Knockin' on IPv6 Doors

Fernando Gont

SI6 NETWORKS

NGI @ Troopers 2018
Heidelberg, Germany. March 12-13, 2018

About...

- Security Researcher and Consultant at SI6 Networks
- Published:
  - 30 IETF RFCs (10+ on IPv6)
  - 10+ active IETF Internet-Drafts
- Author of the SI6 Networks' IPv6 toolkit
  - https://www.si6networks.com/tools/ipv6toolkit
- I have worked on security assessment of communication protocols for:
  - UK NISCC (National Infrastructure Security Co-ordination Centre)
  - UK CPNI (Centre for the Protection of National Infrastructure)
- More information at: https://www.gont.com.ar

Introduction

Going mass scale

- What if we wanted to target the whole IPv6 Internet or a whole country?
- How do we find information about the “most popular” nodes?
- Some boring and dirty work needs to be done
  - What are the TLDs for a given region?
  - What are de suffixes for a given TLD?
  - etc

Going mass scale

- Some techniques need to be adapted or evaluated
  - e.g. dnsrevenum6 tend to fail on very short prefixes
- Other techniques need to be extrapolated
  - e.g. smarts on prefixes as opposed to addresses
- Where else to go and look for information?

Where to start?

Where to get to the most important bits?

- There were at least three datasets of popular sites:
  - Alexa's Top-1M Domains
  - Majestic's List
  - Umbrella list
- All available at: https://github.com/fgont/domain-list
- But far form the number of existing domain names...

Zone files for all

- Some TLDs zones (e.g. .ORG) shared via:

  https://czds.icann.org/

- Some ccTLD zone made voluntarily available:

  https://zonedata.iis.se/

- Some leaked:

  https://github.com/mandatoryprogrammer/RussiaDNSLeak

How about the other zones?

- You can get “some” taste of the zone data with appropriate tools. (65K domains from the UK in less than a day)
- SI6 Toolkit contains multiple tls that help in tihs area:
  - script6 cab generate TLDs with suffixes
  - script6 can also scrap the results of search engines

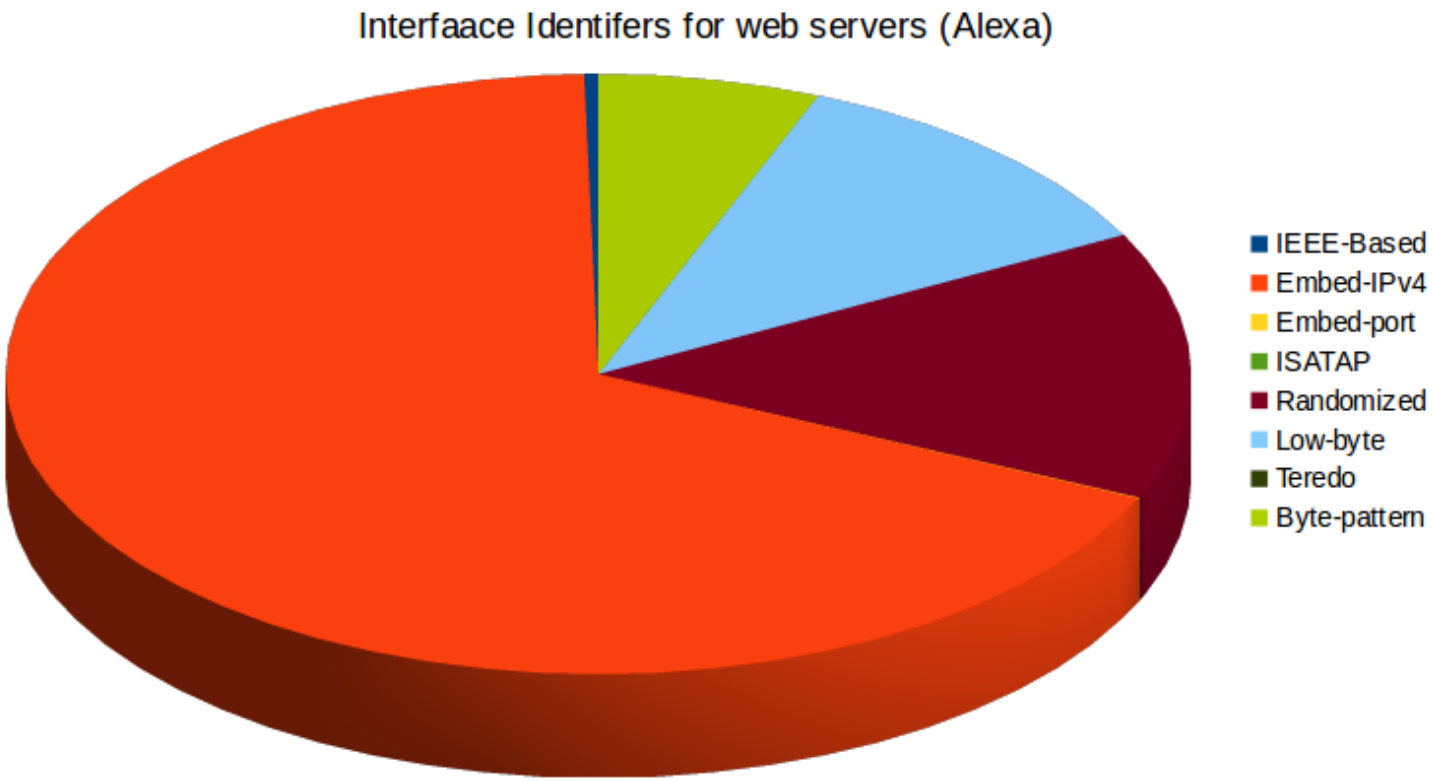
`script6 get-bing` can get you e.g. 65K domains from the UK in less than a day

Address patterns: Any changes?

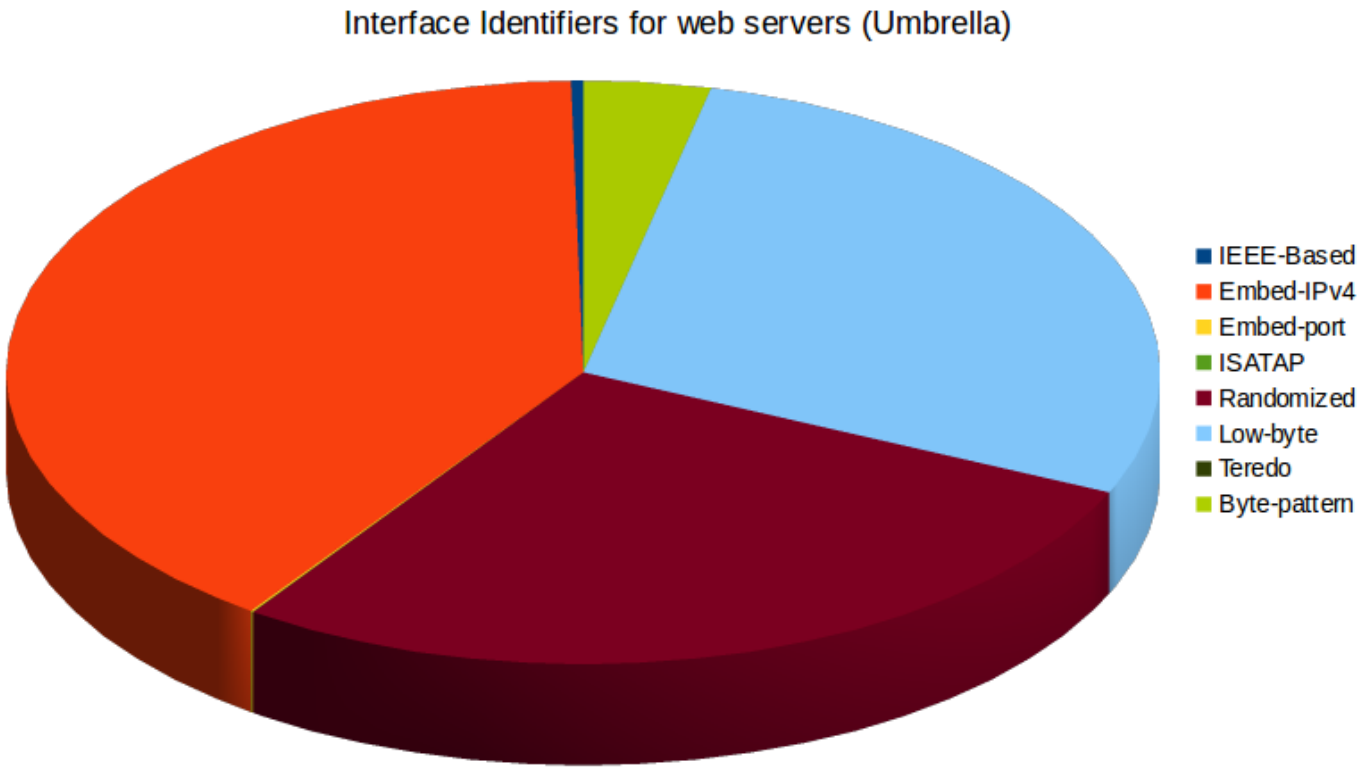
Introduction

- Recent years saw publication of:
  - RFC7217
  - RFC8064
- Any changes?

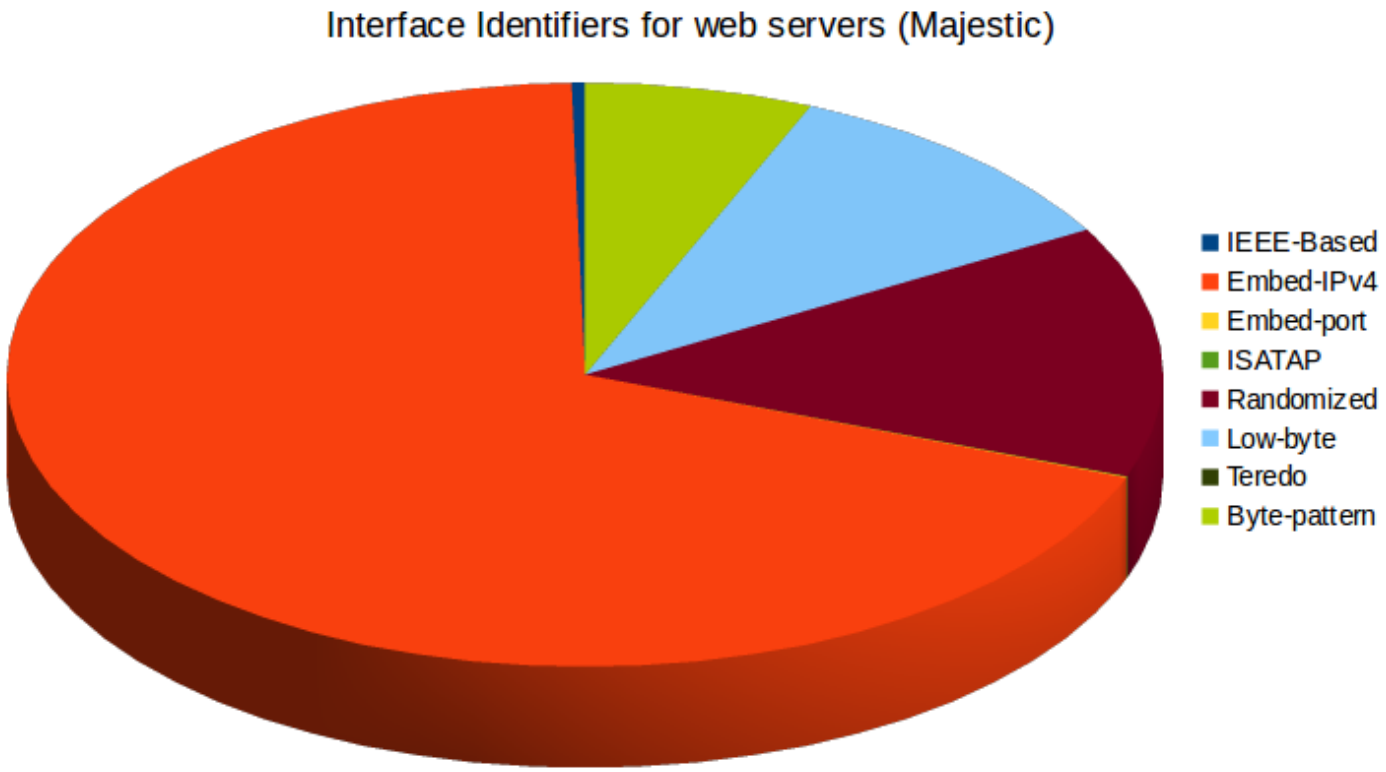
Alexa Dataset



Where to get to the most important bits?



Where to get to the most important bits?



Conclusions

- Use of randomized increased to around 15%-20% for the worst-case scenario
- These figures didn't change much for mailservers or name servers
- Curiosity: there **was not** a move from IEEE-based -> randomized

Finding Routers

Introduction

- Once you have a large number of targets, it becomes mostly trivial
- Simple tool:

```
script6 get-routers
```

Notes on DNS reverse mappings

Introduction

- DNS reverse mapping is among the most powerful techniques for IPv6 enumeration
- Any comments?

“Noise”

- Large number of dynamically generated reverse mappings for some networks:

```
Found: 2001:4998:c:80d::4062 is hz-network-migration-50568-89.gq1.yahoo.com.
Found: 2001:4998:c:80d::4064 is hz-network-migration-50568-91.gq1.yahoo.com.
Found: 2001:4998:c:80d::406d is hz-network-migration-50568-100.gq1.yahoo.com.
Found: 2001:4998:c:80d::4061 is hz-network-migration-50568-88.gq1.yahoo.com.
Found: 2001:4998:c:80d::4066 is hz-network-migration-50568-93.gq1.yahoo.com.
Found: 2001:4998:c:80d::4060 is hz-network-migration-50568-87.gq1.yahoo.com.
Found: 2001:4998:c:80d::4063 is hz-network-migration-50568-90.gq1.yahoo.com.
Found: 2001:4998:c:80d::4068 is hz-network-migration-50568-95.gq1.yahoo.com.
Found: 2001:4998:c:80d::4069 is hz-network-migration-50568-96.gq1.yahoo.com.
Found: 2001:4998:c:80d::406b is hz-network-migration-50568-98.gq1.yahoo.com.
Found: 2001:4998:c:80d::4065 is hz-network-migration-50568-92.gq1.yahoo.com.
Found: 2001:4998:c:80d::406f is hz-network-migration-50568-102.gq1.yahoo.com.
Found: 2001:4998:c:80d::406c is hz-network-migration-50568-99.gq1.yahoo.com.
```

Reliability

- Reverse mappings of /48s were more reliable than those of /32s
- May make sense to split /32s into multiple /48s for reliability purposes

Other gems

PeeringDB

- **So much** information information about IXPs!
- Including the networks and IPv6 addresses in use
- https://www.peeringdb.com/

RIPE Atlas

- In general, these devices are connected at homes or ISPs
- Thus is of help to find some home networks
- https://atlas.ripe.net/probes

Some conclusions

Some conclusions

- The IPv6 addressing architecture has required us to re-think how we do address scans. This has led to:
  - Improvements in scanning techniques
  - Improvements in IPv6 addressing to mitigate these attacks
- As address scanning becomes less attractive, other techniques become more relevant
  - DNS reverse mappings comes to mind
  - But others will likely be developed
- IPv6 is still a moving target: both for attack and for defense

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

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

www.si6networks.com