

# DNSSEC In Higher Education

Joe St Sauver, Ph.D.

Internet2 Nationwide Security Program Manager  
(joe@internet2.edu or joe@uoregon.edu)

AMSAC Call, 1PM Pacific, 1/27/2011

<http://pages.uoregon.edu/joe/amsac-dnssec/>

Disclaimer: all opinions my own

# Purpose of DNSSEC

- The domain name system (DNS) is a fundamental service – virtually every application relies on DNS to translate names (such as `www.internet2.edu`) to IP addresses (such as `207.75.164.151`)
- Unfortunately, cyber attackers can corrupt the answers that DNS servers return, attempting to mislead users into going to the wrong site (for example, if you were trying to go to your bank, you might be taken to a “knock off” bank site in the Ukraine, or you might be involuntarily taken to a malware infected site).
- That intentional DNS misdirection is normally accomplished via a technical attack known as “cache poisoning.” (This is not just a theoretical attack; cyber criminals are actually using this one)
- Cache poisoning attacks can be prevented if the authoritative DNS servers (which answer DNS queries) cryptographically sign their DNS data, and recursive resolvers (which generate DNS queries) cryptographically validate the signatures they’re given.

# Keys and Chains of Trust

- All cryptographic protocols need some solution for managing keys and maintaining “chains of trust.”
- DNSSEC uses a so-called “tree model,” beginning with cryptographic keys for the root of the DNS tree (“.”)
- For a long time, the root wasn't signed, which meant that you needed to manually maintain trust anchors for each DNSSEC-enabled top level domain, or look to a third party to maintain those trust anchors for you. That's no longer a problem: the root got officially signed on July 15<sup>th</sup>, 2010.
- We're also fortunate that the dot edu domain was also DNSSEC signed, effective August 2<sup>nd</sup>, 2010. That means that those of us who want to validate 2<sup>nd</sup> level dot edu DNSSEC signatures now don't need to manually collect and maintain trust anchors for each such domain (unlike dot com, which still isn't DNSSEC signed)

# Are Any Schools Currently Signing Their 2<sup>nd</sup> Level dot edu domains?

- Yes. <http://secspider.cs.ucla.edu/> tracks (most) domains that are DNSSEC signing their zones, including (most) dot edu's.
- Schools that are known to have signed their 2<sup>nd</sup> level dot edu zones include:  
(1) baker.edu, (2) berkeley.edu, (3) bethelks.edu, (4) cameron.edu,  
(5) carnegiemellon.edu, (6) cmu.edu, (7) colostate.edu, (8) columbia.edu,  
(9) csub.edu, (10) desales.edu, (11) eunc.edu, (12) fhsu.edu, (13) gatech.edu,  
(14) gtc.edu, (15) indiana.edu, (16) internet2.edu, (17) iu.edu, (18) iub.edu,  
(19) iupui.edu, (20) jhuapl.edu, (21) k-state.edu, (22) kent.edu, (23) ksu.edu,  
(24) lctcs.edu, (25) lsu.edu, (26) memphis.edu, (27) merit.edu, (28) mit.edu,  
(29) monmouth.edu, (30) odu.edu, (31) ohio-state.edu, (32) osu.edu,  
(33) penn.edu, (34) psc.edu, (35) psu.edu, (36) rpi.edu, (37) rwu.edu,  
(38) shsu.edu, (39) southern.edu, (40) suu.edu, (41) svsu.edu, (42) tbu.edu,  
(43) uaa.edu, (44) ucaid.edu, (45) ucar.edu, (46) ucberkeley.edu,  
(47) ucdavis.edu, (48) ucla.edu, (49) ucr.edu, (50) umbc.edu, (51) umkc.edu,  
(52) upenn.edu, (53) upf.edu, (54) utpa.edu, (55) valencia.edu,  
(56) washjeff.edu, (57) weber.edu, (58) wisc.edu, and (59) wnc.edu
- Note that some schools may have multiple related domains (e.g., carnegiemellon.edu and cmu.edu for example)

# How Many Schools Currently Validate DNSSEC Signatures?

- Unfortunately, we don't have solid data for that question.
- A site can enable DNSSEC validation with no externally discernible sign that they're doing so, and many sites might enable DNSSEC validation even if they don't sign their own zones. For example, while UOregon doesn't sign its own zones yet, it does validate DNSSEC signatures from other domains on its production resolvers (that part's pretty painless).
- Why doesn't EVERYONE enable DNSSEC validation? Multiple potential reasons:
  - Some recursive resolver software may not support DNSSEC
  - DNSSEC works silently; there's no discernible indication that DNSSEC is doing anything for you when everything is working the way it should. If I fix a problem and no one knows, should I bother? Some people apparently think "nah, why bother?"
  - DNSSEC can "break" domains that would otherwise be accessible, if a site accidentally screws up their DNSSEC signatures (e.g., by letting them expire); this may not be viewed as a "feature" by your users
  - DNSSEC requires support for EDNS0 ("extra long" DNS replies); some sites may have older or misconfigured firewalls that are unable to handle EDNS0 extensions
  - Chicken and egg issues ("no one's signing, so why bother trying to validate?")

# What If I Did Want To Try DNSSEC?

- Start by having a conversation with your DNS administrators -- they may already be testing or doing planning with respect to DNSSEC.
- Before embarking on DNSSEC, make sure that your DNS infrastructure is otherwise up to snuff (e.g., if you're running an ancient version of BIND on end-of-life hardware, you need to get the meat-and-potatoes handled before you get dessert!).
- <http://dnscheck.iis.se/> can help ID many DNS configuration issues.
- Recognize that you can “ease into” doing DNSSEC. For example:
  - you can try offering DNSSEC-enabled test resolvers for opt-in use (or you can try the validating resolvers that DNS-OARC is making available; see <https://www.dns-oarc.net/oarc/services/odvr> )
  - you can try signing some less-critical (“toy”) domains to get some signing experience w/o putting critical institutional assets at risk
  - you can decide you only want to sign, or only want to validate – you don't need to do both at once

# DNSSEC Resources for Your DNS Admin Team

- Begin with your current DNS vendor – DNSSEC aware vendors (such as ISC BIND) will often have specific DNSSEC documentation that will walk you through what you need to do, and obviously O’Reilly’s “DNS and BIND” (now in its 5<sup>th</sup> edition) is a bible that every DNS admin should own.
- There are also many freely available community documents, see the list at <http://www.dnssec.net/practical-documents> (I’m particularly fond of ISC’s “DNSSEC in 6 Minutes” (79 slides) from that list, see [alan.clegg.com/files/DNSSEC\\_in\\_6\\_minutes.pdf](http://alan.clegg.com/files/DNSSEC_in_6_minutes.pdf) )
- Some sites may prefer to buy rather than build. If that’s you or a site you know, you should know that there are multiple DNSSEC-enabled appliance vendors you can consider, both for DNSSEC-enabled authoritative servers and for validating resolvers (but at least some of them may not be cheap – federal agencies are prime customers, and pricing sometimes reflects that target audience).

# How AMSAC Might Be Able To Help – Some Ideas

- AMSAC or interested AMSAC participants could:
  - Publicly highlight the importance of DNS as a critical (but potentially vulnerable) service
  - Explicitly endorse DNSSEC as one important way to help improve the trustworthiness of DNS results
  - Lead by example/commit to “eating their own dog food” by working to deploy DNSSEC on their own campuses
  - Acknowledge community participants who have made the effort to deploy DNSSEC (“Map of glory” with stars for DNSSEC-enabled Internet2 participants? Plaque or other tangible award for particularly enthusiastic community DNSSEC boosters?)
  - Explicitly encourage DNSSEC appliance vendors to participate as part of the Internet2 corporate membership

# Thanks For The Chance to Talk Today!

- Are there any questions?