Explorations in the .edu DNS namespace

John Kristoff, Dave Monnier

jtk@ultradns.net, dmonnier@ren-isac.net

Joint Techs

edu zone overview

- EDUCAUSE responsible, Verisign operated
- Approximately 7000 domains in .edu
- edu zone file is not publicly available
  - We infer/reconstruct zone file as best we can
  - we are trying to get access to the actual zone file
- As of 2007-02-13:

```
dig @a3.nstld.com soa edu. +noall +answer
edu.        86400   IN      SOA     L3.NSTLD.COM.
    NSTLD.VERISIGN-GRS.COM. 2007021201 1800 900 604800 86400
```

Surveying the edu namespace

- How do things change over time?
- Are delegations and whois data correct?
- Are edu operators making config/security mistakes?
- What DNS practices need to be encouraged?
- What alerting and monitoring can REN-ISAC provide?
- Does this make for good research projects?

The edu zone file

- Changes are more frequent than we thought
- 2006-04-28 zone file had 7648 domains
- Recently we see slightly less than 7000
- 20 names added or removed in the last two weeks
- 9312 unique NS RRs
- 4461 unique glue records (A RR for server to address mapping)

Open Resolvers

- Open resolvers (full, caching, referral)
- 4200+ (45%) of edu zone NS RRs are fully open

```
$ dig @dns.internet2.edu a +noall +answer www.nytimes.com
www.nytimes.com.        254     IN      A       199.239.136.200
www.nytimes.com.        254     IN      A       199.239.136.245
www.nytimes.com.        254     IN      A       199.239.137.200
www.nytimes.com.        254     IN      A       199.239.137.245
```

NS RRset Diversity

```
$ dig @a3.nstld.com ns +noall +authority +additioal ucdavis.edu
ucdavis.edu.              172800  IN      NS      DNS-TWO.ucdavis.edu.
ucdavis.edu.              172800  IN      NS      DNS-ONE.ucdavis.edu.
DNS-ONE.ucdavis.edu.      172800  IN      A       128.120.252.9
DNS-TWO.ucdavis.edu.      172800  IN      A       128.120.252.10

$ whois -h whois.cymru.com " -t 128.120.252.9"
AS      | IP               | BGP Prefix          | AS Name
6192    | 128.120.252.9    | 128.120.0.0/16      | UCDAVIS-CORE

$ whois -h peer-whois.cymru.com 128.120.252.9
PEER_AS | IP               | AS Name
2153    | 128.120.252.9    | CSUNET-NE - California State University Network

$ traceroute 128.120.252.9 -nq1
[...]
12  137.164.24.226  25.742 m
13  128.120.252.9  25.905 ms

$ traceroute 128.120.252.10 -nq1
[...]
12  137.164.24.226  31.094 ms
13  128.120.252.10  25.781 ms
```

Other security/robustness areas of concern

- Non-DNS services on DNS servers (e.g. TELNET, SMTP, HTTP)
- Source port selection of caching resolvers
- Cache poisoning
- Lame delegations
- Outdated root.hints file
- Delegations (NS RRs) point to CNAMEs
- Port and Protocol (TCP) filtering
- EDNS0 support

Other areas of interest

- Default and custom TTL usage
- IPv6 support
- Private namespace leaks (e.g. RFC 1918 PTRs, .local)
- DNSSEC
- Forward and reverse naming discrepancies
- Authoritative and caching service coupling
- Transitive trust
- Parent and child NS RRset inconsistency

Parting shots

```
$ dig accutech.edu ns +noall +answer
accutech.edu.           3600    IN      NS      ns101.accutech.local.
accutech.edu.           3600    IN      NS      main.accutech.local.

$ dig riosalado.edu ns +noall +answer
riosalado.edu.          600     IN      NS      dns1.riosalado.edu.
riosalado.edu.          600     IN      NS      *.ezp1r.riosalado.edu.
riosalado.edu.          600     IN      NS      dns2.riosalado.edu.

$ dig westminstercollege.edu ns +noall +answer
westminstercollege.edu. 28800   IN      NS      tao.westminstercollege.edu.
westminstercollege.edu. 28800   IN      NS      te.westminstercollege.edu.
westminstercollege.edu. 28800   IN      NS      146.86.1.2.
westminstercollege.edu. 28800   IN      NS      146.86.1.22.
westminstercollege.edu. 28800   IN      NS      chi.westminstercollege.edu.

$ dig nscc.edu ns +noall +answer
nscc.edu.               86400   IN      NS      ns1.tec.net.
nscc.edu.               86400   IN      NS      nsccdcdmz.nscc.edu.
nscc.edu.               86400   IN      NS      nsccdrdns.nscc.edu.
nscc.edu.               86400   IN      NS      ns1.tbr.edu.
nscc.edu.               86400   IN      NS      nsccdcdmz.nsccpub.ext.
```

Analysis Infrastructure

- REN-ISAC provided DNS server/probe host
- DePaul University compsci research/server probe host
- Various scripts (mostly Perl)
- Revision control and databases
- Regularly scheduled tests and analysis
- Web-based submissions and portal pages
- Automated alerting and reporting

Contacting affected sites

- Immediate notifications
  - Some via direct contact
  - Some with notification style email
  - Re-checking and following through

Repeating the process

- Re-checking the entire TLD every N
- Service opportunity
  - On demand services for members
  - Educational opporunity

Unintended value

- Research required collecting all DNS info for the TLD
  - Review of last 6 months of incident data showed 1 DNS server a month compromised