DNS as a Forensics Tool

Dr. Paul Vixie, CEO
Farsight Security, Inc.
2014-06-23 – FIRST, Boston

Internet as Territory

- But what **is** the internet?
  - It's the largest equivalence class in the reflexive transitive symmetric closure of the relationship *can be reached by an IP packet from*
    - (Seth Breidbart)
- IP addresses, IP packets, underlie everything
- We overlay IP with many things, e.g., *the web*
- Most important overlay (a layer) is: DNS

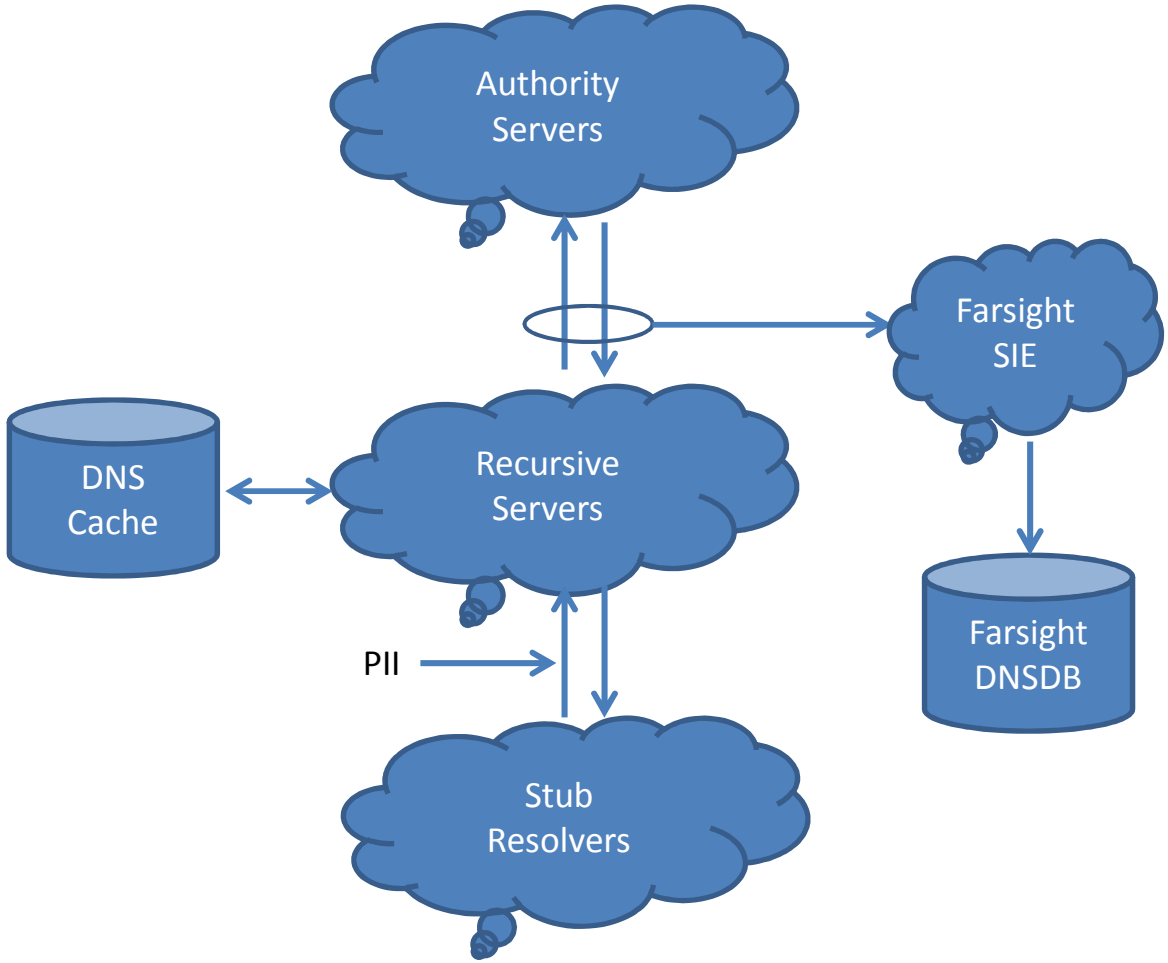
DNS as Map

- Every thing we do every day on the Internet…
  - B2C Web, B2B Web, E-mail, I-M, <*your idea here*>
  - …relies on TCP/IP, and begins with a DNS lookup
- Mobile Internet is dominated by search…
  - …but search itself relies extensively upon DNS
- DNS has a rigorous internal structure
  - Things that are in fact related, are related in DNS
  - You can have *whois* privacy, but not DNS privacy

Criminal DNS

- The Internet has been a great accelerator of human civilization
  - Sadly, the criminals came along for the ride
- Criminals can't do Internet crime without DNS
  - Cheap throw-away domain names
  - DNS registrars and servers in bad neighborhoods
  - *Whois* privacy or simply bad *whois* data
- *Nature, to be commanded, must be obeyed*.
  - (Francis Bacon)

Domain Name System Data Flow

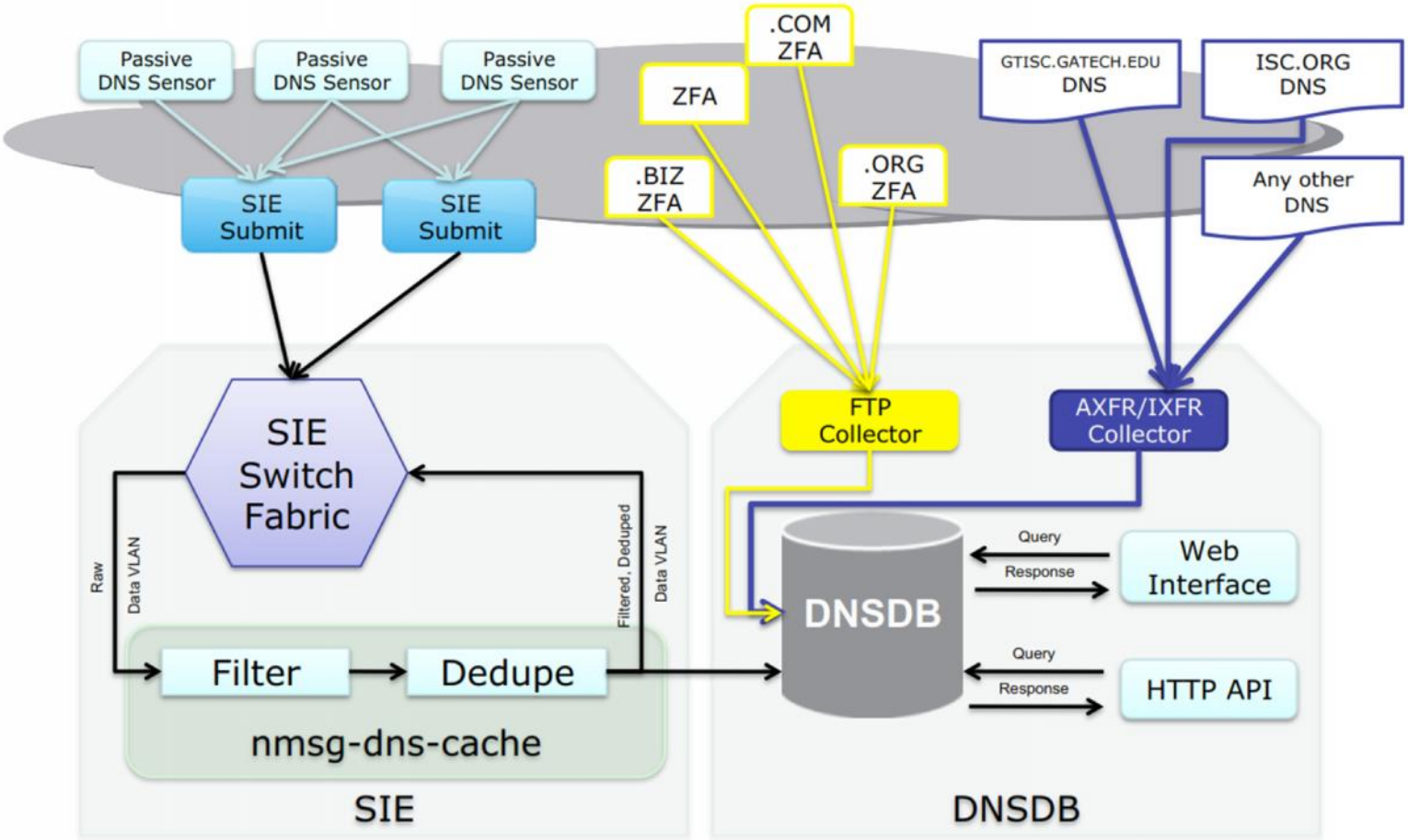


So, About that Internal Structure

- Domain names are grouped into *zones*
- A *zone* has one or more *name servers*
- Each *name server* has one or more *addresses*
- Other domain names also have *addresses*
- IP *addresses* are grouped into *netblocks*
- Domain names appear in a lot of places:
  - Web – http://*domain*/
  - E-mail – somebody@*domain*

Traditional DNS Forensics

- DNS lets anybody look up a <*domain*,*type*>
  - You get back the current set of *resource records*
  - But there's no way to see the history
  - And, your query exposes your interest
- *Whois* lets you check ownership of a domain
  - But it's usually hidden/private or inaccurate




DNSDB Search
Search mode:
RRset
Rdata
Record type:
ANY
Domain name:
*.google.com
Bailiwick:
com
Search
Reset

RRset results for *.google.com/ANY

Found 4 RRsets in 0.22 seconds.

bailiwick	**com.**
first seen	2010-06-24 03:08:18 -0000
last seen	2010-07-26 22:33:51 -0000
first seen in zone file	2010-04-24 16:12:21 -0000
last seen in zone file	2010-07-26 16:10:15 -0000
google.com.	NS ns1.google.com.
google.com.	NS ns2.google.com.
google.com.	NS ns3.google.com.
google.com.	NS ns4.google.com.

bailiwick	**com.**
first seen in zone file	2010-04-24 16:12:21 -0000
last seen in zone file	2010-07-25 16:09:21 -0000
a.l.google.com.	A 74.125.53.9

bailiwick	**com.**
first seen in zone file	2010-04-24 16:12:21 -0000
last seen in zone file	2010-07-25 16:09:21 -0000
b.l.google.com.	A 74.125.45.9

bailiwick	**com.**
first seen in zone file	2010-04-24 16:12:21 -0000
last seen in zone file	2010-07-25 16:09:21 -0000
f.l.google.com.	A 72.14.203.9

Rdata results for **ANY/a.l.google.com.**

Found 2 RRs in 0.10 seconds.

```
20comments.com.  NS  a.l.google.com.
antifavlc.com.   NS  a.l.google.com.
```

RRset results for **antifavlc.com./ANY**

Found 1 RRsets in 0.04 seconds.

bailiwick **com.**
first seen in zone file 2010-04-24 16:12:21 -0000
last seen in zone file 2010-07-25 16:09:21 -0000

```
antifavlc.com.  NS  a.l.google.com.
antifavlc.com.  NS  ns1.google.com.
antifavlc.com.  NS  a.gtld-servers.net.
antifavlc.com.  NS  h.root-servers.net.
```

RRset results for **a.l.google.com./ANY**

Found 1 RRsets in 0.02 seconds.

bailiwick **com.**
first seen in zone file 2010-04-24 16:12:21 -0000
last seen in zone file 2010-07-25 16:09:21 -0000

```
a.l.google.com.  A  74.125.53.9
```

Rdata results for **ANY/h.root-servers.net.**

Found 10 RRs in 0.02 seconds.

.	NS	h.root-servers.net.
5.3.2.0.f.3.0.8.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.0.0.5.0.1.0.0.2.ip6.arpa.	PTR	h.root-servers.net.
53.2.63.128.in-addr.arpa.	PTR	h.root-servers.net.
angelic-mariah.com.	NS	h.root-servers.net.
antifavlc.com.	NS	h.root-servers.net.
arpa.	NS	h.root-servers.net.
groupic.com.	NS	h.root-servers.net.
in-addr.arpa.	NS	h.root-servers.net.
root-servers.net.	NS	h.root-servers.net.
uidspin.com.	NS	h.root-servers.net.

Rdata results for **ANY/a.gtld-servers.net.**

Found 25 RRs in 0.06 seconds.

0.3.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.3.8.a.3.0.5.0.1.0.0.2.ip6.arpa.	PTR	a.gtld-servers.net.
0bits.net.	NS	a.gtld-servers.net.
1marketsource.net.	NS	a.gtld-servers.net.
30.6.5.192.in-addr.arpa.	PTR	a.gtld-servers.net.
antifavlc.com.	NS	a.gtld-servers.net.
apseinc.com.	NS	a.gtld-servers.net.
bigbackend.com.	NS	a.gtld-servers.net.
com.	NS	a.gtld-servers.net.
edu.	NS	a.gtld-servers.net.
fatsoft.net.	NS	a.gtld-servers.net.
foromylockerz2010.com.	NS	a.gtld-servers.net.
frau-inter.net.	NS	a.gtld-servers.net.
gbauer.com.	NS	a.gtld-servers.net.
harrispersonalinjury.net.	NS	a.gtld-servers.net.
housebuildingjobs.net.	NS	a.gtld-servers.net.
net.	NS	a.gtld-servers.net.
ns.hostingseries43.net.	NS	a.gtld-servers.net.
ns2.hostingseries43.net.	NS	a.gtld-servers.net.
offertrust.com.	NS	a.gtld-servers.net.
rf-reborn.com.	NS	a.gtld-servers.net.
shabow.com.	NS	a.gtld-servers.net.
steelwiredisplays.com.	NS	a.gtld-servers.net.
synaptrix.net.	NS	a.gtld-servers.net.
urbemar.net.	NS	a.gtld-servers.net.
witlog.net.	NS	a.gtld-servers.net.

Owner Lookup, Show History

```
$ dnsdb_query -r vix.com/ns/vix.com
...
;; record times: 2010-07-04 16:14:12 .. 2013-05-12 00:55:59
;; count: 2221563; bailiwick: vix.com.
vix.com.  NS  ns.sql1.vix.com.
vix.com.  NS  ns1.isc-sns.net.
vix.com.  NS  ns2.isc-sns.com.
vix.com.  NS  ns3.isc-sns.info.

;; record times: 2013-10-18 06:30:10 .. 2014-02-28 18:13:10
;; count: 330; bailiwick: vix.com.
vix.com.  NS  buy.internettraffic.com.
vix.com.  NS  sell.internettraffic.com.
```

Owner Wildcards, Left Hand

```
$ dnsdb_query -r \*.vix.com/a | fgrep 24.104.150
internal.cat.lah1.vix.com.  A  24.104.150.1
ss.vix.com.                 A  24.104.150.2
gutentag.vix.com.           A  24.104.150.3
lah1z.vix.com.              A  24.104.150.4
mm.vix.com.                 A  24.104.150.11
ww.vix.com.                 A  24.104.150.12
external.cat.lah1.vix.com.  A  24.104.150.33
wireless.cat.lah1.vix.com.  A  24.104.150.65
wireless.ss.vix.com.        A  24.104.150.66
ap-kit.lah1.vix.com.        A  24.104.150.67
cat.lah1.vix.com.           A  24.104.150.225
vix.com.                    A  24.104.150.231
deadrat.lah1.vix.com.       A  24.104.150.232
ns-maps.vix.com.            A  24.104.150.232
ns.lah1.vix.com.            A  24.104.150.234
```

Owner Wildcards, Right Hand

```
$ dnsdb_query -r vixie.\*/ns
;;   zone times: 2010-08-13 16:10:10 .. 2012-12-31 17:24:50
;; count: 872; bailiwick: com.
vixie.com.  NS  ns2317.hostgator.com.
vixie.com.  NS  ns2318.hostgator.com.

;;   zone times: 2010-04-24 16:12:21 .. 2010-08-12 16:09:01
;; count: 111; bailiwick: com.
vixie.com.  NS  ns23.domaincontrol.com.
vixie.com.  NS  ns24.domaincontrol.com.

;;   zone times: 2010-10-20 20:52:43 .. 2012-03-31 20:54:04
;; count: 0; bailiwick: info.
vixie.info.  NS  ns31.domaincontrol.com.
vixie.info.  NS  ns32.domaincontrol.com.
^C
```

Data Lookup, By Name

```
$ ./dnsdb_query -n ss.vix.su/mx
vix.su.                 MX  10 ss.vix.su.
dns-ok.us.              MX   0 ss.vix.su.
mibh.com.               MX   0 ss.vix.su.
iengines.com.           MX   0 ss.vix.su.
toomanydatsuns.com.     MX   0 ss.vix.su.
farsightsecurity.com.   MX  10 ss.vix.su.
anog.net.               MX   0 ss.vix.su.
mibh.net.               MX   0 ss.vix.su.
tisf.net.               MX  10 ss.vix.su.
iengines.net.           MX   0 ss.vix.su.
al.org.                 MX   0 ss.vix.su.
vixie.org.              MX   0 ss.vix.su.
redbarn.org.            MX   0 ss.vix.su.
benedelman.org.         MX   0 ss.vix.su.
```

Data Lookup, by IP Address

```
$ dnsdb_query -r ic.fbi.gov/mx
ic.fbi.gov.  MX  10 mail.ic.fbi.gov.

$ dnsdb_query -r mail.ic.fbi.gov/a
mail.ic.fbi.gov.  A  153.31.119.142

$ dnsdb_query -i 153.31.119.142
ic.fbi.gov.           A  153.31.119.142
mail.ic.fbi.gov.      A  153.31.119.142
mail.ncijtf.fbi.gov.  A  153.31.119.142
```

Data Lookup, by IP Address Block

```
$ dnsdb_query -i 153.31.119.0/24 | grep -v infragard
vpn.dev2.leo.gov.            A  153.31.119.70
mail.leo.gov.                A  153.31.119.132
www.biometriccoe.gov.        A  153.31.119.135
www.leo.gov.                 A  153.31.119.136
cgate.leo.gov.               A  153.31.119.136
www.infraguard.net.          A  153.31.119.138
infraguard.org.              A  153.31.119.138
www.infraguard.org.          A  153.31.119.138
mx.leo.gov.                  A  153.31.119.140
ic.fbi.gov.                  A  153.31.119.142
mail.ic.fbi.gov.             A  153.31.119.142
mail.ncijtf.fbi.gov.         A  153.31.119.142
```

Technical Formatting Notes

- These slides use the “terminal interface”
  - Actual agents use a web browser interface
- These slides show a DNS output conversion
  - The real output is in JSON format, i.e.:

```
$ dnsdb_query -r f.root-servers.net/a/root-servers.net
;; record times: 2010-06-24 03:10:38 .. 2014-03-05 01:22:56
;; count: 715301521; bailiwick: root-servers.net.
f.root-servers.net.  A  192.5.5.241

$ dnsdb_query -r f.root-servers.net/a/root-servers.net -j
{"count": 715301521, "time_first": 1277349038, "rrtype": "A",
"rrname": "f.root-servers.net.", "bailiwick": "root-
servers.net.", "rdata": ["192.5.5.241"], "time_last": 1393982576}
```

End Notes

- Demo
- Questions
- Thanks