DNSSEC on Campus

By

Michael Sinatra

University of California, Berkeley

- You didn't think I was really going to use that font, did you?

What we did

- Began validating DNSSEC responses on our caching resolvers using ISC DLV in October 2008
- Participated in EDUCAUSE EDU testbed, Fall 2009
- Began signing berkeley.edu and most subzones, plus in-addr.arpas in January 2010. Have not yet placed our keys in any DLV or TAR

Why do it?

- Yes there is risk:
  - Research universities should still be willing to be on the bleeding edge.
  - Risk should be reasonable.
  - There is recognition at UC Berkeley that we have had a role in the development of the Internet and we shouldn't (have) abandon(ed) that role.

DLV: How'd it go?

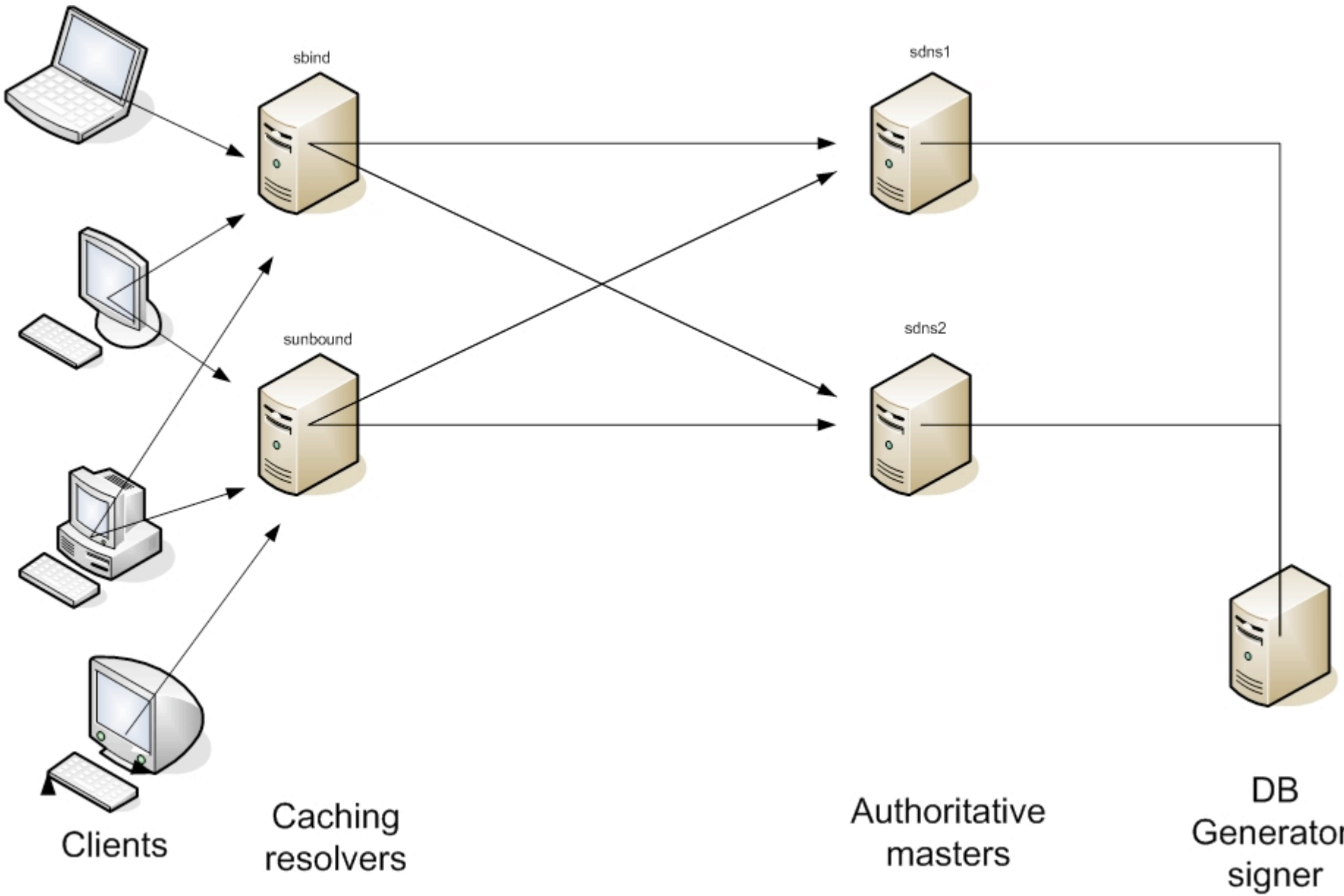
- Surprisingly well.
- Three failures in 16 months.
  - GOV NSEC3 validation
    - This was a BIND (<9.6.0) coding issue (now fixed). unbound already supports NSEC3.
  - Signing issues (the first one was a doozy)
    - (didn't get too much flak, though)
    - This is a basic DNSSEC issue, not a DLV issue

DLV: How'd it go?

- The irony is that early validators may have had an easier time of it.
- Now that GOV agencies are under the gun to "sign-baby-sign," we're seeing a number of issues, and sometimes we're paying for it.

EDU testbed

- UCB participated beginning in September 2009.
- Created our own testbed.
- Published keys in EDU testbed and created stub zones for testbed EDU zone to allow test resolvers to validate.
- Worked well and we learned a lot.


sbind
sunbound
sdns1
sdns2
Clients
Caching resolvers
Authoritative masters
DB Generator/ signer

EDU testbed

- What did we learn
  - Signing is not as hard as I feared, but it is tricky.
  - If your signatures expire (usually because you don't re-sign your zone periodically), your zone WILL BREAK.
  - Serial number manipulation can be tricky, especially when you already have one process and your signing tools assume a different process.
  - ZSK rollover isn't so bad, but KSK rollover can be tricky.
  - Algorithm rollovers (e.g. RSASHA1 to DSA or RSASHA1 to RSASHA512) are even trickier.
    - MUST have KSKs and ZSKs for both algorithms (RFC 4035)…
    - …but implementations handle incomplete algorithm pairs differently!

Signing berkeley.edu

- For real
  - We had a two week campus-wide furlough/shutdown and it was too hard to pass up.
  - Decided to get the signed zones into the authoritative servers but not publish the trust anchor in any TAR or DLV.
    - Wanted to test effects of much larger responses
    - Worried about firewalls and the like
    - Wanted to give myself some leeway will I tweaked my automated signing processes, in case I occasionally screwed sigs up.
    - More time to test!
  - UCB already had an automated signing process, so need to modify that for DNSSEC.
  - Did it for the testbed, now had to modify it for production.

Signing berkeley.edu

- For real
  - Had to warn campus!
    - http://ls.berkeley.edu/mail/micronet/2009/1520.html
    - http://net.berkeley.edu/DNS/dnssec.html
  - You will want to do this!
  - Also, let your secondaries know and make sure that they support DNSSEC. Don't learn nrc.gov's lesson the hard way!

Signing berkeley.edu

- Signed zones were populated into authoritative servers between 1-3 January 2010.
  - Didn't want to mess anything up for end-of-year giving.
  - Populated gradually to make sure that secondaries (U. Oregon, SNS@ISC) could handle. (Didn't doubt it, but did want to verify.)
- Once all auth servers had the signed zones, I worried about firewalls.
  - Created 'sacrificial lamb'.

```
options {
  …
  minimal-responses yes; // only send answer
  max-udp-size 512;      // EDNS0 responses limited to 512B
  …
};
```

Signing berkeley.edu

- Caused NSes that were sending DO (w/EDNS0) but weren't getting responses back to eventually fall over to sacrificial lamb
- Even got a security/abuse report!

```
2010-01-14 09:13:54 - Big Bomb -
Source:128.32.136.6,0,WAN -
Destination:1xx.xxx.xxx.xx,0,LAN
```

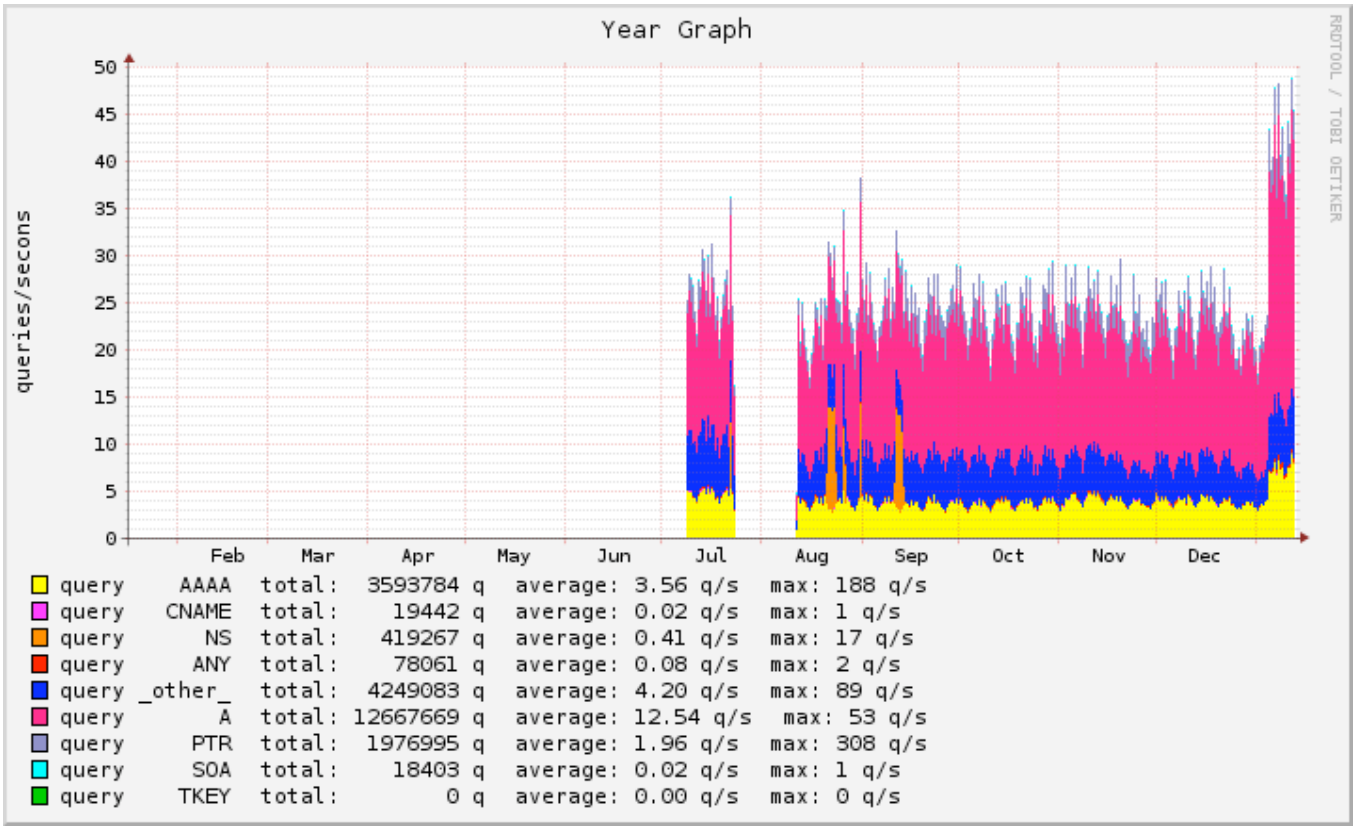
- Real IP address was included, so was able to correlate this with logs:

```
13-Jan-2010 15:13:54.434 client 1xx.xxx.xxx.xxx#1025:
query: www.lib.berkeley.edu IN A -ED (128.32.136.6)
```

- Client hit sacrificial lamb about a second later, and didn't query any other auth servers. Looks like it worked!
- Found many other cases of queriers bouncing around our auth servers and then querying sacrificial lamb.
- Some also disabled EDNS0. (More to discuss in BoF.)

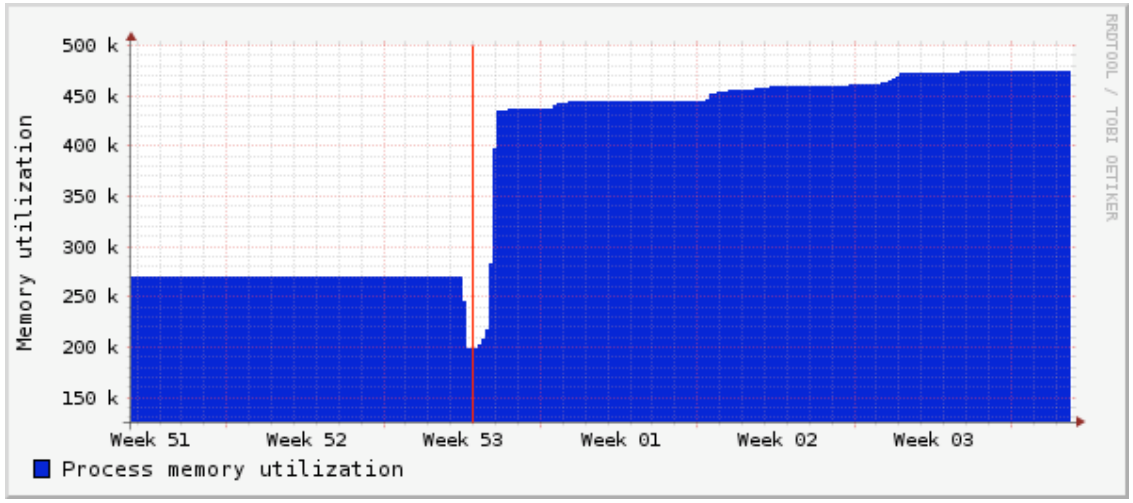
Signing berkeley.edu

- Queries to sacrificial lamb (bindgraph):



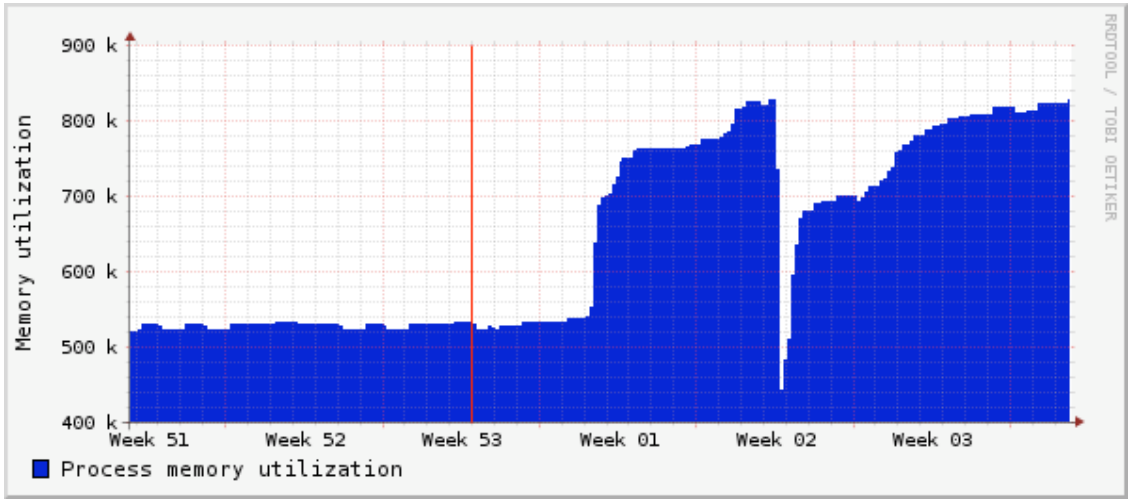
Signing berkeley.edu

- Memory footprint for an authoritative server:



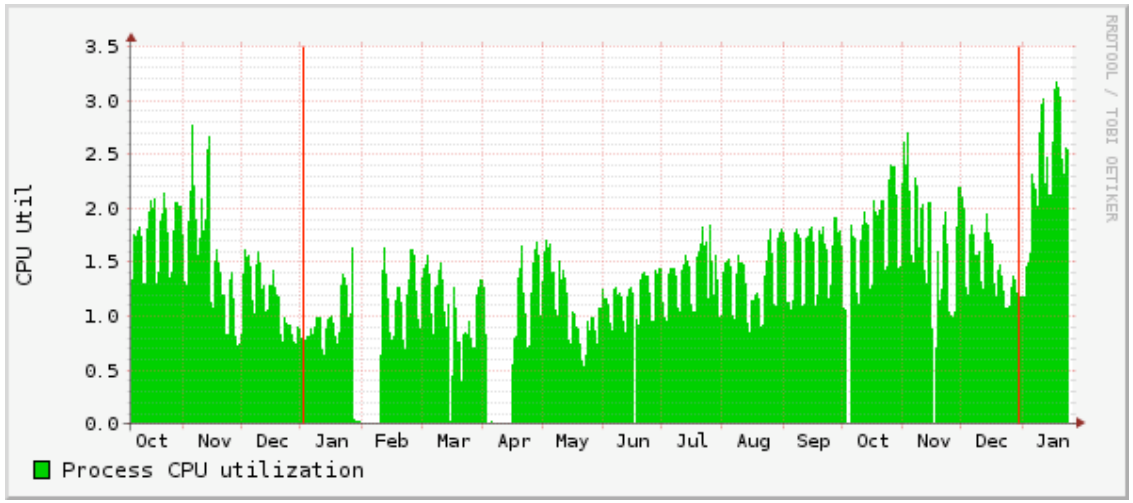
Signing berkeley.edu

- Memory footprint for a caching server:



Signing berkeley.edu

- CPU utilization for a caching server:



Signing berkeley.edu

- Current status:
  - Zones are being signed every night, and I have not experienced any validation problems (yet).
  - Haven't published KSK in any TAR or DLV; may wait until EDU is signed.

Lessons/Concludatory remarks

- Memory/CPU requirements are bigger, but well within today's capacities.
  - Signing is on an old machine and it takes about 30-45 minutes to sign 607 zones of varying sizes.
  - Basically, it has taken us so long to deploy DNSSEC that the hardware has caught up!
- Lot's of stuff to go wrong.
  - Test, test, test
  - Monitor, monitor, monitor
- Outside of my control (not totally)
  - Bugs, implementation issues.
  - Standards under-specify use of KSKs and ZSKs; implementations deal with operational practices differently.
- More things to do:
  - Use smokeping DNS probes at validating and non-validating servers for important zones to make sure validation is working.
  - Better key management for DR and backup.
  - Use FreeBSD jails on masters and put keys outside of the jail where named runs.

Thanks to…

- Internet Systems Consortium
  - Paul Vixie, Mark Andrews, Michael Graff, Keith Mitchell, Peter Losher
- EDUCAUSE
  - Becky Granger
- Verisign
  - Dave Blacka, Matt Larson, David Smith, others…
- UC Berkeley
  - Jim Blair, Paul Fisher (E-mail), (ex-) Network Services Group
- Internet2 DNSSEC working group
  - Everyone, especially Shumon Huque, Casey Deccio, Joe St. Sauver, Scott Rose, Steve Crocker, many others
- Others:
  - Olaf Kolkman

The

End