Higher Education Experiences With DNSSEC Signing

Michael Lambert, Pittsburgh Supercomputing Center
Dan Pritts, Internet2
Michael Sinatra, University of California, Berkeley
Joe St Sauver, Internet2/University of Oregon

4:30-5:30PM, Wed Nov 3, 2010, Ballroom 1

Fall 2010 Internet2 Member Meeting, Atlanta

http://pages.uoregon.edu/joe/dnssec-signing-panel/

Problem Statement

Doing DNSSEC involves **two** tasks:

1) Cryptographically **signing** authoritative DNS records, and

2) **Validating** those signatures on recursive resolvers.

Unfortunately:

There's nothing to validate if people don't sign

A limited number of domains (including relatively few dot edu's) have signed to-date.

24 Signed 2nd Level Dot Edus (per UCLA SecSpider)

Berkeley.edu

Carnegiemellon.edu

Cmu.edu

Desales.edu

Example.edu

Fhsu.edu

Indiana.edu

Internet2.edu

Iu.edu

Iub.edu

Iupui.edu

K-state.edu

Ksu.edu

Lsu.edu

Merit.edu

Monmouth.edu

Penn.edu

Psc.edu

Suu.edu

Tbu.edu

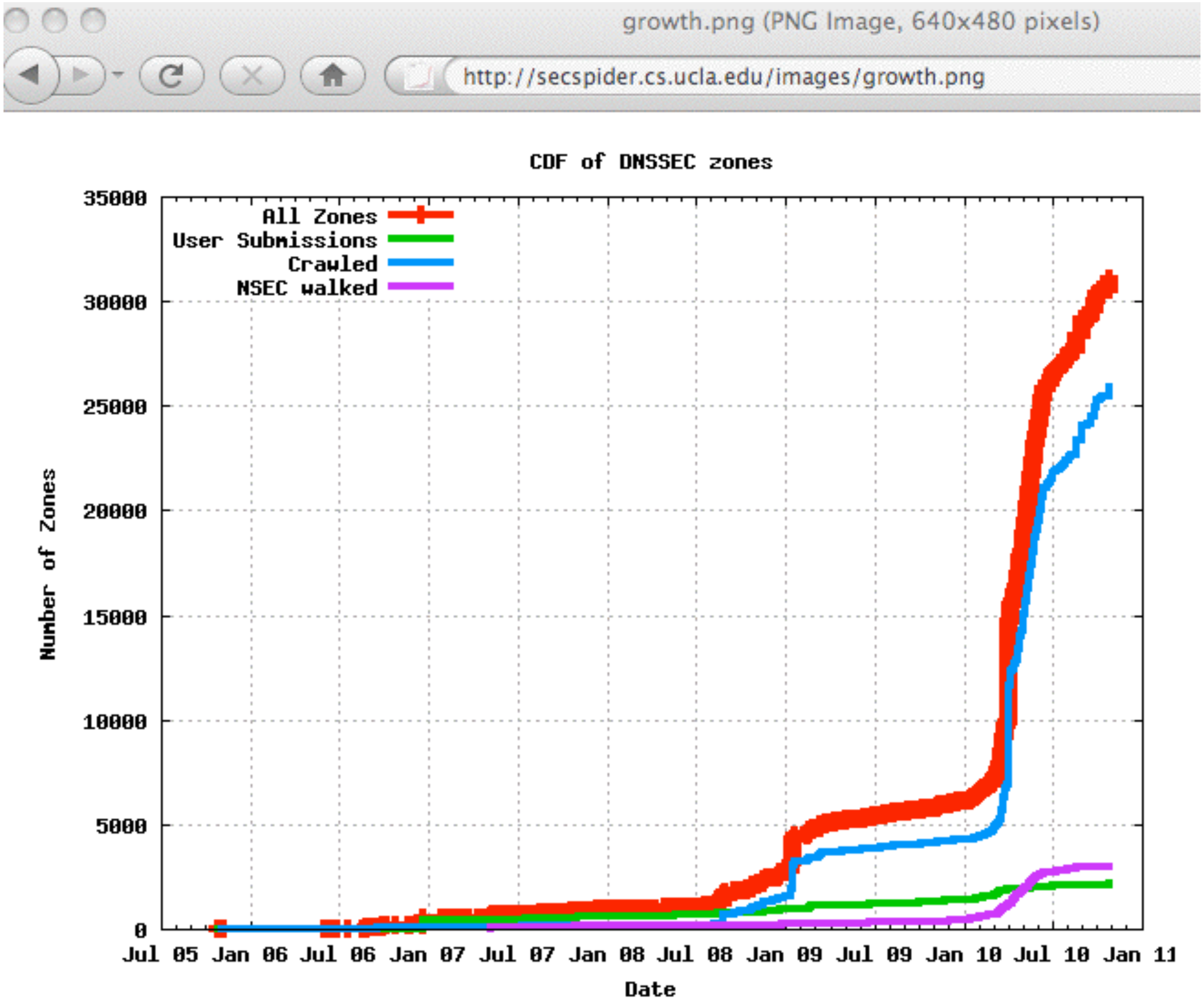
Ucaid.edu

Upenn.edu

Upf.edu

Weber.edu

BUT, We're At A DNSSEC Adoption Inflection Point



Three Panelists Who Have Signed Their 2nd Level Zones

Today we're going to be hearing from representatives of three edus who have signed their production domains:

-- Michael Lambert, Pittsburgh Supercomputing Center

-- Dan Pritts, Internet2

-- Michael Sinatra, University of California, Berkeley

What lessons can we learn from the experiences of these early adopters?

Some Discussion Questions

1) How long have you been signing your zone(s) now?

2) What motivated you to sign your zones?
-- Concerns about DNS insecurity?
-- Desire to experiment and get experience with DNSSEC?
-- Management "encouragement?"
-- Other?

3) What zone or zones did you begin with?
-- A test/trial zone?
-- More important production zone(s)?
-- Have you also signed your inverse address (in-addr/ptr) zone?

Some Discussion Questions

4) What tool or product are you using to sign your zones?

-- Has that tool or product worked well for you? Did you run into any issues? Any tips

-- Did you try any other tools? What was good or bad about those alternatives?

5) Did you see any performance impacts when you signed your zone?

Any increase in zone size?

Any increase in server memory, CPU, I/O, or network usage?

6) Did you spend time thinking about what algorithms you wanted to use to sign your zones? What did you pick and why? How about the key length you selected?

Some Discussion Questions

7) DNSSEC signatures are valid for a specified period of time. What validity period are you using? Have you run into any issues when rolling over keys?

8) What TTLs are you using for your DNSSEC-related records?

9) Do you do dynamic DNS? Is that compatible with DNSSEC?

10) Have you run into any firewall-related issues?

11) Many sites in higher education have offsite secondary DNS servers. Have you encountered any problem with DNSSEC and the secondary DNS servers you may use?

Some Discussion Questions

12) How hard was it to get DNSSEC records added by the registry?

13) How are you protecting your private keys from being compromised? Do you think your organization understands how important those crypto keys are?

14) Are you monitoring your DNSSEC signed zone(s)? If so, what tool are you using to do that monitoring?

15) Do you have any emergency procedures in place to push a resigned zone if there are any unexpected issues?