

Doing DNS as If DNS Actually Mattered

Joe St Sauver, Ph.D.
(joe@uoregon.edu or joe@internet2.edu)
Security Programs Manager, Internet2

IT Security Conference
Fargo, ND
October 21-22, 2008

<http://www.uoregon.edu/~joe/dnssec-nd/>

Disclaimers: All opinions expressed are solely those of the author and do not necessarily represent the opinions of any other entity. Portions of this talk have previously been presented at Internet2 Member Meetings, Internet2 Joint Techs, or MAAWG.

1. Before We Really Get Started, One Brief But Extremely Critical DNS-Related Issue, Just In Case Folks Haven't Heard...

If you take nothing else away from today's talk, please take the next few slides very seriously and check/upgrade your DNS servers as may be necessary.

If you're not the person doing DNS for your site, find out who is your DNS administrator and make sure that they've gotten this issue handled!

The “Kaminsky Vulnerability”

- **Problem:** Dan Kaminsky discovered a very efficient way to do DNS cache poisoning; DNSSEC would fix the issue, but until then you want to be **sure** to patch your resolvers. For more information, see <http://www.kb.cert.org/vuls/id/800113> (see the next slide for a brief excerpt from that notice)
- **To Test:** <https://www.dns-oarc.net/oarc/services/dnsentropy> (see the sample test report two slides forward)
- **If Necessary, Upgrade!** If your resolvers don't pass, upgrade! (If you're using BIND, see <http://www.isc.org/index.pl>)
- **Providers ARE Getting Hit:** For example, see "China Netcom DNS cache poisoning" (08/19/2008): <http://securitylabs.websense.com/content/Alerts/3163.aspx>
- **While upgrading is critical, and certainly better than nothing, DNSSEC is needed to definitively address this issue.**



- **Insufficient transaction ID space**

The DNS protocol specification includes a transaction ID field of 16 bits. If the specification is correctly implemented and the transaction ID is randomly selected with a strong random number generator, an attacker will require, on average, 32,768 attempts to successfully predict the ID. Some flawed implementations may use a smaller number of bits for this transaction ID, meaning that fewer attempts will be needed. Furthermore, there are known errors with the randomness of transaction IDs that are generated by a number of implementations. Amit Klein researched several affected implementations in 2007. These vulnerabilities are described in the following vulnerability notes:

- [VU#484649](#) - Microsoft Windows DNS Server vulnerable to cache poisoning
- [VU#252735](#) - ISC BIND generates cryptographically weak DNS query IDs
- [VU#927905](#) - BIND version 8 generates cryptographically weak DNS query identifiers

- **Multiple outstanding requests**

Some implementations of DNS services contain a vulnerability in which multiple identical queries for the same resource record (RR) will generate multiple outstanding queries for that RR. This condition leads to the feasibility of a 'birthday attack,' which significantly raises an attacker's chance of success. This problem was previously described in [VU#457875](#). A number of vendors and implementations have already added mitigations to address this issue.

- **Fixed source port for generating queries**

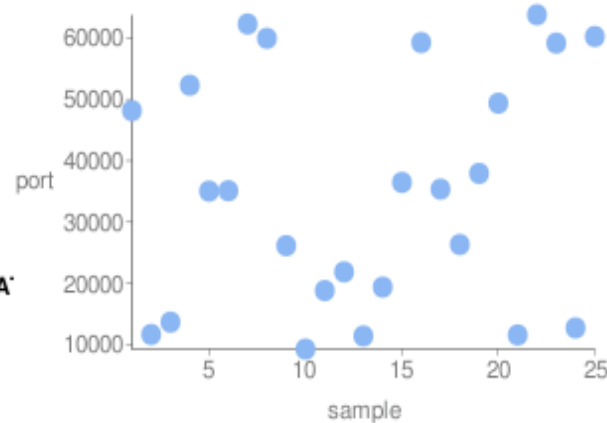
Some current implementations allocate an arbitrary port at startup (sometimes selected at random) and reuse this source port for all outgoing queries. In some implementations, the source port for outgoing queries is fixed at the traditional assigned DNS server port number, 53/udp.

1. 76.165.144.11 (wlan-reg-1-no.internet2.edu) appears to have **GREAT** source port randomness and **GREAT** transaction ID randomness.

Test time: 2008-10-15 14:22:34 UTC

Note that standard deviation is usually, but not always, a good indicator of randomness. Your brain is a better detector of randomness, so be sure to take a look at the scatter plots below. If you see patterns (such as straight lines), the values are probably less random than reported.

76.165.144.11 Source Port Randomness: **GREAT**



Number of samples: 25

Unique ports: 25

Range: 9276 - 63781

Modified Standard Deviation: 19133

Bits of Randomness: 16

Values Seen: 48150 11660 13672 52293 35029 35094 62275 59943 26140 9276
18816 21864 11416 19383 36453 59251 35356 26327 37919 49370
11579 63781 59166 12735 60236

If The Preceding Slides Didn't Mean Much To You, Don't Panic

- We're now about to rewind quite a ways, and fill in some of the background/introductory material that many of you who aren't particularly focused on DNS may be missing.
- Thus, don't worry if the preceding slides seemed chock full of gibberish -- they're aimed at your site's DNS administrator, not necessarily at you (unless you're your site's DNS administrator!)
- Just make sure that one way or the other your DNS administrator DOES see this talk!

2. With That Out of the Way, (Finally!) An Introduction

Format of This Talk

- This talk has been prepared in my normal unusually-detailed format. I use that format for a number of reasons, including:
 - doing so helps to keep me on track when I have limited time
 - audience members don't need to scramble to try to take notes
 - if there are hearing impaired members of the audience, or non-native-English speakers present, a text copy of the talk may facilitate their access to this material
 - a detailed copy of the talk makes it easy for those who are not here today to go over this talk later on
 - detailed textual slides work better for search engines than terse, highly graphical slides
 - hardcopy reduces problems with potential mis-quotation
- BUT I promise that won't read my slides to you, and I wanted to also be sure to leave some time for discussion/questions, too.

You Should Pay Attention to DNS Because:

- **"Everything" relies on DNS** (email, Usenet, IM, the world wide web, P2P, VoIP, you name it), it is ALL is built on top of DNS -- DNS is the foundation technology (or at least DNS is one of just a handful of particularly key foundation technologies – I'll certainly concede that BGP is equally as important as DNS, for example).
- **If I can control your DNS, I control your world.** Going to eBay? Maybe, maybe not, depending on what sort of DNS resolution occurs (and no, SSL certificate issues will not be sufficient to flag DNS misdirection as an issue -- users just don't get the whole certificate thing, and will just blindly accept any SnakeOil, Inc. self-signed certificate they've been handed for a "secure" site).
- **Miscreants can (and have!) attacked the trustworthiness of DNS data** on a variety of levels (cache poisoning and malware that tweaks host file entries and/or DNS registry entries on the PC are just two examples)

You Should Also Pay Attention To DNS Because... (cont. 1)

- **DNS uses UDP.** Because of that, **DNS has issues when it comes to accepting and processing spoofed query sources.** Because DNS accepts a tiny query as input, and potentially generates a huge response as output, **DNS operates as a high-gain online traffic amplifier.** Couple those two phenomena and you can do the online equivalent of vaporizing small cities with a **DNS "death ray."**
- Name servers aren't just a tool for conducting distributed denial of service attacks, **DNS servers are also a target for distributed denial of service attacks** (if I can kill your DNS service, you are off the network even if your transit links aren't flooded with traffic)
- **DNS has traditionally not been a focus of institutional love and investment;** lots of people are running old gear, old code, using part time or student DNS staff, and generally treating DNS very casually despite how operationally critical it has become.

You Should Also Pay Attention To DNS Because... (cont. 2)

- DNS is used for a lot more than just translating FQDNs to dotted quads these days.
- **DNS has effectively become a general-purpose distributed database.** DNS block lists are one example of non-traditional data distributed via DNS, RouteViews IP-to-ASN data is another, and ENUM data (see www.enum.org) is a third.
- A comment from Eric A. Hall, ca. April 16, 2001, noted in passing:
"The current DNS will only keep working if it is restrained to lookups, the very function that it was designed to serve. It will not keep working if the protocol, service, tables and caches are overloaded with excessive amounts of data which doesn't benefit from the lookup architecture."
<http://www.ops.ietf.org/lists/namedroppers/namedroppers.2001/msg00247.html>

You Should Also Pay Attention To DNS Because... (cont. 3)

- **Some people are doing some wild stuff via DNS.** Personal favorites in the "**no,-this-is-not-what-we-intended**" category relate to DNS-based "covert channel" apps such as...
 - "DnsTorrent" (see <http://www.netrogenic.com/dnstorrent/>)
 - "IP over DNS" (see <http://thomer.com/howtos/nstx.html>) or "DNS cat" (see <http://tadek.pietraszek.org/projects/DNScat/>), or
 - "Tunneling Arbitrary Content in DNS" (part of Dan Kaminski's "Attacking Distributed Systems: The DNS Case Study," see http://www.doxpara.com/slides/BH_EU_05-Kaminsky.pdf)Two other great Kaminski DNS-related talks are "Black Ops 2004@LayerOne," see <http://www.doxpara.com/bo2004.ppt> , and "Black Ops of TCP/IP 2005," see http://www.doxpara.com/slides/Black%20Ops%20of%20TCP2005_Japan.ppt
- **Note well:** sites may view "atypical" DNS usage as hostile/illegal.

You Should Also Pay Attention To DNS Because... (cont. 4)

- **Your DNS (or, more precisely, your rDNS) may determine how some people treat your email or other network traffic.**
- For example, some ISPs check that rDNS exists for the sending host; others look for "**non-dynamic**"-looking rDNS host names when deciding whether to accept or reject direct-to-MX email. See, <http://postmaster.aol.com/guidelines/standards.html> or Steve Champeon's very thorough listing at <http://enemieslist.com/>
- There are efforts underway in the IETF to encourage consistent use of rDNS, and to standardize rDNS naming practices:
-- <http://www.ietf.org/internet-drafts/draft-ietf-dnsop-reverse-mapping-considerations-07.txt>
- **What do your campus rDNS naming conventions look like?**

You Should Also Pay Attention To DNS Because... (cont. 5)

- **DNS ties into a ton of other things.**
 - Where do dynamic hosts get their DNS information? Why, often from **DHCP**, of course (so you really want to pay attention to DHCP-related security issues, too).
 - DNS can be used for **load balancing**, and DNS can selectively deliver **different answers** based on a query's source.
 - Planning on doing **IPv6**? How you handle DNS is an integral part of that, whether that's numbering plans, provisioning quad A records, making local DNS servers available via IPv6, etc.
 - DNS ties into broader Domain Name-related **policy issues** in myriad interesting ways (for example: how do you handle evil DNS glue records? what about IP whois/rwhois privacy? how do you manage the rate of routing table growth while still allowing for provider independent addresses and easy multihoming? etc₄)

You Should Also Pay Attention To DNS Because... (cont. 6)

- Some current approaches to dealing with DNS insecurities may negatively impact Internet end-to-end transparency, and ironically, foreclose other approaches to securing DNS (such as DNSSEC). The IAB recently noted in an IETF technical plenary:

"DNSSEC deployment may be hampered by transparency barriers."

[...]

"DNS Namespace Mangling

"– Recursive forwarders modifying responses are incompatible with DNSSEC."

Reflections on Internet Transparency

<http://www3.ietf.org/proceedings/06nov/slides/plenaryt-2.pdf>

Important DNS Characteristics

- **Be available** (remember, if the domain name system is unavailable, for most users, the "Internet is down")
- **Be trustworthy** (if the domain name system returns untrustworthy values, you may be sent to a site that will steal confidential data, or to a site that could infect your computer with malware)
- **Be fast** (rendering even a single web page may require tens -- or hundreds! -- of domain name system queries; can you imagine waiting even a second for each of those queries to get resolved?)
- **Be scalable** (there are billions of Internet users who rely on DNS, all around the world)
- **Be flexible** (different sites may have different DNS requirements)
- **Be extensible** (there are still many things that DNS will be called upon to do, but we don't know what all those things are yet!
We need to have the flexibility to evolve DNS as time goes by)
- **Let's begin by talking a little about how DNS currently works.**

3. A Quick Hand Waving DNS Tutorial

What The Domain Name System Does

- Pretty much everyone here probably conceptually understands how the Domain Name System (DNS) works, but just for the sake of completeness, or those who may look at this talk after the fact, let me begin with a brief (and very incomplete) functional definition:

"DNS is the network service that translates a fully qualified domain name, such as *www.uoregon.edu*, to a numeric IP address, such as *128.223.142.89*. DNS can also potentially do the reverse, translating a numeric IP address to a fully qualified domain name."

- Whenever we use the Internet we're using DNS, and **without DNS, using the Internet would become very inconvenient**. Can you imagine having to remember to go to `http://209.85.171.104/` instead of `http://www.google.com/` for example?

How Does the DNS System *Currently* Work?

- While the fine points can vary, the basic process is:
 - 1) An application (such as a web browser) requests resolution of a fully qualified domain name, such as `www.uoregon.edu`
 - 2) If the desktop operating systems includes a caching DNS client, the DNS client checks to see if that FQDN recently been resolved and cached (stored locally) -- if yes, it will use that cached value.
 - 3) If not, the desktop DNS client forwards the request for resolution to a recursive DNS server which has been manually pre-configured (or to a recursive DNS server which may have been designated as part of DHCP-based host configuration process)
 - 4) If the recursive DNS server doesn't have a recently cached value for the FQDN, the recursive DNS server will begin to make queries, if necessary beginning with the DNS root zone, until it has resolved a top level domain (e.g., `.edu`), primary domain name (`uoregon.edu`), and finally a FQDN (such as `www.uoregon.edu`)

We can simulate this process with dig on the command line. The process begins by bootstrapping via pre-specified name servers for the DNS root ("dot"):

```
% dig +trace www.uoregon.edu
```

```
.      417141 IN      NS      B.ROOT-SERVERS.NET.
.      417141 IN      NS      C.ROOT-SERVERS.NET.
.      417141 IN      NS      D.ROOT-SERVERS.NET.
.      417141 IN      NS      E.ROOT-SERVERS.NET.
.      417141 IN      NS      F.ROOT-SERVERS.NET.
.      417141 IN      NS      G.ROOT-SERVERS.NET.
.      417141 IN      NS      H.ROOT-SERVERS.NET.
.      417141 IN      NS      I.ROOT-SERVERS.NET.
.      417141 IN      NS      J.ROOT-SERVERS.NET.
.      417141 IN      NS      K.ROOT-SERVERS.NET.
.      417141 IN      NS      L.ROOT-SERVERS.NET.
.      417141 IN      NS      M.ROOT-SERVERS.NET.
.      417141 IN      NS      A.ROOT-SERVERS.NET.
```

```
:: Received 436 bytes from 128.223.32.35#53(128.223.32.35) in 0 ms
```

Next, one of the root servers identifies the NS's for the .edu TLD:

edu.	172800	IN	NS	L3.NSTLD.COM.
edu.	172800	IN	NS	M3.NSTLD.COM.
edu.	172800	IN	NS	A3.NSTLD.COM.
edu.	172800	IN	NS	C3.NSTLD.COM.
edu.	172800	IN	NS	D3.NSTLD.COM.
edu.	172800	IN	NS	E3.NSTLD.COM.
edu.	172800	IN	NS	G3.NSTLD.COM.
edu.	172800	IN	NS	H3.NSTLD.COM.

;; Received 306 bytes from 192.228.79.201#53(B.ROOT-SERVERS.NET) in 30 ms

One of those TLD name servers then identifies the NS's for uoregon.edu:

uoregon.edu.	172800	IN	NS	ARIZONA.edu.
uoregon.edu.	172800	IN	NS	RUMINANT.uoregon.edu.
uoregon.edu.	172800	IN	NS	PHLOEM.uoregon.edu.

;; Received 147 bytes from 192.41.162.32#53(L3.NSTLD.COM) in 85 ms

**And then finally, via one of the name servers for uoregon.edu,
we can then actually resolve www.uoregon.edu:**

www.uoregon.edu. 900 IN A 128.223.142.89

uoregon.edu. 86400 IN NS phloem.uoregon.edu.

uoregon.edu. 86400 IN NS arizona.edu.

uoregon.edu. 86400 IN NS ruminant.uoregon.edu.

uoregon.edu. 86400 IN NS dns.cs.uoregon.edu.

;; Received 228 bytes from 128.196.128.233#53(ARIZONA.edu) in 35 ms

DNS is An Inherently Distributed Service

- What you should glean from that example is that DNS is **inherently distributed** – every site doesn't need to store a copy of the the complete Internet-wide mapping of FQDN's to IP addrs.
- This differs dramatically from **pre-DNS** days, when mappings of host names to IP addresses happened via **hosts files**, and each server would periodically retrieve updated copies of the hosts file. (Can you imagine trying to maintain and distribute a hosts file with hundreds of millions, or **billions**, of records each day?)
- Fortunately, because DNS is distributed, it scales very well, far better than replicating host files!
- Unfortunately, because DNS is distributed, it is more complex than the conceptually simple (if practically unworkable) hosts file solution, and there can be substantial variation in how, and how well, sites and DNS administrators do DNS-related activities.
- There are a few things we can generally note, however.

DNS Efficiencies

- Most common DNS queries do not require re-resolving the TLD (.edu, .com, .net, .org, .biz, .info, .ca, .de, .uk, etc.) name servers, or even the name servers for 2nd level domains such as google.com or microsoft.com -- those name servers change rarely if ever, and will typically be statically defined via "glue" records, and cached by the local recursive name server. (Glue records assist with the DNS bootstrapping process, providing a static mapping of name server's FQDNs to its associated dotted quad.)
- Cached data which has been seen by a DNS server will be reused until it "cooks down" or expires; cache expiration is controlled by the TTL (time to live) associated with each data element. TTL values are expressed in seconds.
- Negative caching (the server may remember that a FQDN **doesn't** exist) may also help reduce query loads; see "Negative Caching of DNS Queries (DNS NCACHE)," RFC2308.

A Few More DNS Notes

- The DNS entries for domains are contained in **zones**. For example, there would normally be one zone for uoregon.edu and another zone for oregonstate.edu
- The **primary** DNS server for a given domain normally is augmented by a number of **secondary** (or "slave") DNS servers. Secondary servers are deployed to help insure domains remains resolvable even if a primary server becomes unreachable.
- Secondary DNS servers periodically retrieve updated zone data for the zones they secondary from the primary DNS server. Most sites limit who can download a complete copy of their zone file because having a definitive listing of all hosts in a given domain may be useful for cyber reconnaissance and attack purposes.
- It is common for universities to agree to provide secondary DNS service for each other, e.g., Arizona does runs a secondary for UO. But ALSO see the excellent <http://www.ripe.net/ripe/meetings/ripe-52/presentations/ripe52-plenary-perils-transitive-trust-dns.pdf>

Despite Being Critical to the Functioning of the Internet, DNS Is Seldom Given Much Attention

- Doing DNS for a company is not a particularly “glamorous” or “high prestige” job (unlike being a wide area network engineer, few novices aspire to some day become a DNS administrator)
- DNS servers seldom receive the care or lavish attention that mail servers, web servers, firewalls, or switches and routers receive, and enterprise DNS architectures and operational approaches are frequently quite simple
- To the best of my knowledge, there are no routinely scheduled and reoccurring conferences devoted exclusively to DNS-related research or operational praxis, except <https://www.dns-oarc.net/>
- DNS is thus simultaneously operationally critical **and** managerially insignificant to the point of often being neglected
- **For example, can your domain pass the dnscheck.iis.se tester?**

**.se**[▶ Home](#)[▶ FAQ](#)

Test your DNS-server and find errors

Enter your domain name in the field below to test the DNS-servers that are used. Example: iis.se

Test now

About DNSCheck

DNSCheck is a program that was designed to help people check, measure and hopefully also understand the workings of the Domain Name System, DNS. When a domain (aka zone) is submitted to DNSCheck it will investigate the domain's general health by traversing the DNS from root (.) to the TLD (Top Level Domain, like .SE) to eventually the nameserver(s) that holds the information about the specified domain (like iis.se). Some other sanity checks, for example measuring host connectivity, validity of IP-addresses and control of DNSSEC signatures will also be performed.



About the domain name system. DNS

**4. Even If You Aren't Paying Much
Attention to DNS, the Bad Guys Sure Are:
For Example, Consider Malware and DNS**

Spam-Related Malware Relies on DNS

- Much of the most virulent malware out there has been deployed to facilitate spamming, and that spam-related malware is notorious for generating large numbers of DNS queries for MX host information (so the spamware can determine where it should connect to dump its spam).
- Spam related malware may also refer to upstream command and control hosts by their FQDNs, thereby making it possible for the miscreants to repoint their malware's command and control host from one dotted quad to another, should the system currently "hosting" their C&C get filtered or cleaned up.
- At the same time that malware critically **relies** on DNS, ironically other malware may **also** be actively working to interfere with legitimate DNS uses.

Why Would Malware Interfere With DNS?

- Authors of some viruses, trojan horses and other malware may interfere with user DNS for a variety of reasons, including:
 - attempting to block access to remediation resources (such as system patches, AV updates, malware cleanup tools)
 - attempting to redirect users from legitimate sensitive sites (such as online banks and brokerages) to rogue web sites run by phishers
 - attempting to redirect users from legitimate sites to malware-tainted sites where the user can become (further) infected
 - attempting to redirect users to pay-per-view or pay-per-click web sites in an effort to garner advertising revenues

Examples of Malware Interfering with DNS

- **Trojan.Qhosts** (discovered 10/01/2003)
<http://www.sarc.com/avcenter/venc/data/trojan.qhosts.html>
"Trojan.Qhosts is a Trojan Horse that will modify the TCP/IP settings to point to a different DNS server."
- **MyDoom.B** (published 1/28/2004)
<http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=38114>
"The worm modifies the HOSTS files every time it runs to prevent access to the following sites [list of sites deleted]"
- **JS/QHosts21-A** (11/3/2004)
<http://www.sophos.com/virusinfo/analyses/jsqhosts21a.html>
"JS/QHosts21-A comes as a HTML email that will display the Google website. As it is doing so it will add lines to the Windows Hosts file that will cause requests for the following websites to be redirected: www.unibanco.com.br, www.caixa.com.br, www.bradesco.com.br"

More Examples of Malware Tweaking DNS

- **Trojan.Flush.A** (discovered 3/4/2005)
<http://www.sarc.com/avcenter/venc/data/trojan.flush.a.html>
'Attempts to add the following value [...]:
"NameServer" = "69.50.176.196,195.225.176.37"'
- **DNSChanger.a** (added 10/20/2005)
http://vil.mcafeesecurity.com/vil/content/v_136602.htm
"Symptoms: [...] Having DNS entries in any of your network adaptors with the values: 85.255.112.132, 85.255.113.13"
- **DNSChanger.c** (added 11/04/2005)
http://vil.nai.com/vil/Content/v_136817.htm
"This program modifies registry entries pertaining to DNS servers to point to the following IP address: 193.227.227.218"

ZLOB Trojan (9/3/2006)

- ZLOB is a piece of "fake video codec" DNS-tinkering malware, see http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_ZLOB.ALF&VSect=Sn and <http://www.trendmicro.com/vinfo/secadvisories/default6.asp?VNAME=The+ZLOB+Show%3A+Trojan+poses+as+fake+video+codec%2C+loads+more+threats&Page=> , which notes:

TROJ_ZLOB.ALF, for instance, modifies an affected system's registry to alter its DNS (Domain Name System) settings, such that it connects to a remote DNS server that is likely controlled by a remote malicious user. Thus, using this setup, the said remote user can decide what IP address the affected system connects to when the affected user tries to access a domain name.

At the time when it was first detected, TROJ_ZLOB.ALF redirects users to adult-themed sites. Of course, by now the DNS server could have been changed already -- perhaps by the highest bidder it was rented to -- so that connections are redirected to other, possibly malicious, sites instead.

Trojan.Flush.K (1/18/2007)

- http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-011811-1222-99&tabid=2 states:

'The Trojan then creates the following registry entries: [...]
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\Tcpip\Parameters\Interfaces\[RANDOM
CLSID]"DhcpNameServer" = "85.255.115.21,85.255.112.91"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\Tcpip\Parameters\Interfaces\[RANDOM
CLSID]"NameServer" = "85.255.115.21,85.255.112.91"

- And there are MANY, MANY more. **The bad guys ARE attempting to accomplish their goals via your users' reliance on DNS.**

The Mechanics: 53/UDP and 53/TCP

- Most DNS queries are made over port 53/UDP, but some queries may return more data than would fit in a normal single DNS UDP packet (512 bytes). When that limit is exceeded, DNS will normally truncate, and retry the query via 53/TCP.
- Occasionally you may run into a site where either 53/**UDP** or 53/**TCP** has been blocked outright for all IP addresses (including for real name servers!) at a site. That's a really bad idea.
- Blocks on **all** 53/**TCP** traffic sometimes get temporarily imposed because of the misperception that "all" normal DNS (at least all traffic except for zone transfers) happens "only" via UDP; that is an incorrect belief. Real DNS traffic (other than zone transfers) **can, may and will** actually use 53/TCP from time to time.
- Blocks on **all** 53/**UDP** may sometimes get installed because of concerns about spoofed traffic, or worries about the non-rate adaptive nature of UDP traffic in general, or simply by mistake.

(Less?) Crazy Tweaks to User DNS Traffic

- Because of the high cost of handling user support calls, some ISPs may attempt to avoid user support calls (and associated costs) by "managing" user DNS traffic.
- What does "managing" mean?
 - **blocking/dropping all** port 53 traffic, **except** to/from the DNS server(s) that the ISP provides for their customers (this will often be implemented via router or firewall filters)
 - **redirecting** all user DNS traffic that isn't destined for the ISP's customer DNS servers (e.g., redirecting DNS is something that's common enough that Cisco even includes redirecting DNS as an example for its Intelligent Services Gateway, see:
http://www.cisco.com/en/US/products/ps6566/products_configuration_guide_chapter09186a0080630d65.html#wp1048400)
 - **selectively redirecting user DNS traffic**, if it appears that the customer is infected (e.g., Simplicita's commercial DNS switch³⁶)

Just "For the Record..."

- I am generally **not** a big fan of **redirecting or rewriting all customer DNS traffic, or limiting users to just their provider's DNS servers** as a "solution." Why?
 - doing DNS filtering/redirection breaks Internet transparency in a very fundamental and bad way
 - if the provider's designated DNS servers end up having issues, DNS filtering/redirection substantially reduces customer options
 - port-based filtering/redirection can be surmounted by technically clued people thru use of non-standard ports for DNS
 - port-based filtering/redirection (or even deep packet inspection approaches) can be overcome by VPN-based approaches
 - some services (such as commercial DNSBLs) may be limited to just subscribing DNS servers; the DNS server that you redirect me through may not be allowed to access that data.
- I would encourage you to consider **passive DNS monitoring** as an alternative way of identifying systems which need attention.

What About Blocking ***JUST* Malicious DNS Servers** at the Network Level?

- Assume you succeed in identifying one or more malicious name servers being used by your users. Most security folks would then be inclined to do the "logical" thing and block access to those name servers. Good, right? You're protecting your users by blocking access to just those servers, eh? Well... *yes*, you are, but when you do so, when you block those malicious name servers, ALL name resolution for those infested users (crummy though it may be), will typically suddenly cease. "The Internet is down!"
- **Suggestion: IF you DO decide to block specific malicious DNS servers, and I CAN sympathize with the desire to do that, be SURE to notify your support staff so that they can add DNS checks to their customer troubleshooting processes.**

Note: You May End Up Blocking Bad DNS Servers W/O Knowing You're Doing That

- For example, assume you're using the Spamhaus DROP (Do Not Route or Peer list, see <http://www.spamhaus.org/DROP/>), an excellent resource you should all know about and consider using.
- Some of those DROP listings **may** happen to cover bad DNS servers which will no longer be reachable by infected clients once you begin using DROP.
- Thus, even though you may not be focused on blocking bad DNS servers, by filtering some prefixes at the network level, you may inadvertently end up filtering name servers your users may be using.
- Isn't this all just so much "fun?"

5. DNSSEC: What Is It?

DNSSEC "By the [RFC] Numbers"

- DNSSEC is defined by four RFCs (available online from <http://www.ietf.org/rfc.html>)
 - RFC4033, "DNS Security Introduction and Requirements,"
 - RFC4034, "Resource Records for the DNS Security Extensions,"
 - RFC4035, "Protocol Modifications for the DNS Security Extensions"
 - RFC5155, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence"

If you really want to know about DNSSEC, read those RFCs, plus also see:

- RFC3833, "A Threat Analysis of the Domain Name System"
- RFCs can make for rather dry reading, however, so let me just dive right in with my personal take on DNSSEC...

DNSSEC in a Nutshell

- DNSSEC uses public key asymmetric cryptography to guarantee that if a DNS resource record (such as an A record, or an MX record, or a PTR record) is received from a DNSSEC-signed zone, and checks out as valid on a local DNSSEC-enabled recursive name server, then we know:
 - it came from the authoritative source for that data
 - it has not been altered en route
 - if the server running the signed zone says that a particular host does not exist, you can believe that assertion
- But what about other things, like insuring that no one's sniffing your DNS traffic, or making sure that DNS service is always available?

DNSSEC Intentionally Focuses on Only One of The Three Traditional Information Security Objectives

- While there are three "C-I-A" information security objectives:
 - Information Confidentiality
 - Information Integrity, and
 - Information Availability

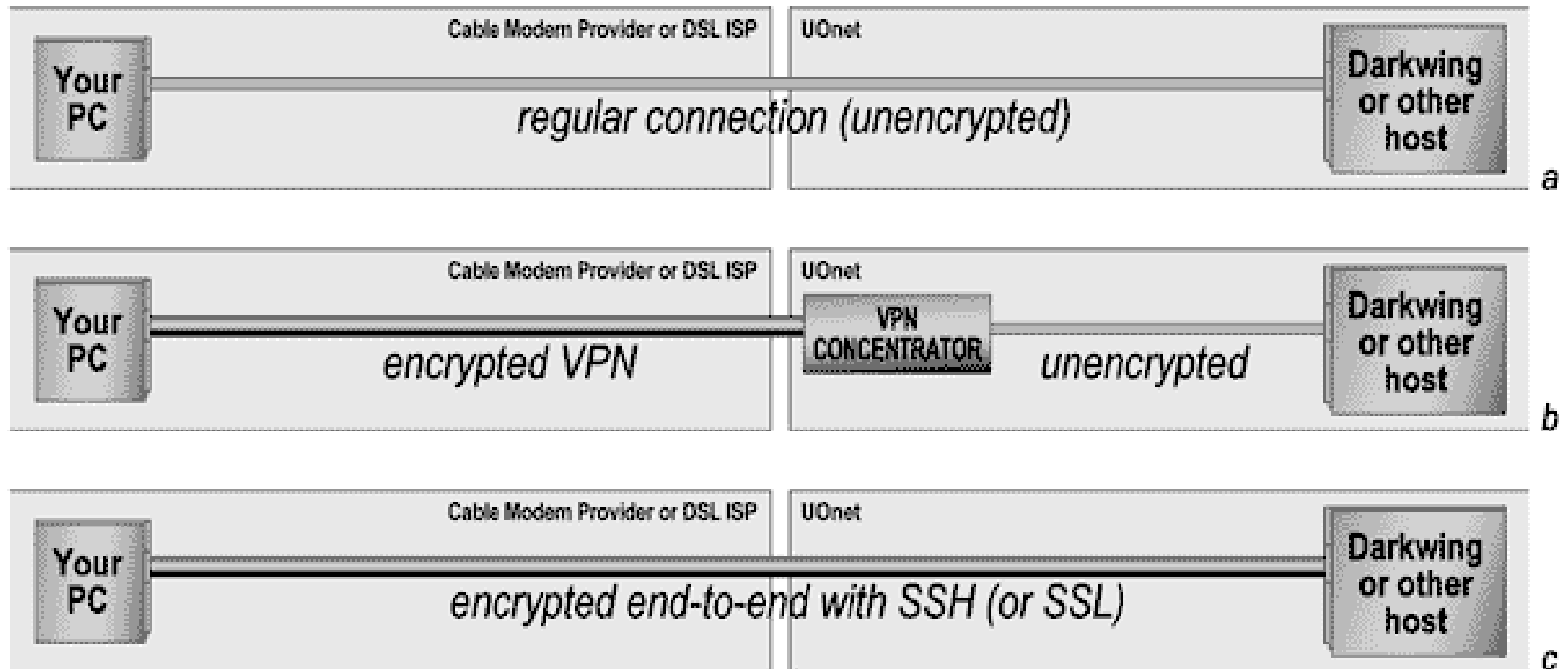
DNSSEC is intentionally **NOT** designed to keep DNS data confidential, and it is also intentionally **NOT** designed to improve the availability of DNS data -- it's sole focus is on insuring the **integrity** of DNS data.

- And, to the extent that DNSSEC is not an end-to-end protocol, its ability to even insure information integrity is less than perfect.

DNSSEC As A Non-"End-to-End" Protocol

- To understand the difference between an end-to-end protocol and one that works only along part of a complete path (e.g., to or from some intermediate point), consider the difference between using SSH and using a typical VPN.
- SSH secures traffic all the way from one system (such as your laptop) to the other system you're connecting to (perhaps a server running Linux) – it is "end-to-end."
- A VPN, however, may terminate on a hardware firewall or VPN concentrator, and from that point to the traffic's ultimate destination, traffic may travel unsecured. This is NON end-to-end.
- DNSSEC is more like the VPN example than the SSH example: **DNSSEC only secures traffic to the local recursive name server**, it typically cannot and will not secure traffic all the way down to the desktop. Thus, a bad guy can still attack DNS traffic that is in flight from the local recursive name server to the endhost.

Non-End-to-End and End-to-End Protocols



What About Using TSIG To Secure The Last Hop for DNSSEC?

- TSIG is defined by RFC2845, and was originally created to improve the security of zone transfers, and to provide a secure way by which trusted clients could dynamically update DNS.
- For the purpose of providing DNSSEC with last hop integrity, TSIG has a number of potential shortcomings, including:
 - it uses a form of symmetric cryptography, so all clients need to be given a copy of a shared secret key (yuck)
 - the only hashing mechanism defined for TSIG in the RFC is HMAC-MD5, which is no longer particularly robust
 - clocks need to be roughly in sync (user laptops or desktops often have system clocks which aren't very well synchronized)
- **The DNSSEC data validation check could be moved from the local recursive DNS server all the way down to the laptop or desktop itself, IF the DNS server running on the laptop or desktop knew how to do DNSSEC (but no such luck if you're running Windows)...**

DNSSEC [Non] Support in Microsoft Windows




[Steve Riley \[MSFT\]](#)8/21/2008 6:29 PM PST

No, DNSSEC isn't supported in any version of Windows.

--
Steve Riley
steve.riley@microsoft.com
<http://blogs.technet.com/steriley>
<http://www.protectyourwindowsnetwork.com>

"totojepast" <totojepast@razdva.cz> wrote in message
news:4cdf919f-4cba-4940-aead-fb1d460c0fbe@k13g2000hse.googlegroups.com...
> Is the Windows XP DNS resolver able to check the validity of the DNS
> data using DNSSEC? Is this feature turned on by default?
>
> And does the Windows Server support DNSSEC for publishing the public
> DNS records?

Was this post helpful to you?

 Reply |   Top

[Steve Riley \[MSFT\]](#)8/21/2008 6:42 PM PST

“Is DNSSEC supported by Windows? in General Security Discussion”

<http://www.microsoft.com/communities/newsgroups/en-us/default.aspx?dg=microsoft.public.security&tid=b79048c0-9ede-41a4-9976-8d0df53749be&mid=0a907a01-2dc6-4a22-b075-f2de8c4bbaba&cat=&lang=&cr=&sloc=&p=6>

The Document Mentioned On The Preceding Slide

- Quoting from
<http://technet.microsoft.com/en-us/library/cc728328.aspx>

"Client support for DNSSEC

"The DNS client does not read and store a key for the trusted zone and, consequently, it does not perform any cryptography, authentication, or verification. When a resolver initiates a DNS query and the response contains DNSSEC resource records, programs running on the DNS client will return these records and cache them in the same manner as any other resource records. This is the extent to which Windows XP DNS clients support DNSSEC. When the DNS client receives the SIG RR relating to the RRset, it will not perform an additional query to obtain the associated KEY record or any other DNSSEC records."

Loomis, Gilbert R. [GILBERT.R.LOOMIS at saic.com](mailto:GILBERT.R.LOOMIS@saic.com)

Thu Sep 4 16:30:24 UTC 2008

- Previous message: [\[dns-operations\] Google Chrome Pre-Caching](#)
- Next message: [\[dns-operations\] DNSSEC support in Microsoft Windows products](#)
- Messages sorted by: [\[date\]](#) [\[thread\]](#) [\[subject\]](#) [\[author\]](#)

For clarity, and definitely not speaking for Microsoft,
but only based on the publically available info that
I have--here's the statement of "best estimate" status
that I put together for an interested customer:

=====

Microsoft had previously indicated that DNSSEC
per RFC 4035 would be present in "SP1 for Longhorn
Server"

<https://www.dns-oarc.net/files/workshop-2006/Microsoft-DNSSEC.pdf>
but WS2008 was labeled as SP1 upon release to
match up with Vista SP1 which RTM'd at the same
time. Based on current TechNet docs, WS2008 SP1
does not appear to support DNSSEC validation
other than the minimal support for serving RFC2535
records (but doing no actual validation or signing)
that was present in WS2003.

<http://technet.microsoft.com/en-us/library/cc753802.aspx>

That implies that SP2 for WS08, expected out sometime
in 2009, will be required for DNSSEC support--and
even then, RFC4035 will only be supported on servers
that have been updated to WS08 and *perhaps* on Vista
clients. Many, if not most, organizations with
existing DNS Servers running Microsoft are still
using Windows Server 2003. And for US Federal
Government users, all these transitions must be
managed and completed by December 2009.

Note that even RFC4035 support may not suffice for
some DNS operators, if NSEC3/Opt-Out turn out to
be (believed as) necessary due to zone size or
constraints on data publishing.

=====

Rip Loomis, CISSP, PMP
Chief Systems Security Engineer
SAIC Cyber Security Solutions
www.saic.com/infosec/

This Is The Memo Referred To On the Previous Slide Says dot gov Will Be Signed by Jan 2009; Agencies Have Until Dec 2009 to Get Signed

New Policy

This memorandum addresses two important issues in following through with the existing policy and expanding its scope to address all USG information systems.

- A. The Federal Government will deploy DNSSEC to the top level .gov domain by January 2009. The top level .gov domain includes the registrar, registry, and DNS server operations. This policy requires that the top level .gov domain will be DNSSEC signed and processes to enable secure delegated sub-domains will be developed. Signing the top level .gov domain is a critical procedure necessary for broad deployment of DNSSEC, increases the utility of DNSSEC, and simplifies lower level deployment by agencies.
- B. Your agency must now develop a plan of action and milestones for the deployment of DNSSEC to all applicable information systems. Appropriate DNSSEC capabilities must

<http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf>

August 22nd, 2008

What Would a User See If a DNS Resource Record Failed DNSSEC Validation?

- **Answer: nothing.** Users would see nothing that would indicate a DNSSEC validation failure had occurred. Such a failure is normally "silent" and indistinguishable (to the user) from many other types of DNS failures. It is probably just me, but I've got mixed feelings about DNSSEC validation failures being opaque to users. Instinctively, we know that DNSSEC validation might fail due to:
 - operational error: it would be good to make sure that's noticed and corrected, and users could act as "canaries in the coal mine"
 - an active attack; it would be REALLY good to know that's happening!
 - something completely unrelated to DNSSEC might be busted
- Silent failure modes that confound several possible issues just strike me as a bad idea.

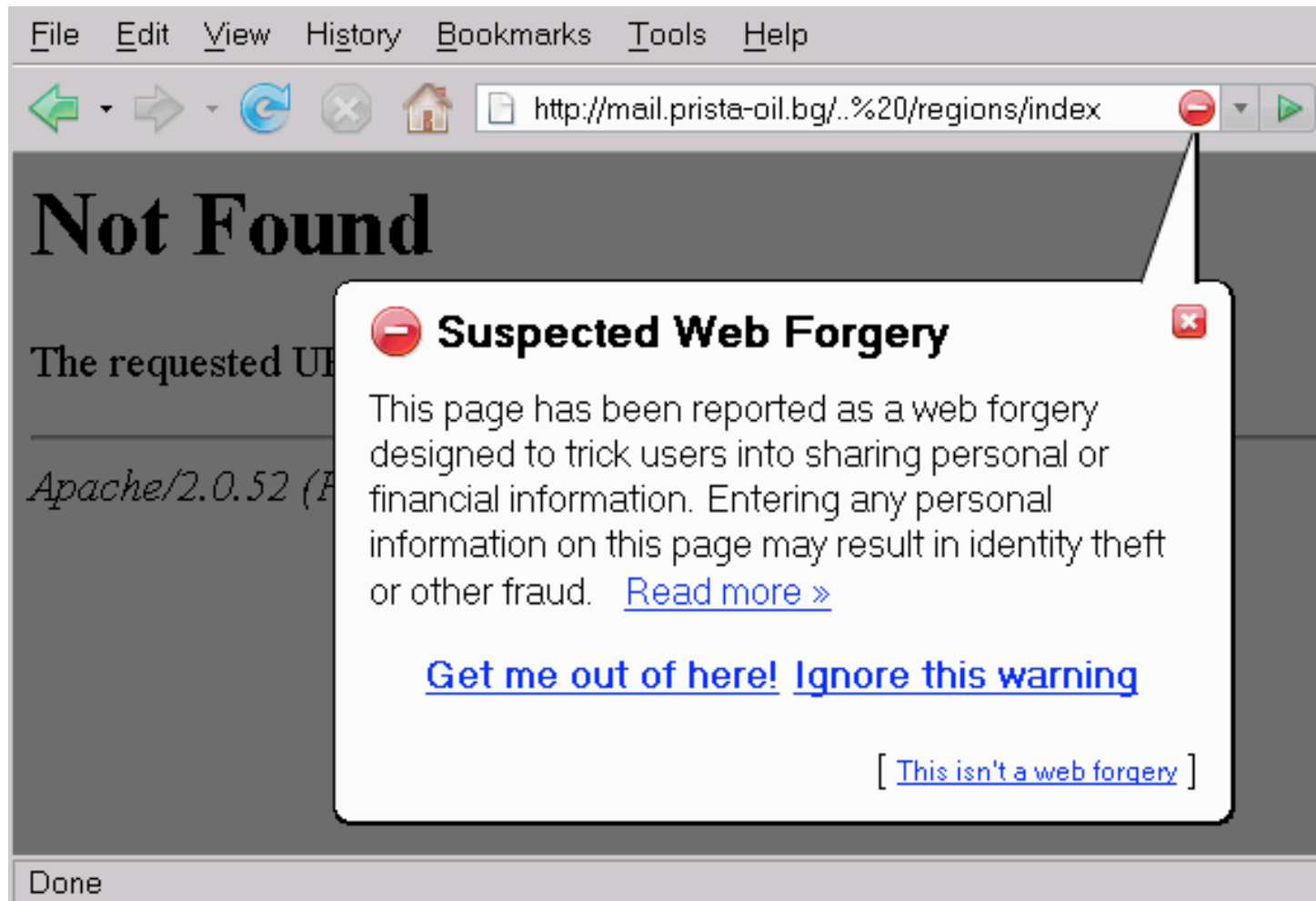
What Does a User See When A DNSSEC-Signed Record Is Cryptographically Valid?

- **Answer: nothing.** When a DNSSEC-signed record is cryptographically valid, users ALSO sees NOTHING at all.
- If DNSSEC "just works" (except for when it silently breaks when people attempt to do bad things), will people even **know** they're receiving a benefit from it?
- DNSSEC **needs** application layer visibility!
- DNSSEC should have something kin to the little padlock icon for SSL encrypted secure web sessions (for when DNS records have valid DNSSEC signatures) OR something that's FAR more "in your face" and visible when shenanigans are occurring, kin to what Firefox shows when a phishing site is detected...

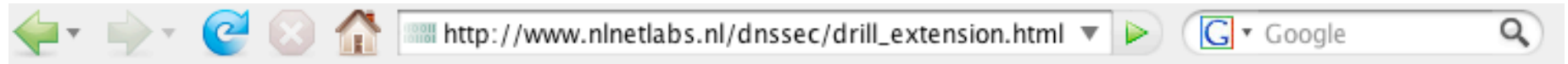
What Would A User See If a DNS Administrator “Screws Up” A DNSSEC Implementation?

- **Answer: nothing.** And this time, we really mean “nothing.”
- For example, if an administrator fails to keep keys current, a zone using a new key might not be recognized as valid, and then that zone wouldn’t be used, thereby breaking access to all the systems using names from the zone at that site.
- Similarly, if an administrator mis-signs a zone or makes even the slightest modification to a signed zone, that zone will fail to validate, and again, the DNS information from that mis-signed or broken zone won’t be usable.
- Obviously there is some asymmetry in the potentially visible costs and benefits associated with DNSSEC.

What A Firefox User Sees By Default When Attempting to Visit A Phishing Site



Drill Extension For Firefox



Drill Extension

This extension performs DNSSEC lookups for the main hostname of the current page in firefox. It uses [Drill](#) to chase the signatures up to a trusted key. The user can specify trusted keys by putting them in a directory of his choice (see usage).

If you run it now, you'll get insecure on almost all websites, because since the DNS root is not signed, there is no way to verify that a result is verifiably insecure.

Download

The current release is 0.7, get it here: [drill-0.7.xpi](#).

Don't forget to install drill, from the [ldns library](#). It needs that to do the actual verification.

Usage

After installing the extension, the statusbar shows a new icon: normally, for unverified pages, the icon will be:



If the hostname record in the DNS is signed and can be traced up to a trusted key, the icon will look like this:



By clicking on preferences in the extension menu, or just clicking on the icon, you will get to the preferences dialog:

Another Issue: The DNSSEC Trust Model

- Talking about phishing makes me think about trust models.
- Trust models focus on the question of, "Why should I believe you're really you?" "Why should I accept 'your' credentials as being authentic?" This is a pivotal question in cryptography.
- Some crypto protocols, such as GPG/PGP, are decentralized, and employ a "web-of-trust" trust model where I trust your public key because it has been signed by other keys which I recognize/trust.
- Other crypto protocols, such as PKI, are more centralized or "top down." In the PKI model, I trust a particular PKI certificate because it has been signed by a trusted certificate authority ("CA")
- **DNSSEC was originally intended to use a centralized top-down trust model, with a signed root.** The trusted signed root would then sign immediately subordinate TLDs; those TLDs would sign second level domains immediately below them, etc.
- **One slight problem: the root still hasn't been signed.**

Signing The Root (".")

- From the DNS Root Server System Advisory Committee meeting, in Vancouver, Dec 2nd, 2007 (see www.icann.org/en/committees/dns-root/)

“DNSSEC update: (Richard Lamb) have an implementation that is ready for deployment. running since July 2007. now backing up keys to alternate site. It is expected to be used for .arpa ... a backup system is now in place. ICANN is wanting SLA's for the .arpa servers - contracts with the operators. There is ongoing work doing risk assessment for the root zone administration. Documentation, writing an operations manual for root zone signing process and procedures. Currently waiting on secondary selection for signed root zone publication. The demo system answers on v4/v6 on port 53 - much traffic from NLnet. RSSAC expressed a strong concern that this demo may become entrenched as an alternate root system. Questions about what is being tested are raised. It is not the service delivery. Is it key generation? Zone publication? or end-system/client use of the signed data? A recommendation to periodically turn off the demo system for 2xTTL plus a few hours as well as forcing key compromise might be useful. That ICANN is actively looking for contractual secondaries for root and arpa, as different than the existing roots is a fundamental change to the existing relations with 8 the operators. Richard will work with the IANA staff and come back to the RSSAC list within the week on what types of questions/experiments to ask/work on.

Signing The Root (".") (cont.)

- [continuing from previous slide]

“DNSSEC deployment: (Russ Mundy) few inputs to DNSSEC deployment and SSAC since last meeting. se. inputs from "small boxes" - some % of these DSL boxes would just kill DNS queries if the data was signed. **also - how ssac should/should not make comments about DNSSEC in public. no formal statement from ssac on dnssec. now may not be the right time.** [emphasis added]

“future issues: algorithm rollover considerations. also, islands and Trust Anchor Mgmt. how are TAs to be managed. a suggestion to look to the minutes of the last RIPE mtg - the TA-repository work might be useful. also - should recommend to TLDs to sign their zones as soon as possible. parallel heirarchies are difficult to maintain”



28 January 2008

SAC 026: SSAC Statement to ICANN and Community on Deployment of DNSSEC

SSAC notes the DNSSEC deployment efforts of ICANN and the community at large and encourages continued efforts to improve the security of the domain name system. We recognize that any technology deployment on a global scale is apt to reveal issues not considered in protocol design and development and in controlled (test) environments. SSAC notes that several such issues have been exposed with respect to DNSSEC¹ and recommends the following actions.

1. As manager of the IANA function, ICANN should continue its efforts to support and

<http://www.icann.org/en/committees/security/sac026.pdf>

NTIA Notice of Inquiry: "Enhancing the Security and Stability of the Internet's Domain Name and Addressing System," October 9th

- <http://edocket.access.gpo.gov/2008/E8-23974.htm>

SUMMARY: The Department of Commerce (Department) notes the increase in interest among government, technology experts and industry representatives regarding the deployment of Domain Name and Addressing System Security Extensions (DNSSEC) at the root zone level. The Department remains committed to preserving the security and stability of the DNS and is exploring the implementation of DNSSEC in the DNS hierarchy, including at the authoritative root zone level. *Accordingly, the Department is issuing this notice to invite comments regarding DNSSEC implementation at the root zone.*

DATES: Comments are due on November 24, 2008



(DEMO) DNSSEC STATUS



To test using this demo (nameserver ns.iana.org) refer to the sample BIND configuration file [here](#).

Note: This data, including the signed zones, are purely for test purposes and are not to be used in any production capacity. We do not guarantee their availability, and they may not otherwise function from time-to-time.

ZONE (serial)	STATE / LAST UPDATED	VALIDITY PERIODS (keyid)	EFFECTIVITY PERIODS (keyid)	TRUST ANCHORS
root (2008101940)	Ok 2008-OCT-19 16:25:49	2008-OCT-01 2008-NOV-15 (04183 KSK) 2008-OCT-01 2008-NOV-15 (34291 KSK) 2008-OCT-19 2008-OCT-25 (42651 ZSK)	2007-JAN-01 2008-DEC-31 (04183 KSK) 2008-JAN-01 2009-DEC-31 (34291 KSK) 2008-OCT-01 2008-NOV-15 (42651 ZSK)	<pre> -----BEGIN PGP SIGNED MESSAGE----- Hash: SHA1 \$ORIGIN . @ 1 IN DNSKEY 257 3 5 (AwEAAbWmiPoQlFp+snq84lbEPx2kPgessP91 ieS+jeabIsxi9tE9MCbEeCrRqPtKT1p50l+C 0cvapYFAsg8VhyDIMiTpYw8KHTgh267GciKf VxxRRZy68ndKRHC/bq8zqD4cYxVdJofTbIAM bxdX8OdYwtJ7ZFS7B14aSSQ/1y/8stX+l3oA PgSbcIhjCMKzHOLoR9npD6gGJpUud5zoyG1+ GkVvuD7XPQpzmQ08KAYmZ7/Nh2MmJHzfWp4L glqT4cdCT/S8YtDE46I9+vDGLhknHIyEyI5m P9kZWXZa58wWbv9ZBTzN0PNPWOHfPw045wU AqrRagTbRs7sWw/fpKgC5I0=) ; key id = 4183 1 IN DNSKEY 257 3 5 (AwEAAff8EiNa/S3wovNzPUMuBqelPsJnNoen cXDNMpmjTgngGMPct+8KDKxM6FwvPSRx15gN RyRQfzSPU0WshDNkBV2TmtVpzqn/dsurbmTo ixRzLyLK2Kd2adg5o5yS/gaTgCo0HVBmIruS N3FVI2ugCWJBFLkFGHLvMJ0BTSYVqWGWQIzp EPKCbKN+L9nrLcvJRCWG59Yq6BusSEKlZSK3 jMhYQs6y5iICGAVol+3VyjN93/1XkeUG6u7d lQsyiy9fxfeUvmn004y0TjAgjZqdwKZB0K9M A7qcALG3Tw2TXEdQsn9aY3DzNii3YEBidzER mY7n4hIUrilr59MnuNJq2x0=) ; key id = 34291 -----BEGIN PGP SIGNATURE----- Version: GnuPG v1.4.7 (GNU/Linux) iD8DBQFI43hf0a+84A9skdIRArYlAKCBnlthRm3pUtu4CcC2XWkhoD5y/ACfTSgz ofKrGcPD4l42CHUmDJfDnnc= =V5Pt -----END PGP SIGNATURE----- </pre>

[DS Records](#)

What About The TLDs? Are The TLDs At Least Signed and Supporting DNSSEC?

- A very limited number are, including .se (Sweden), .bg (Bulgaria), .pr (Puerto Rico), cz (Czech Republic), .br (Brasil) and .museum. For example:




```
% dig +dnssec +bufsize=4096 se @catcher-in-the-rye.nic.se  
[snip]
```

```
:: AUTHORITY SECTION:
```

```
se.          7200  IN      SOA    catcher-in-the-rye.nic.se. [etc]  
se.          7200  IN      TYPE46 \# 150      0006050[etc]  
se.          7200  IN      TYPE47 \# 17       03302D3[etc]  
se.          7200  IN      TYPE46 \# 150      002F050[etc]
```

- Most other TLDs (including .edu, .com, .net, .ca, .cn, .de, .fr, .jp, .uk, etc.) are **neither** signed nor supporting the use of DNSSEC at this time. This does not prevent domains **under** those TLDs from doing DNSSEC, but when a domain under one of those TLDs does do DNSSEC, they exist as an "island of trust."


Folks Are Working To Get Additional ccTLD's Signed

<http://ws.edu.isoc.org/workshops/2008/cctld-ams/> Google

Advanced ccTLD & DNSSEC Workshop

The ISOC-sponsored Advanced ccTLD workshop series is aimed at ccTLD operators who have either already attended the initial ccTLD Workshop series, or for ccTLD operators who are at an operational level where they would benefit from the topics presented in this workshop.

Local Host



Instructors

Jaap Akkerhuis (NLnet Labs)	Daniel Karrenberg (RIPE NCC)
Hervey Allen (NSRC)	Olaf Kolkman (NLnet Labs)
John Crain (ICANN)	Duane Wessels (DNS-OARC)

Organizers

Mirjam Kühne (ISOC)	Martin Kupres (ISOC)
Steve Huter (NSRC)	

Agenda

Advanced ccTLD Workshop Attendee List

Attendees:

Adriatik Allamani	AL (Albania)
Barjon Rama	AL (Albania)
Luis León Cárdenas Graide	CL (Chile)
Cristián Rojas	CL (Chile)
Elena Grimany	CU (Cuba)
Ayitey Bulley	GH (Ghana)
Godfred Ofori-Som	GH (Ghana)
Nicholas Wambugu	KE (Kenya)
Dr. Paulos B. Nyirenda	MW (Malawi)
Eswari Prasad Sharma	NP (Nepal)
Rakeshman Karmacharya	NP (Nepal)
Cesar Rodas	PY (Paraguay)
Daniel Brassel	PY (Paraguay)
Medard BASSENE	SN (Sénégal)
Khalil Rakhmanov	TJ (Tajikistan)
Wafa Dahmani	TN (Tunisia)
Atef LOUKIL	TN (Tunisia)

A gTLD DNSSEC Shining Star: Dot Org



Islands Of Trust

- Remember, DNSSEC was designed to work using a **centralized, top-down trust model**. If the root isn't signed, all the stuff under the root must establish **alternative trust anchors**. In some cases (such as .se), the trust anchor may be the TLD, but in other cases, the trust anchor may be 2nd-level domain (such as nanog.org).
- Because there is **no central trust anchor**, unless you can come up with an alternative way of establishing a chain of trust, **you must obtain trustworthy keys for each of those individual islands of trust**. (Key management is the 2nd thing, after trust models, to always scrutinize when considering about a crypto effort!)
- If each site that wants to do DNSSEC has to do a "scavenger hunt" for each island of trust's DNSSEC keys, that's **rather inconvenient** particularly if (1) trust islands periodically **rekey**, (2) there are **thousands** of domains, and (3) given that if a site **fails** to keep each trust island's keys current, any data served by that trust island with their new key will be mistakenly viewed as bogus and get dropped.⁶⁶

“It Is Not Trivial to Find and Maintain Trust Anchors”



1.4 Finding trust-anchors

It is not trivial to find and maintain trust anchors. If you want to get started with validation of DNSSEC here are a few places where you can find more information.

- RIPE NCC maintains a set of keys on their secured website under <https://www.ripe.net/projects/dnssec/keys/index.html> (Note that this is a secured website, check the certificate).

http://www.mozilla.org/projects/security/pki/nss/ref/ssl/sslerr.html		
SEC_ERROR_OCSP_INVALID_SIGNING_CERT	-8048	"Invalid OCSP signing certificate in OCSP response."
	-8047	"Certificate is revoked in issuer's

DLV

- To avoid these problems, ISC has proposed DLV (Domain Lookaside Validation) as a temporary/transitional model.
- In the DLV model, even if the root or a TLD isn't ready to support DNSSEC and sign its zone, perhaps a trusted third party can collect, authenticate and deliver the required keys. Someone attempting to do DNSSEC then has only to configure the DLV server or servers as an anchor of trust, thereafter automatically trusting domains that are anchored/validated via the DLV.
- DLV is described at <http://www.isc.org/pubs/tn/isc-tn-2006-1.html> and in <http://www.ietf.org/rfc/rfc4431.txt>
- DLV is supported in current versions of BIND
- One sample DLV registry: <http://www.isc.org/index.pl?/ops/dlv/> (and there may/will be others).
- Obviously, assuming you need to trust the data that a DLV registry secures, you will want to be extremely careful when adding trusted DLV registries. (I'm quite comfortable trusting ISC's registry)

What About the In-Addr Zones?

- In addition to the root and the TLDs, the rDNS ("inverse-address") zones would also be a top priority for DNSSEC signing.
- In-addrs are queried when you have a dotted quad, and you want to find the associated fully qualified domain name.
- RIPE has signed the in-addrs that it is responsible for, however other registries (such as ARIN, APNIC, LACNIC, etc.) have yet to do the same for the in-addr zones they control.
- It would be great to see progress in that area, along with getting the root and the major TLDs signed.

The Zone Enumeration Issue And NSEC3

- As originally fielded, DNSSEC made it possible to exhaustively enumerate, or "walk," a zone, discovering all known hosts. An example of such a tool is Zonewalker, <http://josefsson.org/walker/>
- Zone enumeration gives miscreants a real "boost up" when it comes to reconnoitering a domain, and this was a real problem for some TLDs in countries with strong privacy protections.
- NSEC3 (see RFC5155, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence") addresses the zone enumeration issue through use of salted hashes, which handles both that concern as well as the problem that "the cost to cryptographically secure delegations to unsigned zones is high for large delegation-centric zones and zones where insecure delegations will be updated rapidly."
- For our purposes, it is sufficient to know that NSEC3 effectively eliminates the zone enumeration problem.

Are Name Servers (the Software Programs) DNSSEC-Ready?

- Another potential stumbling block might be the name server software. If the name server software you use doesn't support DNSSEC, your ability to do DNSSEC will obviously be limited.
- An excellent summary of DNSSEC capabilities by name server product is available at <http://www.icann.org/en/committees/security/sac030.htm> but let's just walk through this a bit from other sources, too...
- First, what name server products do people run?

BIND Dominates The DNS Server Market

- <http://dns.measurement-factory.com/surveys/200710.html> ...

BIND 9	201,723	64.53%
BIND 8	45,547	5.63%
BIND 4	1,387	0.22% (70.38% total)
Embedded Linux	51,720	19.29%
Microsoft Windows DNS 2000	11,548	1.80%
Microsoft Windows DNS 2003	3,246	0.84%
Microsoft Windows DNS NT4	868	0.10% (2.74% total)
PowerDNS	14,448	6.59%
Other (including Cisco CNR)	1,623	1.00%

["199,820 additional nameservers could not be identified"]

The Good News:

Current Versions of BIND Support DNSSEC

- The good news for folks interested in deploying DNSSEC is that the current version of BIND supports DNSSEC, and BIND has the lion's share of the current DNS server market, as shown by the table on the proceeding page.
- I must admit that I am a little disconcerted to see ancient versions of BIND still in use – are people REALLY running BIND 4 or BIND 8? You really don't want to be running ancient versions of **anything** on systems exposed to the Internet these days! Job one is to get current! (Please remember the starting slides of this talk, talking about the Kaminsky vulnerability!)

What About Microsoft's DNS Servers?


- Quoting <http://technet.microsoft.com/en-us/library/cc728328.aspx> (updated January 21st, 2005) [emphasis added]:

"Windows Server 2003 DNS provides basic support of the DNS Security Extensions (DNSSEC) protocol as defined in RFC 2535." *[however, note that RFC2535 dated March 1999, was made obsolete by RFC4033, RFC4034, and RFC4035 ca. March 2005]*

"The current feature support allows DNS servers to perform as secondary DNS servers for existing DNSSEC-compliant, secure zones. DNS supports the storing and loading of the DNSSEC-specific resource records (RRs). **Currently, a DNS server is not capable of signing zones and resource records (creating cryptographic digital signatures) or validating the SIG RRs.** The DNSSEC resource records are KEY, SIG, and NXT." [the March 2005 RFC's deprecated those earlier DNSSEC record types]

The Most Recent News From MS on DNSSEC Support in Windows Server

Mr.T7 - Posted on Thu Sep 11 12:25:16 2008

 Reply  Quote  Post already rated

Windows Server 2008 does not fully support DNSSEC (reference RFCs 4033, 4034 and 4035).

Microsoft will implement the Domain Name System Security Extensions (DNSSEC) as specified in RFCs 4033, 4034 and 4035 to allow federal agencies to comply with the SC-20 and SC-21 security controls proposed in NIST 800-53 in the next release of Windows Server and client operating systems. Microsoft's DNSSEC support will allow agencies to satisfy requirements outlined in the [memorandum](#) issued by the Office of Management and Budget (OMB).

Regards,

Tim

Microsoft Consulting Services

Mr.T

- Source: <http://social.technet.microsoft.com/forums/en-US/winserversecurity/thread/59db10cf-8561-464e-8ab0-2e60c0ec90aa/>

Coming Back to Our Tour of DNS Software

Support for DNSSEC: How About PowerDNS?

- <http://doc.powerdns.com/types.html> describes the record types supported by PowerDNS; while the DNSSEC records are “fully supported,” DNSSEC processing is not performed on them.

See, for example, the entry for RRSIG:

RRSIG (since 2.9.21)

The RRSIG DNSSEC record type is fully supported, as described in RFC 3757. Note that while PowerDNS can store, retrieve and serve DNSSEC records, no further DNSSEC processing is performed.

What About The Large Number of "Unidentified" Name Servers?

- In some cases those may be sites running one of the mentioned products, but they may have disabled version strings and/or taken other steps to limit the ability of potential miscreants to successfully "fingerprint" the name server software running on their servers.
- In other cases, however, sites may be running an alternative DNS implementation, such as D. J. Bernstein's **DJBDNS** (aka TinyDNS), see <http://cr.yp.to/djbdns.html> or <http://tinydns.org/>
- If you're considering doing DNSSEC and you're currently using those products, you should note that the author of those products explicitly does NOT support DNSSEC in DJBDNS, and to the best of my knowledge has no plans to change that stance. You can see his discussion and rationale for this at <http://cr.yp.to/djbdns/blurp/security.html> and at <http://cr.yp.to/djbdns/forgery.html>

What About The "Embedded Linux" Name Servers Which Were Mentioned in The Survey of DNS Software Usage?

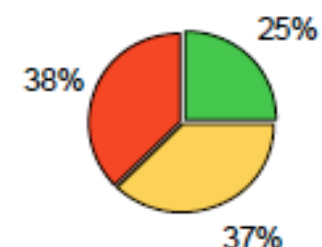
- Embedded Linux is a stripped down version of Linux that's often run on hardware network appliances, including at least some DSL or cable modems, and some "firewall"/"broadband router" devices.
- Based on the survey numbers, I believe at least some those hardware network devices offer DNS service as well as other functions.
- **Folks have begun to look at how DNSSEC might interact with those home hardware firewall class devices; the news is not universally wonderful.**

<http://download.nominet.org.uk/dnssec-cpe/DNSSEC-CPE-Report.pdf>

			Out of the Box Usage Mode	Route DNS to Upstream Resolver	Proxy DNS over UDP	A. EDNS0 Compatibility	B. Signed Domain Compatibility	E. Request Flag Compatibility	D. Checking Disabled Compatibility	C. DNSSEC OK Compatibility	Proxy DNS over TCP
1	2Wire	270HG-DHCP	Proxy	OK	OK	FAIL	OK	OK	FAIL	FAIL	FAIL
2	Actiontec	MI424-WR	Proxy	OK	OK	FAIL > 512	OK	OK	OK	OK	FAIL
3	Apple	Airport Express	Proxy	OK	OK	FAIL > 512	OK	FAIL	FAIL	FAIL	OK
4	Belkin	N (F5D8233)	Proxy	OK	OK	FAIL > 1500	OK	OK	OK	OK	FAIL
5	Belkin	N1 (F5D8631)	Proxy	OK	OK	FAIL > 1500	OK	OK	OK	OK	FAIL
6	Cisco	c871	Route	OK	OK	FAIL > 512	OK*	OK*	OK*	OK*	FAIL
7	D-Link	DI-604	Proxy	MIX	OK	FAIL > 1472	OK	OK	OK	OK	FAIL
8	D-Link	DIR-655	Proxy	OK	OK	OK	OK	OK	OK	OK	FAIL
9	Draytek	Vigor 2700	Proxy	OK	OK	FAIL > 1464	OK	FAIL	FAIL	OK	FAIL
10	Juniper	SSG-5	Route	OK	OK	OK	OK	OK	OK	OK	FAIL
11	Linksys	BEFSR41	Varies	OK	OK	FAIL > 1472	OK	OK	OK	OK	FAIL
12	Linksys	WAG200G	Varies	OK	OK	OK	OK	OK	OK	OK	FAIL
13	Linksys	WAG54GS	Varies	OK	OK	OK	OK	OK	OK	OK	FAIL
14	Linksys	WRT150N	Varies	OK	OK	FAIL > 512	OK	OK	OK	OK	FAIL
15	Linksys	WRT54G	Varies	OK	OK	FAIL > 512	OK	OK	OK	OK	FAIL
16	Netgear	DC834C	Proxy	OK	OK	FAIL > 512	OK	FAIL	FAIL	MIX	FAIL

- All 24 units could **route** DNSSEC queries addressed to upstream resolvers (referred to herein as route mode) without size limitations.
- 22 units could **proxy** DNS queries addressed directly to them (referred to herein as proxy mode), with varying degrees of success.
- 6 of 22 DNS proxies had difficulty with DNSSEC-related flags and/or validated responses that effectively prevented DNSSEC use in proxy mode.
- 16 of 22 DNS proxies could successfully pass DNSSEC queries and return validated responses of some size.
- 18 DNS proxies limited responses over UDP to either 512 bytes or a size constrained by the MTU. Only 4 could return responses over UDP up to 4096 bytes, while just 1 could proxy DNS over TCP (no size limit). Such limits can interfere with returning longer DNSSEC responses.
- When deployed with factory defaults, 15 units are likely to be used as DNS proxies, while 3 always route DNS queries. The rest (6) vary over time, preferring to route DNS after being connected to a WAN.

As a consequence, we conclude that just 6 units (25%) operate with full DNSSEC compatibility "out of the box." 9 units (37%) can be reconfigured to bypass DNS proxy incompatibilities. Unfortunately, the rest (38%) lack reconfigurable DHCP DNS parameters, making it harder for LAN clients to bypass their interference with DNSSEC use.



“What’s That EDNS0 Thing They Mentioned?”

- While we're on the topic of network hardware devices, you should know that name servers doing DNSSEC requires a feature known as EDNS0, as defined in RFC2671, "Extension Mechanisms for DNS (EDNS0)," August 1999.
- Normally, DNS UDP responses are limited to just 512 bytes, a size that's too small for the much larger DNSSEC records. To better handle delivery of DNSSEC records, EDNS0 allows clients and servers to negotiate the maximum size datagram which can be handled, with the expectation that at least some hosts might negotiate datagram sizes as high as 4KB. Name servers doing DNSSEC must do EDNS0.
- Why's that a problem? Well, as shown on the preceding page, some firewalls or broadband “routers” may block UDP DNS traffic > 512 bytes.

6. So Why Aren't People Using DNSSEC?

Deployment of DNSSEC to Date? NIL

- "The first version (RFC 2535, March 1999) defines the KEY, SIG, and NXT record types. The second version (RFC 4035, March 2005) essentially obsoletes the first-generation RR types and adds four new ones: DNSKEY, NSEC, RRSIG, and DS. We queried the set of nameservers for both old and new RR types. Among the **2,053,150** zones with at least one working nameserver, we found **36 (0.0018%) with first-generation DNSSEC records**. We also found **8 zones publishing second-generation DNSSEC records**. There is no overlap between the two first- and second-generation subsets. Needless to say, DNSSEC adoption is still very small. Unfortunately, our use of the COM and NET zones probably under-represents DNSSEC adoption across the whole Internet. Some European CCTLDs have been more proactive in encouraging the use of DNSSEC." [emphasis added]
- <http://dns.measurement-factory.com/surveys/200710.html>

Another View of DNSSEC Penetration: UCLA's SecSpider

- SecSpider: The DNSSEC Monitoring Project
<http://secspider.cs.ucla.edu/> reports (as of Sunday, October 19th, 2008) that it knows about just 1675 production DNSSEC-enabled zones (and please note that many of those zones are NOT what might be considered “major” or “widely recognized” zones)
- See also <http://public.oarci.net/files/workshop-2006/Osterweil-SecSpider.pdf> ...

"From our web crawl (of 18M zones), we estimate that the deployment status of DNSSEC is roughly 0.0015% "

An Opportunity for Schools in North Dakota: You Could Be The First .edu To Sign Your Entire Domain (Not Just a Subdomain)

DNSSEC Zone stats				
http://secpider.cs.ucla.edu/zone-dat-prod11.html				
zenteris.de.	Fri Aug 17 14:00:20 2007 UTC	Sat Oct 18 02:59:14 2008 UTC	Yes	Yes
dnssec.netsec.colostate.edu.	Fri Oct 3 16:56:29 2008 UTC	Fri Oct 3 16:56:29 2008 UTC	No	No
b.dnssec.netsec.colostate.edu.	Tue Sep 30 07:53:22 2008 UTC	Thu Oct 9 08:05:40 2008 UTC	No	No
n.dnssec.netsec.colostate.edu.	Tue Sep 30 18:09:46 2008 UTC	Fri Oct 3 18:20:47 2008 UTC	No	No
bind.dnst.netsec.colostate.edu.	Tue Sep 16 17:02:19 2008 UTC	Thu Oct 16 09:02:05 2008 UTC	Yes	Yes
ai.mit.edu.	Wed Jan 30 08:25:45 2008 UTC	Thu Oct 16 08:25:19 2008 UTC	Yes	Yes
csail.mit.edu.	Thu Oct 18 09:11:15 2007 UTC	Thu Oct 16 17:44:17 2008 UTC	Yes	Yes
lcs.mit.edu.	Mon Nov 5 10:36:29 2007 UTC	Thu Oct 16 20:28:17 2008 UTC	Yes	Yes
chrr.ohio-state.edu.	Thu Aug 7 17:16:02 2008 UTC	Thu Oct 16 17:33:40 2008 UTC	Yes	Yes
secpider.cs.ucla.edu.	Sat Mar 8 16:30:18 2008 UTC	Fri Oct 17 14:06:48 2008 UTC	Yes	Yes
pixaco.es.	Tue Dec 19 11:35:40 2006 UTC	Fri Oct 17 13:28:06 2008 UTC	Yes	Yes

Or, If You're a K12, You Could Be The First K12 To Sign Your k12.nd.us Domain

DNSSEC Zone stats				
http://secspider.cs.ucla.edu/zone-dat-prod20.html				
filebase.org.uk.	Wed Sep 17 02:02:18 2008 UTC	Thu Oct 16 18:47:07 2008 UTC	Yes	Yes
asclepion.us.	Tue Dec 19 10:04:13 2006 UTC	Thu Oct 16 08:38:05 2008 UTC	Yes	Yes
dento.us.	Tue Dec 19 15:15:33 2006 UTC	Sun Sep 28 17:50:54 2008 UTC	No	No
donteat.us.	Sat Aug 2 06:19:23 2008 UTC	Thu Oct 16 18:15:05 2008 UTC	Yes	Yes
cc.gt.atl.ga.us.	Mon Aug 4 17:01:56 2008 UTC	Thu Oct 16 17:28:18 2008 UTC	Yes	Yes
jobservice.us.	Sat Oct 11 19:12:23 2008 UTC	Thu Oct 16 19:55:59 2008 UTC	Yes	Yes
q3q.us.	Fri Jul 18 03:01:54 2008 UTC	Fri Oct 17 13:40:47 2008 UTC	Yes	Yes
jobservice.ws.	Sat Oct 11 19:12:33 2008 UTC	Thu Oct 16 19:56:24 2008 UTC	Yes	Yes

But why haven't folks been signing?

For Example, Maybe....

- **People simply don't know DNSSEC exists?** Well at least that's no longer an excuse for the folks at this IT Security session. :-)
- **Are people willing to try DNSSEC, but simply don't know the "recipe" to get going?** If so, let me recommend three resources:
 - Olaf Kolkman/NLNet Lab's "DNSSEC HOWTO, a tutorial in disguise," see http://www.nlnetlabs.nl/dnssec_howto/
 - Geoff Huston's three part (plus followup) DNSSEC saga:
<http://www.potaroo.net/ispcol/2006-08/dnssec.html>
<http://www.potaroo.net/ispcol/2006-09/dnssec2.html>
<http://www.potaroo.net/ispcol/2006-10/dnssec3.html> and
http://www.circleid.com/posts/dnssec_once_more_with_feeling/
 - The RIPE NCC's DNSSEC Training Course:
<http://www.ripe.net/training/dnssec/material/dnssec.pdf>
- **Are people waiting for the root zone (or major TLDs) to be signed?** Or are people waiting for more of their peers to take the plunge and report back, first?

Or Are There More Fundamental Problems?

- Are people just really busy, with slow uptake just the normal resistance to yet one more thing – *ANYTHING* MORE! – to handle without substantial additional resources?
- Does DNSSEC solve what's perceived by the community to be a **"non-existent" or "unimportant" problem?**
- Are there **critical administrative tools** missing? (if that's the issue, then see <http://www.dnssec-tools.org/> and http://www.ripe.net/disi/dnssec_maint_tool/)
- Does DNSSEC **demand too many system resources (e.g., does it make zone files too large, or is the CPU crypto overhead too great, or would it swamp the network with additional DNS-related network traffic?)** (Nice discussion of some of increased resource issues at <http://www.nominet.org.uk/tech/dnssectest/faq>)
- Are people waiting to see what the "big guys" do w.r.t. DNSSEC?

The Biggest Guy Out There

- One of the largest and most influential entities out there is the U.S. Federal government. With adoption of "Recommended Security Controls for Federal Information Systems," NIST 800-53 Rev. 2 (see <http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf> , December 2007), agencies theoretically had a year from December 2007 to begin doing DNSSEC. Relevant security controls from 800-53 include:
 - SC-8 "TRANSMISSION INTEGRITY
 - SC-20 "SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)"
 - SC-21 "SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)"
- See also NIST SP 800-81, "Secure Domain Name System (DNS) Deployment Guide," May 2006.
- December 2008 is fast approaching (and don't forget about the OMB Memorandum mentioned previously as well)

Unfortunately...

- Federal agencies face a HUGE number of information security requirements under FISMA, and in many cases while agencies are working hard to try to comply, they simply haven't been able to fully do so yet. The 8th FISMA Report Card, released in May, 2008 shows many federal agencies still able to make only a D or F grade overall (<http://republicans.oversight.house.gov/media/PDFs/Reports/FY2007FISMAReportCard.pdf>).
- Given the many fundamental computer security issues in play, is there reason to believe that the (comparatively) obscure issue of DNSSEC, out of all the FISMA requirements laid on Federal agencies, will end up becoming a noteworthy and ubiquitous Federal cyber security success story?
- It is probably fundamentally unfair to expect the federal government to do something which even the most security conscious private entities haven't yet done...
- And now, with a change of administration coming, well, progress may be even harder to achieve in the federal cybersecurity space.

Federal Agencies And Commercial Partners

- Many federal agencies also work closely with commercial partners (such as commercial DNS providers & content delivery networks):

:: ANSWER SECTION:

gov.	259200	IN	NS	A.GOV.ZONEEDIT.COM.
gov.	259200	IN	NS	E.GOV.ZONEEDIT.COM.
gov.	259200	IN	NS	B.GOV.ZONEEDIT.COM.
gov.	259200	IN	NS	D.GOV.ZONEEDIT.COM.
gov.	259200	IN	NS	C.GOV.ZONEEDIT.COM.
gov.	259200	IN	NS	F.GOV.ZONEEDIT.COM.
gov.	259200	IN	NS	G.GOV.ZONEEDIT.COM.

www.irs.gov.	900	IN	CNAME	www.irs.gov.edgesuite.net.
www.navy.mil.	12882	IN	CNAME	www.navy.mil.edgesuite.net.

- Because of that, DNSSEC-ifying some "federal" online resources will also require active involvement of commercial partners.

Something to Note: DNSSEC Adoption Doesn't Need to Be Symmetric

- When deploying DNSSEC, adoption doesn't need to be symmetric:
 - you can sign your own zones with DNSSEC on your authoritative name servers, yet **not** check DNSSEC on your recursive user-facing name servers, or
 - you can check DNSSEC on your recursive customer-facing facing name servers, yet **not** publish DNSSEC records for your own domains on your authoritative name servers
- Most sites will eventually want to "take the whole plunge" (or skip the technology entirely), but sometimes different people have decision making authority for different parts of the organization, and you should recognize that asymmetric adoption is a possibility.

Thanks for the Chance to Talk Today!

- Even if you don't deploy DNSSEC tomorrow, be sure to at least deal with the Kaminsky vulnerability from the start of the talk, and maybe work on getting issues flagged by <http://dnscheck.iis.se/> addressed.
- Are there any questions?
- *If there aren't any questions, or we have extra time, we could also take a couple of minutes to talk about securing open recursive DNS servers.*

Securing Open Recursive DNS Servers

We started out by asking you to test and if necessary fix your configuration, so we might as well close with one additional DNS-related request

Authoritative and Recursive DNS Servers

- There are different types of name servers, with “authoritative” and “recursive” DNS servers being the two most important types:
 - Authoritative servers are definitive for particular domains, and should provides information about those domains (and ONLY those domains) to anyone.
 - Recursive servers are customer-facing name servers that should answer DNS queries for customers (and ONLY for customers) concerning any domain.
- DNS servers that aren't appropriately limited can become abused.

For Example...

- Consider a situation where a DNS server is recursive AND is open for use by anyone (a server that's cleverly termed an “open recursive DNS server”).
- While it might seem sort of “neighborly” to share your name server with others, in fact it is a really bad idea (the domain name system equivalent of running an open/abusable SMTP relay, in fact).
- The problem? Well, there are actually **multiple** problems, but one of the most important ones is associated with spoofed UDP traffic and distributed denial of service attacks.

Spoofed DNS Attack Scenario

Dramatis personae:

- Attacker, who's working from non-BCP38 filtered network. Let's call him/her “A”
- Attack target – let's refer to that entity as “T”
- Open recursive domain name server on large, high bandwidth pipe, denoted below as “NS”

Act 1, Scene 1:

- “A” generates spoofed DNS queries with “T”'s address as the "source" address of the queries
- “NS” receives the spoofed queries and dutifully returns the “responses” for those queries to “T”
- “A” repeats as desired, thereby DoS'ing “T” via “NS”

Some Spoofed DNS Attack Scenario Notes

- From “T”’s point of view, the attack comes from “NS” not from “A”
- DNS queries are small and use UDP, so an attacker can generate a “large” query volume
- DNS response traffic is also UDP, which means that it is insensitive to net congestion.
- DNS responses can be **large** relative to size of DNS queries (output over input ratios can run over 8X on most DNS servers, and on servers supporting RFC2671 EDNS0 extensions, observed amplification can exceed 70X).
- “A” can employ **multiple query sources**, and **use multiple NS's** for even more traffic (oh boy!)

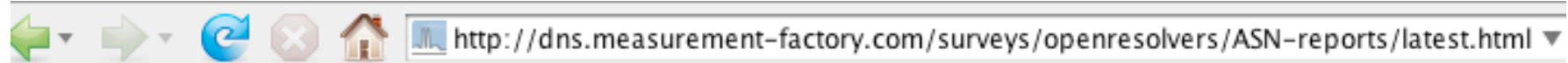
This Is A Well Known Vulnerability

- I'm not letting the “cat out of the bag” about a big secret; this is a well-known, well-documented threat:
 - “The Continuing Denial of Service Threat Posed by DNS Recursion, v2.0”
www.us-cert.gov/reading_room/DNS-recursion033006.pdf
 - “DNS Amplification Attacks”
www.isotf.org/news/DNS-Amplification-Attacks.pdf
 - "DNS Distributed Denial of Service (DDoS) Attacks"
www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf

Open Domain Name Servers Worldwide

- Unfortunately, despite this being a well known problem, it is estimated that 52.1% of all name servers worldwide run as open recursive name servers. (see <http://dns.measurement-factory.com/surveys/200710.html>)
- And in a spirit of self-criticism, feel free to note that UO's name servers were open until we secured them this past February 1st, 2006. (see <http://cc.uoregon.edu/cnews/winter2006/recursive.htm>)
- **If *our* domain name servers were open recursive until Feb 2006, *how about yours*? Please work to get them secured.**
- **You could run separate authoritative and recursive name servers, or try BIND's "views" feature as another alternative to address this issue.**

Open Domain Name Servers by ASN



This table shows the number of known open resolvers for each autonomous system as of Sun Oct 19 06:00:01 UT

count	asn	name
12891	21844	THEPLANET-AS - THE PLANET
4569	3462	HINET Data Communication Business Group
3676	4713	-Allocated by APNIC-
3590	32244	LIQUID-WEB-INC - Liquid Web, Inc.
3335	4766	KIXS-AS-KR Korea Telecom
3110	8167	TELESC - Telecomunicacoes de Santa Catarina SA
3105	7132	SBIS-AS - SBC Internet Services
3071	3561	SAVVIS - Savvis
2961	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.
2910	23352	SERVERCENTRAL - Server Central Network
2899	5617	TPNET Polish Telecom_s commercial IP network
2520	36351	SOFTLAYER - SoftLayer Technologies Inc.
2418	3595	GNAXNET-AS - Global Net Access, LLC
2344	16276	OVH OVH
2225	4323	TWTC - Time Warner Telecom, Inc.
2119	3356	LEVEL3 Level 3 Communications
2052	4134	CHINANET-BACKBONE No.31,Jin-rong Street
2024	9121	TTNET Ttnet Autonomous System
1918	209	ASN-QWEST - Qwest
1889	25653	FORTRESSITX - FortressITX
1876	3786	LGDACOM LG DACOM Corporation
1873	7018	ATT-INTERNET4 - AT&T WorldNet Services
1818	701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Busi
1778	8001	NET-ACCESS-CORP - Net Access Corporation
1772	1650	EDU-PLANET-ASN1 Michigan Academic Network (MAnet) Information C

And Some Extra Credit

Monitor Your Own DNS Traffic

- If you monitor your own DNS traffic, you may be able to identify local compromised hosts, as well as external attacks. Some DNS monitoring tools you should know about include:
- DNSTOP: <http://dns.measurement-factory.com/tools/dnstop/>
- And the DNS Tools at OARC (www.dns-oarc.net/oarc/tools), including (but not limited to):
 - DNSCAP: DNS traffic capture utility
 - NCAP: Network Capture Library and Tools (like libpcap and tcpdump)

If You Find Yourself Interested in DNSSEC In Spite of All the Obstacles, You May Want to Join the DNSSEC Deployment Working Group

For more information about how to do this, see:

<http://www.dnssec-deployment.org/wg/>