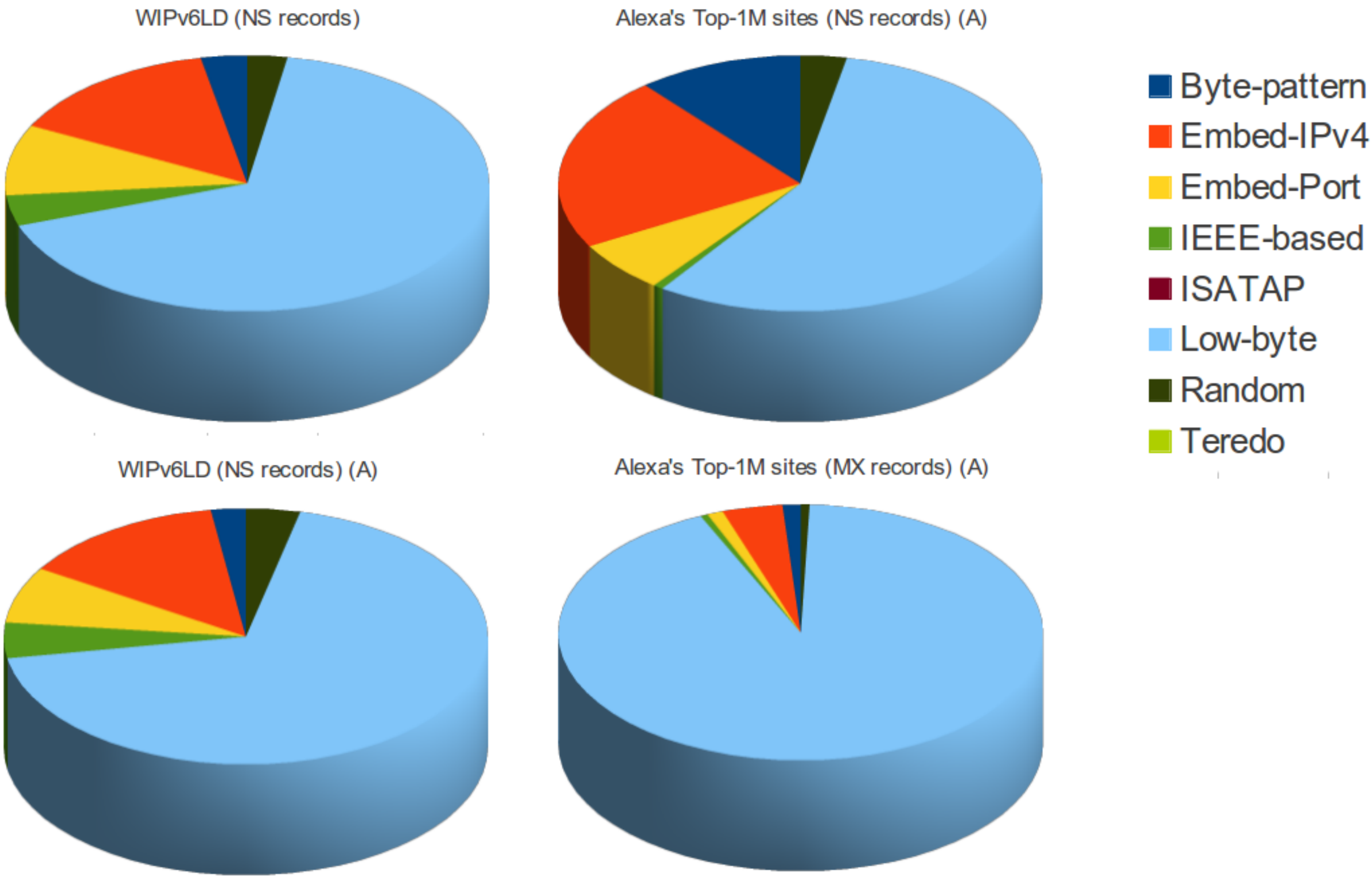
IPv6 address distribution for the web



IPv6 address distribution for mail servers

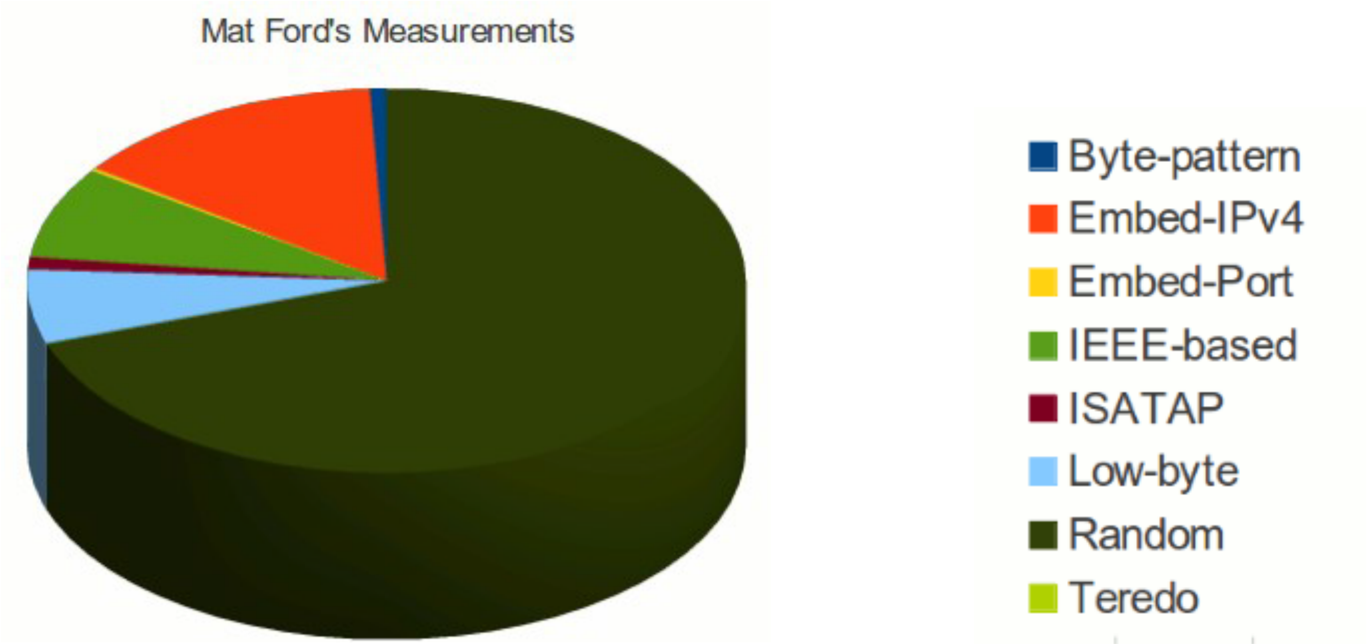


IPv6 address distribution for the DNS



UK IPv6 Council Security Workshop
London, UK. July 12, 2017

Client addresses



- Caveats:
  - Graphic illustrates IID types used for outgoing connections.
  - No data about IID types used for stable addresses when RFC4941 is employed.

Source: <http://www.internetsociety.org/blog/2013/05/ipv6-address-analysis-privacy-transition-out>

IPv6 address patterns

- MAC-address based
  - e.g.: 2001:db8::**fad1**:**22**ff:fe**c0**:**fb44**
- Embed-IPv4:
  - 2000:db8::**192.168.0.1** <- Embedded in 32 bits
  - 2000:db8::**192**:**168**:**0**:**1** <- Embedded in 64 bits
- Embed-port:
  - 2001:db8::**1**:**80** <- n:port
  - 2001:db8::**80**:**1** <- port:n
- Low-byte addresses:
  - 2001:db8::**n1**:**n2** <- where n1 is typically greater than n2

Some take-aways from our study

- Server addresses clearly do follow patterns
  - The majority of addresses follow patterns with a small search space
- Passive measurements on client addresses are of little use
  - Due to IPv6 temporary addresses (RFC4941)

IPv6 address scanning

- scan6 can target specific address patterns
- “What if I'm lazy enough to 'set' an appropriate address pattern?”
  - scan6 infers the address pattern for you!
- Example:

```
# scan6 -d DOMAIN/64 -v
```

Conclusions about scanning attacks

- IPv6 address scanning attacks are **feasible**, but typically harder than in IPv4
- They require more “intelligence” on the side of the attacker
- It is **possible** to make them infeasible
  - Just do not employ addresses that follow patterns
  - RFC7217 and RFC8064 fix that for SLAAC
- It is likely that many other scanning strategies/techniques will be explored (more on this later)

IPv6 Extension Headers
Reconnaissance and Troubleshooting

path6: An EH-enabled traceroute

- How far do your IPv6 EH-enabled packets get?
- No existing traceroute tool supported IPv6 extension headers
- 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

path6: An EH-enabled traceroute (II)

- Example of traceroute with 8-byte DOH:

```
# path6 -d DEST -u 8 -p icmp
```

- Example of traceroute with fragmentation:

```
# path6 -d DEST -p icmp -P 500 -y 256
```

- Example of traceroute with TCP payload:

```
# path6 -d DEST -p tcp -a 80
```

blackhole6: Finding IPv6 blackholes

- How it works?
  - path6 without EHs + path6 with EHs + a little bit of magic

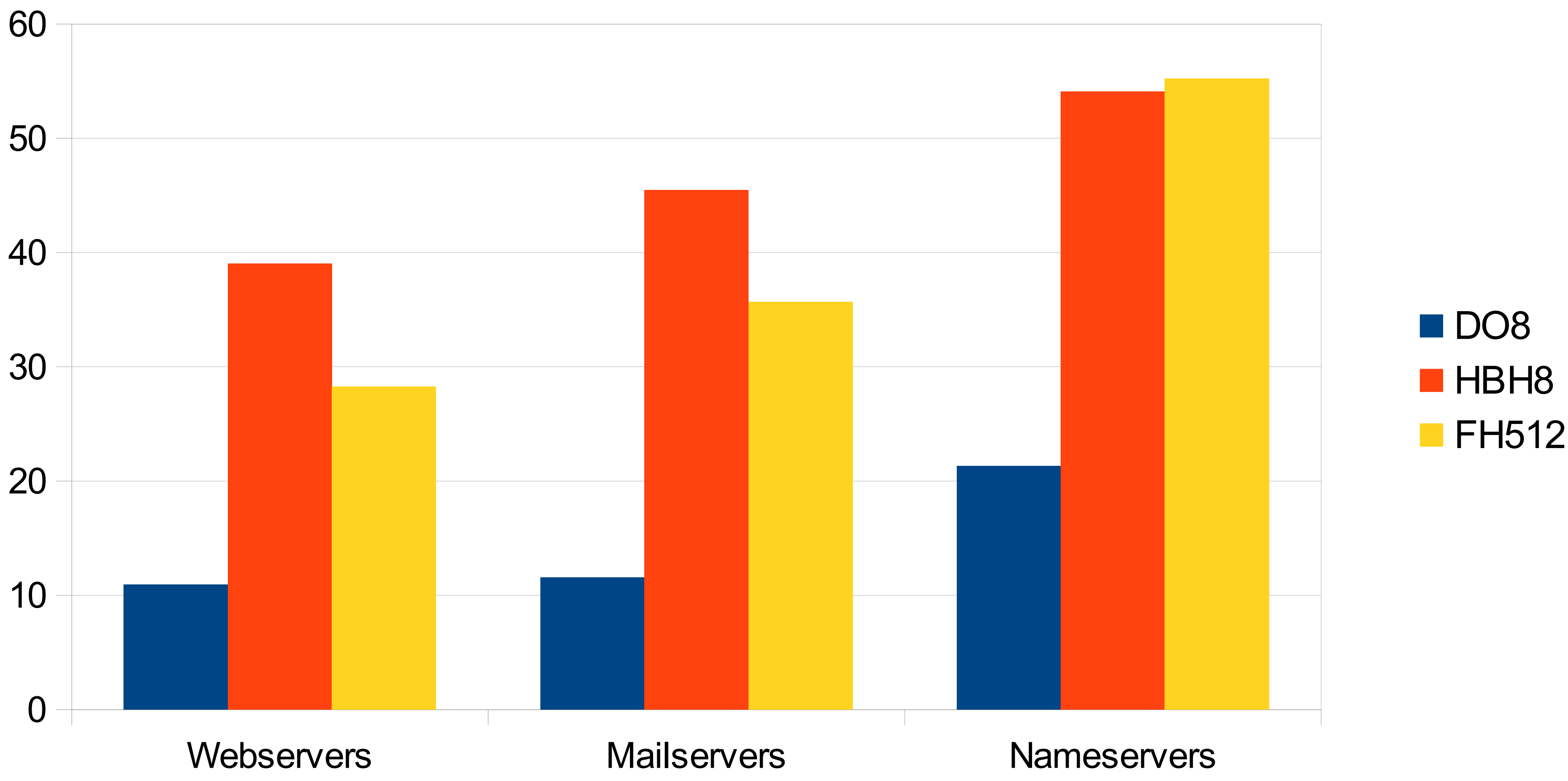
```
fgont@satellite:~$ sudo blackhole6 www.google.com do8
SI6 Networks IPv6 Toolkit v2.0
blackhole6: A tool to find IPv6 blackholes
Tracing www.google.com (2607:f8b0:400b:807::1012)...

Dst. IPv6 address: 2607:f8b0:400b:807::1012 (AS15169 - GOOGLE - Google
Inc.,US)
Last node (no EHs): 2607:f8b0:400b:807::1012 (AS15169 - GOOGLE - Google
Inc.,US) (13 hop(s))
Last node (DO 8): 2001:5a0:12:100::72 (AS6453 - AS6453 - TATA
COMMUNICATIONS (AMERICA) INC,US) (7 hop(s))
Dropping node: 2001:4860:1:1:0:1935:0:75 (AS15169 - GOOGLE - Google
Inc.,US || AS15169 - GOOGLE - Google Inc.,US)
```

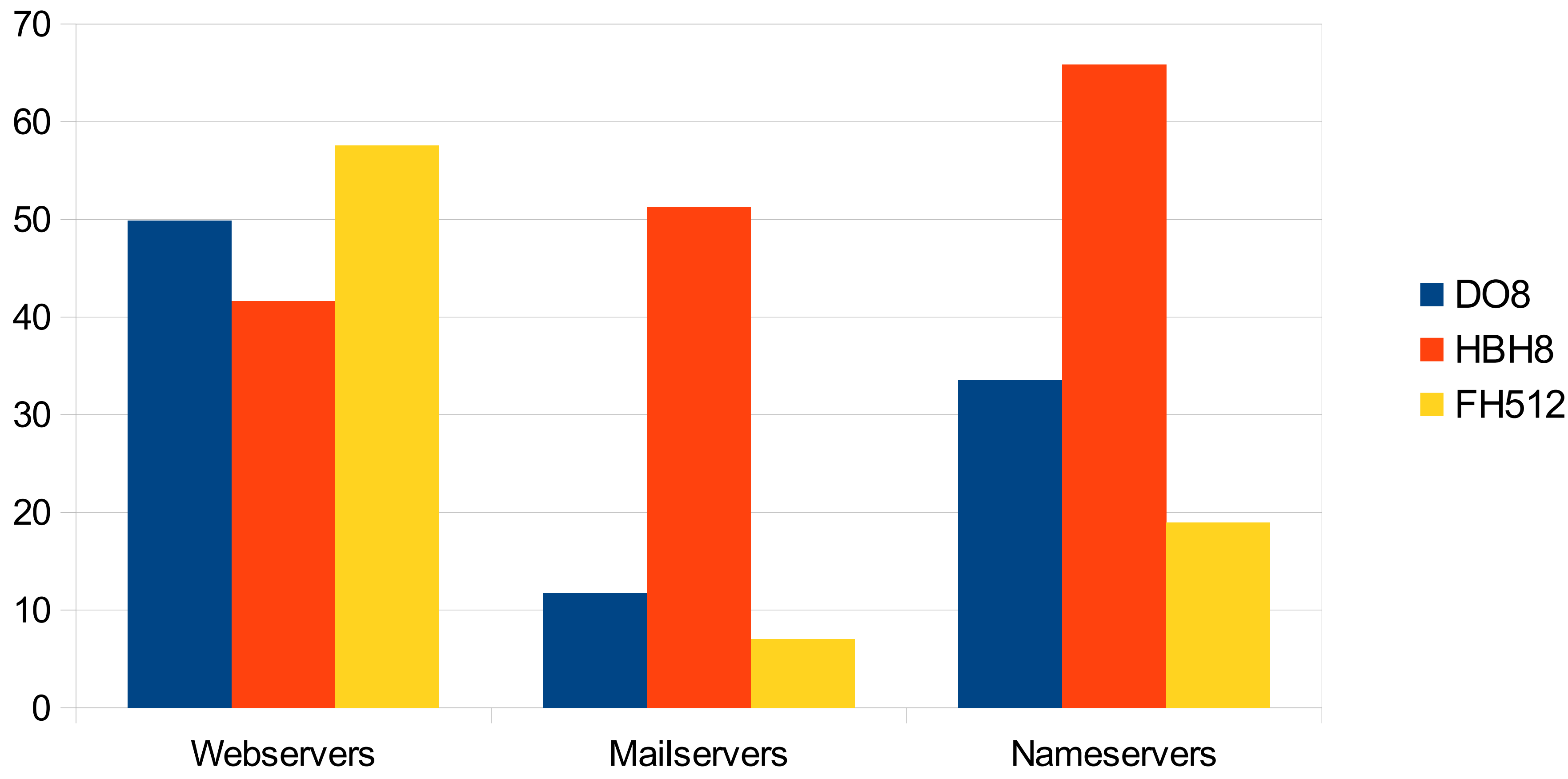
IPv6 Extension Headers

In The Real World

Packet Drop rate for Alexa's Top 1M sites



Drops by diff AS for Alexa's Top 1M sites



So... what does this all mean?

- Good luck with getting IPv6 EHs working in the Internet!
  - They are widely dropped
- IPv6 EHs “not that cool” for evasion, either
  - Chances are that you will not even hit your target

Neighbor Discovery for IPv6

Neighbor Discovery for IPv6

Address Resolution

Address Resolution in IPv6

- Employs ICMPv6 Neighbor Solicitation and Neighbor Advertisement
- It (roughly) works as follows:
  - Host A sends a NS: Who has IPv6 address fc01::1?
  - Host B responds with a NA: I have IPv6 address, and the corresponding MAC address is 06:09:12:cf:db:55.
  - Host A caches the received information in a “Neighbor Cache” for some period of time (this is similar to IPv4’s ARP cache)
  - Host A can now send packets to Host B

Neighbor Discovery for IPv6

Address Resolution Attacks

“Man in the Middle” or Denial of Service

- They are the IPv6 version of IPv4’s ARP cache poisoning
- Without proper authentication mechanisms in place, its trivial for an attacker to forge Neighbor Discovery messages
- Attack:
  - Send forged Neighbor Advertisement, with a forged target link-layer address option
- If the “Target Link-layer address” corresponds to a non-existing node, traffic is dropped, resulting in a DoS.
- If the “Target Link-layer address” is that of the attacker, he can perform a “man in the middle” attack.

Performing the attack with the na6 tool

- Run the tool as:

```
# na6 -i IFACE -t VICTIMADDR -E MACADDR -o -c -L
```

Neighbor Discovery for IPv6
Address Resolution Attacks – Countermeasures

Possible mitigations for ND attacks

- Do you mitigate similar vulnerabilities for IPv4?
- Possible mitigations for IPv6:
  - SAVI / ND snooping
  - Monitor Neighbor Discovery traffic (e.g., with NDPMon)
  - Restrict access to the local network
  - Use static entries in the Neighbor Cache
  - Deploy SEND (SEcure Neighbor Discovery)

Neighbor Discovery for IPv6
Stateless Address Auto-configuration (SLAAC)

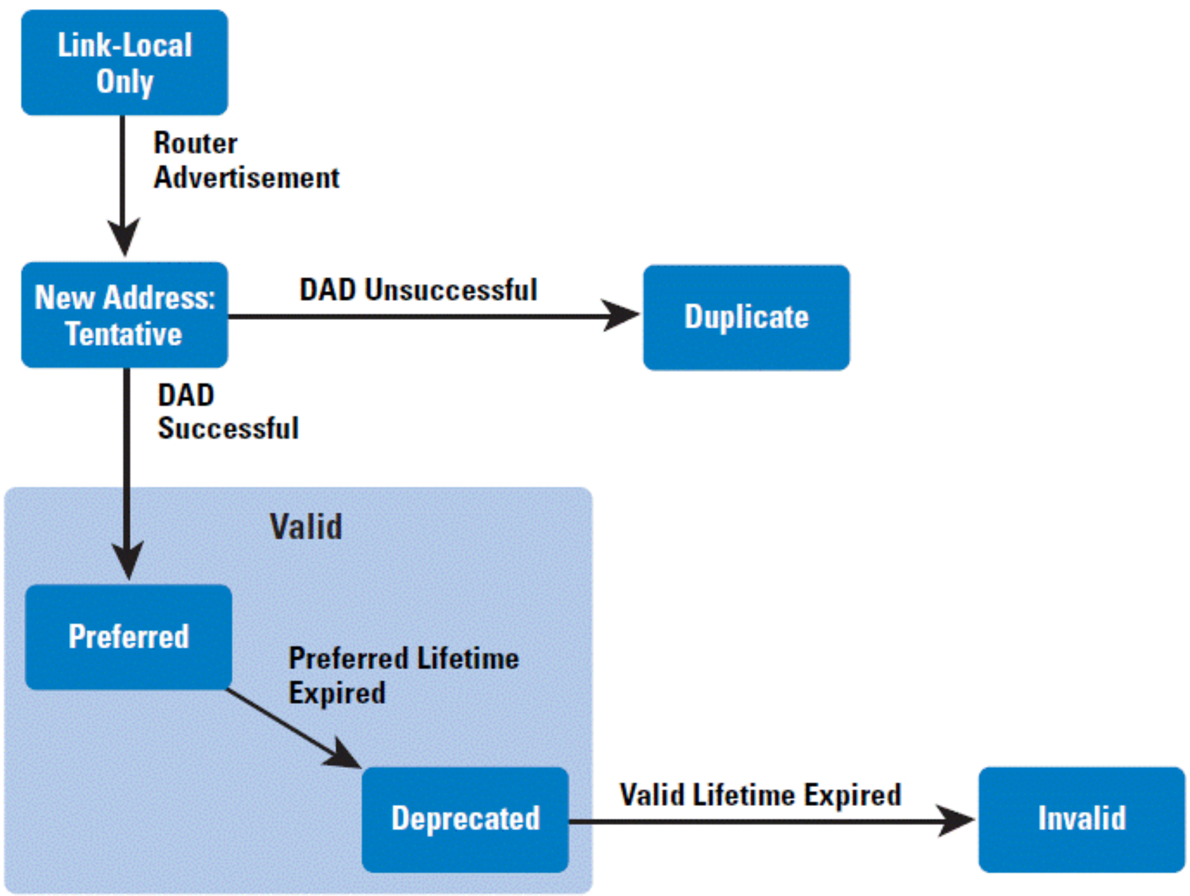
Brief overview

- Two auto-configuration mechanisms in IPv6:
  - Stateless Address Auto-Configuration (SLAAC)
    - Based on ICMPv6 messages
  - DHCPv6
    - Based on UDP packets
- SLAAC is mandatory, while DHCPv6 is optional
- Basic operation of SLAAC:
  - Host solicit configuration information by sending Router Solicitation messages
  - Routers convey that information in Router Advertisement messages:
    - Auto-configuration prefixes
    - Routes
    - Network parameters
    - etc.

SLAAC: Step by step

- It works (roughly) as follows:
  1. The host configures a link-local address
  2. It checks that the address is unique – i.e., it performs Duplicate Address Detection (DAD) for that address
     - Sends a NS, and waits for any answers
  3. The host sends a Router Solicitation message
  4. When a Router Advertisement is received, it configures a “tentative” IPv6 address
  5. It checks that the address is unique – i.e., it performs Duplicate Address Detection (DAD) for that address
     - Sends a NS, and waits for any answers
  6. If the address is unique, it typically becomes a “preferred” address

Address Autoconfiguration flowchart



Neighbor Discovery for IPv6

SLAAC attacks

Exploit DAD for DoS attacks

- Listen to NS messages with the Source Address set to the IPv6 “unspecified” address (::)
- Respond to such messages with a Neighbor Advertisement message
- As a result, the address will be considered non-unique, and DAD will fail
- The host will not be able to use that “tentative” address
- Perform this attack with the na6 tool as follows:

```
# na6 -i IFACE -b ::/128 -L -vv
```

Or possibly:

```
# na6 -i em0 -b ::/128 -B VICTIMMAC -L -vv
```

Disable an Existing Router

- Forge a Router Advertisement message that impersonates the local router
- Set the "Router Lifetime" to 0 (or some other small value)
- As a result, the victim host will remove the router from the "default routers list"
- Perform this attack with the ra6 tool:

```
# ra6 -i IFACE -s ROUTERADDR -d TARGETADDR -t 0 -l 1 -v
```

Possible mitigations for SLAAC attacks

- Do you mitigate similar attacks for the IPv4 case?
- Possible mitigations:
  - Deploy Router Advertisement Guard (RA-Guard) -- **beware of RFC7113 attacks!**
  - Monitor Neighbor Discovery traffic (e.g., with NDPMon)
  - Restrict access to the local network
  - Deploy SEND (SEcure Neighbor Discovery)

Upper-layer attacks

Brief Overview

- IPv6 is just a network-layer protocol
- Everything above the network layer is essentially the same
  - Transport-layer attacks
  - Application layer attacks
  - etc,

tcp6: TCP-based attacks

- The tcp6 tool can send arbitrary TCP/IPv6 packets
- It can also trigger virtually any TCP state at a target system
- Example: SYN-flood attack

```
# tcp6 -s SRCPRF -d TARGET -a DSTPORT -X S -F
100 -l -z 1 -v
```

Mitigations for upper-layer attacks

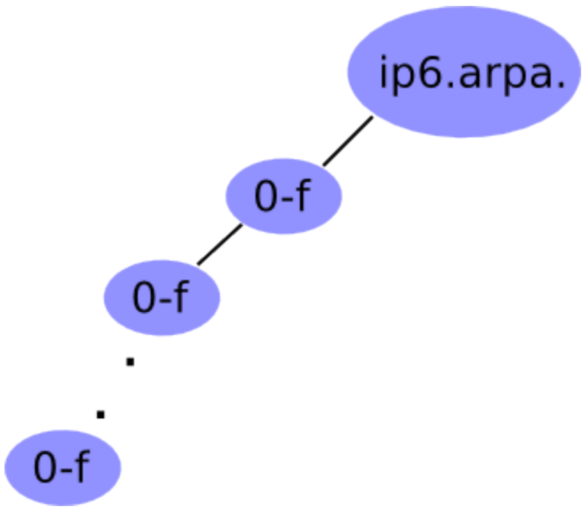
- Usually the same as in the IPv4 case
- Caveat: Mitigations on a per-IPv6-prefix basis (rather than (per-address)

DNS support for IPv6

DNS for Network Reconnaissance

- Most of this ground is well-known from the IPv4-world:
  - DNS zone transfers
  - DNS bruteforcing
  - etc.
- DNS reverse-mappings particularly useful for “address scanning”

IPv6 DNS reverse mappings



- Technique:
  - Given a zone X.ip6.arpa., try the labels [0-f].X.ip6.arpa.
  - If an NXDOMAIN is received, that part of the "tree" should be ignored
  - Otherwise, if NOERROR is received, "walk" that part of the tree
- Example (using dnsrevenum6 from THC-IPv6):

```
$ dnsrevenum6 DNSSERVER IPV6PREFIX
```

Mitigating DNS reverse mappings scans

- Reverse mappings only actually required for mail servers
- For the general case:
  - Do not configure reverse mappings, or,
  - Wildcard reverse mappings

Some conclusions

- Many IPv4 vulnerabilities have been re-implemented in IPv6
  - We just didn't learn the lesson from IPv4, or,
  - Different people working on IPv6 than working on IPv4, or,
  - The specs could make implementation more straightforward, or,
  - **All of the above?** :-)
- Still quite some work to be done in IPv6 security
  - There is always room for improvements
  - **We need IPv6, and should work to improve it**
- **There's no question that you should deploy IPv6**

Questions?

Thank you's

- Veronika McKillop
- Tim Chown
- Andy Butcher
- UK IPv6 Council
- Axians

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

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

www.si6networks.com