

A survey of DNSSEC deployment in the U.S. R&E community

**Shumon Huque; University of Pennsylvania
Bill Owens; NySERNET**

**Joint Techs Conference, Stanford University, July 16th 2012
<http://events.internet2.edu/2012/jt-stanford/>**

Abstract:

DNSSEC (DNS Security Extensions) is a system to verify the authenticity of DNS data using public key signatures.

Although a small number of institutions in the R&E community have been at the forefront of DNSSEC deployment, the adoption rate in the larger community is still quite low.

This talk will present some results of an ongoing project to survey the status of DNSSEC deployment in the US Research & Education and a few other communities. It also surveys the status of several other DNS capabilities, such as availability of the service over IPv6 transport, TCP transport, EDNS0 support, etc.

Agenda

- DNSSEC deployment monitoring project overview
- Live demo of the website
- New uses of DNSSEC by applications (DANE/TLSA etc)
 - (time permitting)

DNSSEC at a glance

- “DNS Security Extensions”
- A system to verify the authenticity of DNS “data” using public key signatures
 - Specs: RFC 4033, 4034, 4035, 5155 (and more)
- Helps detect DNS spoofing, misdirection, cache poisoning ..
- Additional benefits:
 - Ability to store and use cryptographic keying material in the DNS, eg. SSHFP, IPSECKEY, CERT, DKIM, TLSA, etc ..

Other surveys

- SecSpider
 - <http://secspider.cs.ucla.edu/>
- NIST's IPv6 and DNSSEC deployment status
 - <http://fedv6-deployment.antd.nist.gov/>
 - <http://www.dnsops.gov/USAdotGOV-status.html>
- Verisign Labs scorecard
 - <http://scoreboard.verisignlabs.com/>
- Internet Society's Deploy360 program
 - <http://www.internetsociety.org/deploy360/dnssec/statistics/>

Our survey

- Useful to have a survey more specifically targeted at our community, and related communities of interest to us
 - Internet2 members
 - R&E networks (GigaPoPs and RONs)
 - ESNNet & Department of Energy Labs
 - Others? (InCommon, ISPs, Tech companies, ...)
- And that provides more details about various DNS/DNSSEC configuration parameters

Our survey

- Examine externally visible characteristics of the Authoritative DNS service at these institutions
- In addition to DNSSEC, we also assess the deployment of features like Pv6 transport, TCP transport, EDNS0 support etc

<http://www.huque.com/app/dnsstat/>

DNSstat - some DNS zone statistics

This project looks at externally visible characteristics of the authoritative DNS service for a selected set of DNS domains or zones. Its original motivation was to assess the state of deployment of features like **DNSSEC** and **IPv6 transport** in the US Research and Education community, but now includes a few other categories of institutions also. Clicking on the name of each category (in the 1st column) will display a table of DNS features and statistics (eg. [internet2](#), [esnet](#), etc).

The information collected includes: the number of name server records associated with the domain (zone), the number of name server addresses, how many of the servers respond to UDP queries and TCP queries, how many of the servers advertise IPv6 addresses and also respond to IPv6 DNS queries, how many of the servers support EDNS0, whether the zone supports DNSSEC. If DNSSEC is supported, what algorithms are used for the key signing and zone signing keys. If NSEC3 is supported the associated parameter information. If DS records are available (ie. there is a secure delegation from the parent), what DS hash algorithms are in use. The detail view for each individual zone has additional details.

For each category of institution, there are also two additional subcategory views that show only DNSSEC enabled, and only IPv6 enabled domains. A domain is considered to be IPv6 enabled, if it advertises at least one nameserver with an IPv6 address.

DNSstat zone information categories

Category	Description	Total Domains	DNSSEC Enabled	IPv6 Enabled
internet2	Internet2 Members	210	14 (6.7%)	60 (28.6%)
esnet	ESNet community	11	9 (81.8%)	11 (100.0%)
ivyleague	The Ivy League	8	1 (12.5%)	4 (50.0%)
nysernet	NYSERNet members	30	0 (0.0%)	10 (33.3%)
gigapop	Internet2 GigaPoPs	16	3 (18.8%)	11 (68.8%)
usnews_20	US News Top 20 universities	20	1 (5.0%)	8 (40.0%)
times_hied_50	Times Higher Ed Top 50	50	5 (10.0%)	32 (64.0%)
techcom	Top Tech Companies	44	1 (2.3%)	10 (22.7%)
tld	Top Level Domains	313	97 (31.0%)	267 (85.3%)
All	All domains in all categories	632	126 (19.9%)	378 (59.8%)

Category stats

Category	Total	DNSSEC-enabled	IPv6-enabled
Internet2 members	210	14 (6.7%)	60 (28.6%)
ESNet community	11	9 (81.8%)	11 (100%)
Ivy League	8	1 (12.5%)	4 (50.0%)
NySERNET	30	0 (0.0%)	10 (33.3%)
GigaPoPs	16	3 (18.8%)	11 (68.8%)
US News top 20	20	1 (5.0%)	8 (40.0%)
Times HigherEd 50	50	5 (10.0%)	32 (64.0%)
Tech companies	44	1 (2.3%)	10 (22.7%)
Top Level Domains	313	97 (31.0%)	268 (85.6%)
Total	632	126 (19.9%)	379 (60.0%)

[Joint Techs, Stanford University, Jul 2012]

Internet2 member progress

- 210 total domains
- Probing this category the longest (6 months)
- No change in DNSSEC-enabled; small change in IPv6-enabled

<u>Month</u>	<u>DNSSEC- enabled</u>	<u>IPv6- enabled</u>
2012-Feb	14	55
2012-Mar	14	57
2012-Apr	14	59
2012-May	14	60
2012-Jun	14	60
2012-Jul	14	60

[Joint Techs, Stanford University, Jul 2012]

Data per zone

- Number of nameserver records & nameserver addresses
- Number of servers responding to UDP queries
- Number of servers responding to TCP queries
- Number of working IPv6 servers vs total IPv6 servers
- Number of servers supporting EDNS0
- DNSSEC support:
 - KSK and ZSK key algorithms; NSEC3 parameters; DS algorithms

Data per zone

- Also a per-zone page with additional details and debugging information.

DNS domain statistics (internet2)

A detailed [description of the columns](#) used in the table can be found at the bottom of the page.

Clicking on a domain name (first column) displays more information for that domain.

Number of domains: **210**

[DNSSEC Enabled](#): **14** (6.7%)

[IPv6 Enabled](#): **60** (28.6%)

DNSstat zone information table (internet2)

Domain	Organization Name	NScount	UDP	TCP	IPv6	EDNS0	DNSSEC	NSEC3	DS
alaska.edu	University of Alaska Fairbanks	4,4	4,4	4,4		4,4			
albany.edu	University At Albany, State University of New York	7,9	9,9	9,9	2,2	9,9			
american.edu	American University	4,4	3,4	3,4		1,4			
arizona.edu	University of Arizona	5,5	5,5	5,5		5,5			
astate.edu	Arkansas State University	4,5	3,5	3,5	0,1	3,5			
asu.edu	Arizona State University	4,4	4,4	4,4		4,4			
auburn.edu	Auburn University	5,6	6,6	5,6	1,1	5,6			
baylor.edu	Baylor University	4,4	3,4	3,4		3,4			
bc.edu	Boston College	2,2	2,2	2,2		2,2			
bcm.edu	Baylor College of Medicine	5,5	5,5	5,5		5,5			
berkeley.edu	University of California, Berkeley	6,12	12,12	12,12	6,6	12,12	k=10 z=10		2
bgsu.edu	Bowling Green State University	4,4	4,4	4,4		4,4			
binghamton.edu	Binghamton University	3,3	2,3	2,3		2,3			

Looking at [berkeley.edu](#): it has:

NSCount: 6 nameserver records, 12 nameserver addresses

UDP response: 12 of 12 servers, TCP response 12 of 12 servers

IPv6 response: 6 of 6 servers; EDNS0 response 12 of 12 servers

It has DNSSEC, uses algorithm 10 (RSASHA512) for its KSK & ZSK, and publishes a DS record in EDU with algorithm 2 (SHA2)

[Joint Techs, Stanford University, Jul 2012]

DNS zone details for: berkeley.edu (University of California, Berkeley)

Date of latest check: July 10, 2012, 8:48 a.m.

Time required for check: 4.52 seconds

Zone Summary information:

- 6 Nameserver records (IPv4=6, IPv6=6)
- 12 Nameserver addresses (IPv4=6, IPv6=6)
- Successful DNS/UDP response: 12 of 12 servers
- Successful DNS/TCP response: 12 of 12 servers
- Successful DNS/IPv4 response: 6 of 6 servers
- Successful DNS/IPv6 response: 6 of 6 servers
- Zone supports DNS over TCP queries on all its servers (12 responses of 12)
- Zone advertises IPv6 on at least one of its servers (6 of 6 IPv6 addresses responded)
- Zone supports DNSSEC (DNS Security Extensions)
 - KSK keytag 12834, algorithm 10 (RSASHA512)
 - ZSK keytag 28219, algorithm 10 (RSASHA512)
- Zone does not use NSEC3
- Zone has published DS (Delegation Signer) records
 - DS keytag 12834, algorithm 2 (SHA-256)

[Analyze this zone with DNSViz](#)

Debugging information:

```
Found nameserver: phloem.uoregon.edu.  
  Found IPv6 address: 2001:468:d01:20::80df:2023  
  Found IPv4 address: 128.223.32.35  
Found nameserver: adns2.berkeley.edu.  
  Found IPv6 address: 2607:f140:ffff:fffe::e  
  Found IPv4 address: 128.32.136.14  
Found nameserver: adns1.berkeley.edu.  
  Found IPv6 address: 2607:f140:ffff:fffe::3  
  Found IPv4 address: 128.32.136.3  
Found nameserver: sns-pb.isc.org.  
  Found IPv6 address: 2001:500:2e::1  
  Found IPv4 address: 192.5.4.1  
Found nameserver: aodns1.berkeley.edu.  
  Found IPv6 address: 2607:f010:3f8:8000:0:ff:fe00:53  
  Found IPv4 address: 192.35.225.133  
Found nameserver: ns.v6.berkeley.edu.  
  Found IPv6 address: 2607:f140:ffff:fffe::6  
  Found IPv4 address: 128.32.136.6  
NS records 6, IP4 6, IP6 6
```


Number of domains: **14**
 Secure delegations: **12 (85.7%)**
 NSEC3 Enabled: **6 (42.9%)**

DNSstat zone information table (internet2 - DNSSEC)

Domain	Organization Name	NScount	UDP	TCP	IPv6	EDNS0	DNSSEC	NSEC3	DS
berkeley.edu	University of California, Berkeley	6,12	12,12	12,12	6,6	12,12	k=10 z=10		2
cmu.edu	Carnegie Mellon University	3,4	4,4	4,4	1,1	4,4	k=7 z=7		1,2
indiana.edu	Indiana University	3,5	5,5	5,5	2,2	5,5	k=10 z=10,10		2,1
internet2.edu	Internet2	4,7	7,7	7,7	3,3	7,7	k=7,7 z=7,7,7	1,0,10	2,1,2,1
ksu.edu	Kansas State University	5,7	7,7	7,7	2,2	7,7	k=8 z=8	1,0,10	
lsu.edu	Louisiana State University	4,6	6,6	6,6	2,2	6,6	k=8 z=8	1,0,10	2
mst.edu	University of Missouri - Rolla	6,6	6,6	6,6		6,6	k=5 z=5		2,1
okstate.edu	Oklahoma State University	2,2	2,2	2,2		2,2	k=5 z=5		
sdsmt.edu	South Dakota School of Mines and Technology	8,16	14,16	16,16	7,8	16,16	k=8 z=8	1,0,5	2,1
ualr.edu	University of Arkansas at Little Rock	4,7	5,7	5,7	1,3	5,7	k=7 z=7	1,0,10	1
ucr.edu	University of California, Riverside	4,8	8,8	8,8	4,4	8,8	k=10 z=10	1,0,10	1,2
uiowa.edu	University of Iowa	4,10	10,10	10,10	4,4	10,10	k=8 z=8		1,2
umbc.edu	University of Maryland, Baltimore County	3,3	3,3	3,3		3,3	k=5 z=5		2
upenn.edu	University of Pennsylvania	5,8	8,8	8,8	3,3	8,8	k=5 z=5,5		2,1
Domain	Organization Name	NScount	UDP	TCP	IPv6	EDNS0	DNSSEC	NSEC3	DS

Key Usage Statistics

Key Signing Keys (KSK):

RSASHA256 (8) = 4 (26.7%)
 RSASHA512 (10) = 3 (20.0%)
 RSASHA1 (5) = 4 (26.7%)
 RSASHA1-NSEC3-SHA1 (7) = 4 (26.7%)

Zone Signing Keys (ZSK):

RSASHA256 (8) = 4 (22.2%)
 RSASHA512 (10) = 4 (22.2%)
 RSASHA1 (5) = 5 (27.8%)
 RSASHA1-NSEC3-SHA1 (7) = 5 (27.8%)

DNSSEC - Internet2

DNSSEC stats: Internet2 members

domain	DNSSEC	NSEC3	DS
berkeley.edu	k=10 z=10		2
cmu.edu	k=7 z=7		2,1
indiana.edu	k=10 z=10,10		1,2
internet2.edu	k=7,7 z=7,7,7	1,0,10	1,2
ksu.edu	k=8 z=8	1,0,10	
lsu.edu	k=8 z=8	1,0,10	2
mst.edu	k=5 z=5		2,1
okstate.edu	k=5 z=5		
sdsmt.edu	k=8 z=8	1,0,5	1,2
ualr.edu	k=7 z=7	1,0,10	1
ucr.edu	k=10 z=10	1,0,10	2,1
uiowa.edu	k=8 z=8		1,2
umbc.edu	k=5 z=5		2
upenn.edu	k=5, z=5, 5		1,2

[Joint Techs, Stanford University, Jul 2012]

DNSSEC algorithms

Key Signing Keys (KSK)

RSASHA256 (8)	=	4	(26.7%)
RSASHA512 (10)	=	3	(20.0%)
RSASHA1 (5)	=	4	(26.7%)
RSASHA1-NSEC3-SHA1 (7)	=	4	(26.7%)

Zone Signing Keys (ZSK)

RSASHA256 (8)	=	4	(22.2%)
RSASHA512 (10)	=	4	(22.2%)
RSASHA1 (5)	=	5	(27.8%)
RSASHA1-NSEC3-SHA1 (7)	=	5	(27.8%)

NSEC3 deployment

- Internet2 community NSEC3 deployment summary
- 6 of 14 DNSSEC zones (42.9%)
- All use hash algorithm 1 (SHA-1)
- All use Flags=0 (i.e. there is no use of the Opt-out feature)
- Number of hash iterations range from 5 to 10

Secure Delegations

- Summary of secure delegations (DS records) for Internet2
- 12 signed zones in total
- 10 of them have DS records
- Missing 2 are: ksu.edu and okstate.edu
- ksu.edu has DLV record published at dlv.isc.org

- Note: .EDU is signed and has a sole registrar (Educause) that is capable of publishing DS records for any EDU domain

IPv6 transport

- More promising adoption rate than DNSSEC in every category of institution
- Internet2 has 60 of 210 zones (28.6%)
- But noticeable number of domains have broken IPv6 transport to some subset of their nameservers
 - this can be seen by looking at the IPv6 column: the 1st number is the number of IPv6 servers that responded to queries, the 2nd number is the number of IPv6 servers advertised

IPv6 transport

DNSstat zone information table (internet2)

Domain	Organization Name	NScount	TCP	IPv6	EDNSC
alaska.edu	University of Alaska Fairbanks	4,4	4,4		4,4
albany.edu	University At Albany, State University of New York	7,9	6,9	2,2	6,9
american.edu	American University	4,4	2,4		0,4
arizona.edu	University of Arizona	5,5	5,5		5,5
astate.edu	Arkansas State University	4,5	3,5	0,1	3,5
asu.edu	Arizona State University	5,5	5,5		5,5
auburn.edu	Auburn University	5,6	5,6	1,1	5,6
baylor.edu	Baylor University	4,4	3,4		3,4
bc.edu	Boston College	2,2	2,2		2,2

1 IPv6 nameserver, but 0 working

from detail page:

```
Trying DNS/UDP query to passage.uark.edu., 2604:fc00:f:7::103  
DNS/UDP failed: passage.uark.edu., 2604:fc00:f:7::103 (<class  
'dns.exception.Timeout'>, )
```

[Joint Techs, Stanford University, Jul 2012]

Live demonstration

[Joint Techs, Stanford University, Jul 2012]

Times HigherEd top 50

Number of domains: 5
NSEC3 Enabled: 0 (0.0%)

DNSstat zone information table (times_hied_50 - DNSSEC)

Domain	Organization Name	Nscount	TCP	IPv6	EDNS0	DNSSEC	NSEC3	DS
berkeley.edu	University of California, Berkeley	6,12	12,12	6,6	12,12	k=10 z=10,10		2
cam.ac.uk	Cambridge University	7,10	10,10	3,3	10,10	k=5 z=5		1,2
cmu.edu	Carnegie Mellon University	3,4	4,4	1,1	4,4	k=7 z=7		1,2
imperial.ac.uk	Imperial College London	4,7	7,7	3,3	7,7	k=5 z=5		1,2
upenn.edu	University of Pennsylvania	5,8	8,8	3,3	8,8	k=5 z=5,5		2,1
Domain	Organization Name	Nscount	TCP	IPv6	EDNS0	DNSSEC	NSEC3	DS

- 5 (10%) DNSSEC enabled: UC Berkeley, Cambridge U, Carnegie Mellon U, Imperial College, and Penn. None are NSEC3.
- 32 (64%) IPv6 Enabled

[Joint Techs, Stanford University, Jul 2012]

ESNet community

DNS domain statistics (esnet)

A detailed [description of the columns](#) used in the table can be found at the bottom of the page.

Clicking on a domain name (first column) displays more information for that domain.

Number of domains: **11**

[DNSSEC Enabled](#): **9** (81.8%)

[IPv6 Enabled](#): **11** (100.0%)

DNSstat zone information table (esnet)

Domain	Organization Name	NScount	UDP	TCP	IPv6	EDNS0	DNSSEC	NSEC3	DS
ameslab.gov	Ames Laboratory	6,10	10,10	10,10	4,4	10,10	k=7,7 z=7,7	1,0,10	
anl.gov	Argonne National Laboratory	6,10	10,10	10,10	4,4	10,10			
bnl.gov	Brookhaven National Laboratory	3,4	4,4	4,4	1,1	4,4	k=5 z=5,5,5		1,2
es.net	Energy Sciences Network	3,6	6,6	6,6	3,3	6,6	k=5,5 z=5,5		1,2
fnal.gov	Fermilab	5,10	10,10	10,10	5,5	10,10	k=7 z=7,7	1,0,10	1
jlab.org	Jefferson Lab	5,9	8,9	8,9	3,4	8,9	k=5,5 z=5,5		
lbl.gov	Lawrence Berkeley National Lab	5,9	9,9	9,9	4,4	9,9	k=7 z=7	1,0,10	2,1
ornl.gov	Oak Ridge National Lab	4,7	7,7	7,7	3,3	7,7	k=7 z=7,7	1,0,100	1,2
pnl.gov	Pacific Northwest National Lab	2,4	4,4	4,4	2,2	4,4	k=7,7 z=7	1,0,10	2
pppl.gov	Princeton Plasma Physics Lab	4,7	7,7	7,7	3,3	7,7	k=7 z=7	1,0,10	2
slac.stanford.edu	Stanford Linear Accelerator Lab	3,4	3,4	1,4	0,1	3,4			
Domain	Organization Name	NScount	UDP	TCP	IPv6	EDNS0	DNSSEC	NSEC3	DS

DNS domain statistics (esnet - DNSSEC enabled)

A detailed [description of the columns](#) used in the table can be found at the bottom of the page.

Clicking on a domain name (first column) displays more information for that domain.

Number of domains: **9**

Secure delegations: **7 (77.8%)**

NSEC3 Enabled: **6 (66.7%)**

DNSstat zone information table (esnet - DNSSEC)

Domain	Organization Name	NScount	UDP	TCP	IPv6	EDNS0	DNSSEC	NSEC3	DS
ameslab.gov	Ames Laboratory	6,10	10,10	10,10	4,4	10,10	k=7,7 z=7,7	1,0,10	
bnl.gov	Brookhaven National Laboratory	3,4	4,4	4,4	1,1	4,4	k=5 z=5,5,5		1,2
es.net	Energy Sciences Network	3,6	6,6	6,6	3,3	6,6	k=5,5 z=5,5		1,2
fnal.gov	Fermilab	5,10	10,10	10,10	5,5	10,10	k=7 z=7,7	1,0,10	1
jlab.org	Jefferson Lab	5,9	8,9	8,9	3,4	8,9	k=5,5 z=5,5		
lbl.gov	Lawrence Berkeley National Lab	5,9	9,9	9,9	4,4	9,9	k=7 z=7	1,0,10	2,1
ornl.gov	Oak Ridge National Lab	4,7	7,7	7,7	3,3	7,7	k=7 z=7,7	1,0,100	1,2
pnl.gov	Pacific Northwest National Lab	2,4	4,4	4,4	2,2	4,4	k=7,7 z=7	1,0,10	2
pppl.gov	Princeton Plasma Physics Lab	4,7	7,7	7,7	3,3	7,7	k=7 z=7	1,0,10	2
Domain	Organization Name	NScount	UDP	TCP	IPv6	EDNS0	DNSSEC	NSEC3	DS

Key Usage Statistics

Key Signing Keys (KSK):

RSASHA1 (5) = 5 (38.5%)

RSASHA1-NSEC3-SHA1 (7) = 8 (61.5%)

Zone Signing Keys (ZSK):

RSASHA1 (5) = 7 (43.8%)

RSASHA1-NSEC3-SHA1 (7) = 9 (56.3%)

[Joint Techs, Stanford University, Jul 2012]

GigaPoPs

Why no DS records? Lack of DNSSEC capable registrars?

DNS domain statistics (gigapop)

A detailed [description of the columns](#) used in the table can be found at the bottom of the page.

Clicking on a domain name (first column) displays more information for that domain.

Number of domains: **16**

[DNSSEC Enabled](#): **3** (18.8%)

[IPv6 Enabled](#): **11** (68.8%)

DNSstat zone information table (gigapop)

Domain	Organization Name	NScount	UDP	TCP	IPv6	EDNS0	DNSSEC	NSEC3	DS
3rox.net	Three Rivers Optical Exchange	3,5	5,5	5,5	2,2	5,5	k=5 z=5,5		
cenic.org	CENIC	3,3	3,3	3,3		3,3			
flrnet.org	Florida LambdaRail	2,2	2,2	2,2		2,2			
gigapop.net	Northern Lights GigaPoP	3,5	5,5	5,5	2,2	5,5			
greatplains.net	Great Plains Network	4,7	7,7	7,7	3,3	7,7			
indiana.gigapop.net	Indiana GigaPoP	3,5	5,5	5,5	2,2	5,5			
loni.org	Louisiana Optical Network Initiative	3,4	4,4	4,4	1,1	4,4			
magpi.net	MAGPI	3,5	5,5	5,5	2,2	5,5	k=5 z=5,5		
maxgigapop.net	Mid-Atlantic Crossroads	2,3	2,3	2,3	0,1	2,3			
mcnc.org	MCNC	3,3	3,3	3,3		3,3			
merit.edu	MERIT Network Inc	3,3	3,3	3,3		3,3	k= z=7		
nox.org	Northern Crossroads	3,5	5,5	5,5	2,2	5,5			
nysernet.org	NYSERNet	3,4	4,4	4,4	1,1	4,4			
pnw-gigapop.net	Pacific Northwest GigaPoP	3,6	6,6	6,6	3,3	6,6			
sox.net	Southern Crossroads	3,5	5,5	5,5	2,2	5,5			
uen.org	Utah Education Network	2,2	2,2	2,2		2,2			

[Joint Techs, Stanford University, Jul 2012]

Tech companies

Number of domains: 44

DNSSEC Enabled: 1 (2.3%)

IPv6 Enabled: 10 (22.7%)

DNSstat zone information table (techcom)

Domain	Organization Name	NScount	UDP	TCP	IPv6	EDNS0	DNSSEC
adobe.com	Adobe	4,4	4,4	4,4		4,4	
akamai.com	Akamai	8,8	8,8	8,8		8,8	
alcatel-lucent.com	Alcatel-Lucent	6,6	6,6	6,6		6,6	
amazon.com	Amazon	10,18	18,18	18,18	8,8	18,18	
apple.com	Apple	8,8	8,8	8,8		8,8	
att.com	AT&T	4,4	4,4	4,4		4,4	
brocade.com	Brocade Networks	4,8	8,8	8,8	4,4	7,8	
bt.com	BT Group	4,4	4,4	4,4		4,4	
chinamobileltd.com	China Mobile	3,3	1,3	2,3		1,3	
cisco.com	Cisco	2,2	2,2	2,2		2,2	
comcast.com	Comcast	5,10	10,10	10,10	5,5	10,10	k=5 z=5
ebay.com	eBay	4,4	4,4	0,4		4,4	
emc.com	EMC	6,6	6,6	6,6		6,6	
ericsson.com	Ericsson	3,4	4,4	3,4	1,1	4,4	
facebook.com	Facebook	3,3	3,3	3,3		3,3	
foxconn.com	Foxconn Technology Group	3,3	3,3	3,3		3,3	
fujitsu.com	Fujitsu	6,6	6,6	6,6		6,6	
google.com	Google	4,4	4,4	4,4		0,4	
hitachi.com	Hitachi	6,12	12,12	12,12	6,6	12,12	

Only Comcast has DNSSEC!

[Joint Techs, Stanford University, Jul 2012]

Tech companies - IPv6

DNS domain statistics (techcom - IPv6 enabled)

A detailed [description of the columns](#) used in the table can be found at the bottom of the page.

Clicking on a domain name (first column) displays more information for that domain.

Number of domains: 10

DNSstat zone information table (techcom - IPv6)

Domain	Organization Name	NScount	UDP	TCP	IPv6	EDNS0	DNSSEC	NSEC3	DS
amazon.com	Amazon	10,18	18,18	18,18	8,8	18,18			
brocade.com	Brocade Networks	4,8	8,8	8,8	4,4	8,8			
comcast.com	Comcast	5,10	10,10	10,10	5,5	10,10	k=5 z=5		1,2
ericsson.com	Ericsson	3,4	4,4	3,4	1,1	4,4			
hitachi.com	Hitachi	6,12	12,12	11,12	6,6	12,12			
ibm.com	IBM	4,5	5,5	5,5	1,1	5,5			
microsoft.com	Microsoft	5,10	10,10	9,10	5,5	10,10			
netflix.com	Netflix	6,12	11,12	12,12	5,6	12,12			
symantec.com	Symantec	8,14	14,14	14,14	6,6	14,14			
telekom.com	Deutsche Telekom	3,5	5,5	5,5	2,2	5,5			
Domain	Organization Name	NScount	UDP	TCP	IPv6	EDNS0	DNSSEC	NSEC3	DS

Tech companies

- Of the 44 surveyed, only one (Comcast) has deployed DNSSEC for their domain name
- Only 10 (22.7%) have IPv6 reachable DNS servers
- Google lacks any EDNS0 support
- Facebook & Google have no IPv6 reachable DNS, even though they support IPv6 on their websites
 - So clients using IPv6-only DNS resolvers will not be able to reach their sites!
- A lot of partially broken TCP support

ToDo List

- DNSSEC validation of (some) zone records
- Are name servers distributed across >1 ASN?
- Are any IPv6 nameservers native to the zone
- Are nameservers distributed across multiple zones?
- Other categories of institutions
- History of deployment growth over time
- History of detected DNSSEC key changes
- Additional vantage points for measurement

New uses of DNSSEC

[Joint Techs, Stanford University, Jul 2012]

Application use of DNSSEC

- One of the more exciting prospects for DNSSEC
- DNSSEC allows applications to securely obtain (authenticate) cryptographic keying material stored in the DNS
- A variety of existing and proposed record types have been designed to store crypto material:
 - SSHFP, IPSECKEY, CERT
 - DKIM _domainkey TXT record (p=... public key data)
 - TLSA (upcoming, see IETF DANE working group)

Application use of DNSSEC

- Securely obtaining other assertions from the DNS
 - DKIM/ADSP
 - Route Origination Authorizations (controversial - see RPKI, the standardized mechanism to do this, which will allow BGP path validation also)

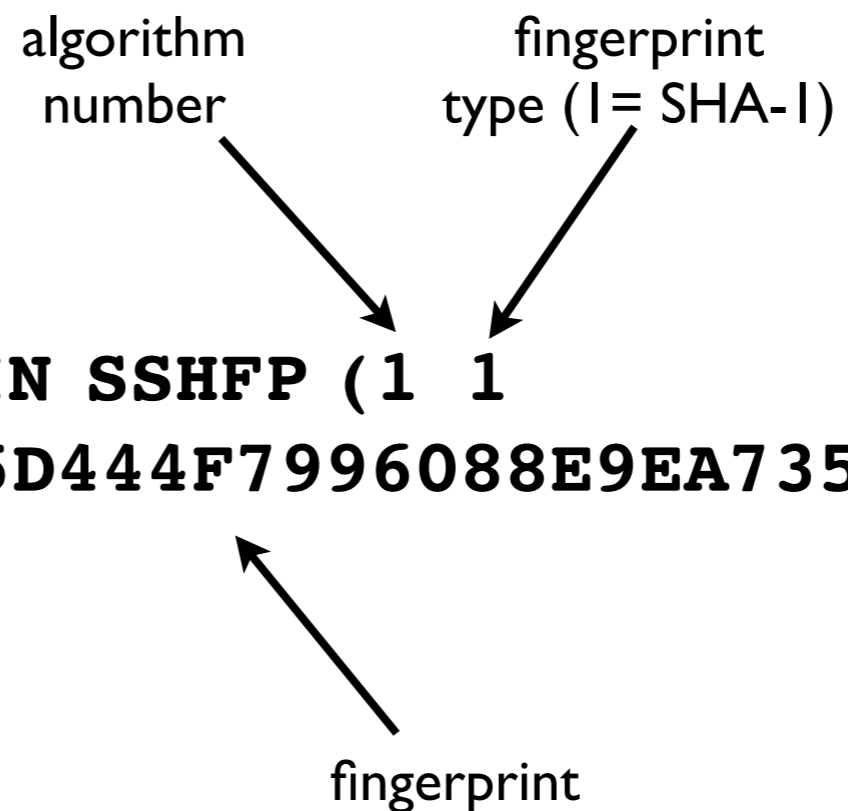
SSHFP record

- SSH Host Key Fingerprint (RFC 4255)
- Allows you to validate SSH host keys using DNS (i.e. securely using DNSSEC)

algorithm number fingerprint type (1 = SHA-1)

**grodd.magpi.net. 86400 IN SSHFP (1 1
F60AE0994C0B02545D444F7996088E9EA7359CBA)**

fingerprint



IPSECKEY record

- RFC 4025: method for storing IPSEC keying material in DNS
- rdata format: precedence, gateway-type, algorithm, gateway address, public key (base64 encoded)
- This one hasn't seen much adoption to date

```
38.2.0.192.in-addr.arpa. 7200 IN IPSECKEY ( 10 1 2  
192.0.2.38  
AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ== )
```

Public CA model problems

- Applications need to trust a large number of global certificate authorities, and this trust appears to be unfounded
- No namespace constraints! **Any** of them can issue certificates for **any** entity on the Internet, whether you have a business relationship with them or not
- Least common denominator security: our collective security is equivalent to weakest one
- Furthermore, many of them issue subordinate CA certificates to their customers, again with no naming constraints
- Most are incapable of issuing certs with any but the most basic capabilities (eg. alternate name forms or other extensions)

DANE/TLSA record

- The DNS-Based Authentication of Named Entities (DANE) Protocol for Transport Layer Security (TLS)
 - draft-ietf-dane-protocol-23 (almost published as RFC)
 - RR type code for TLSA record is assigned (52)
- Use DNSSEC for better & more secure ways to authenticate SSL/TLS certificates:
 - by specifying authorized public CAs, allowable end entity certs, authorizing new non-public CAs, or even directly authenticating certs without involving CAs!

TLSA record example

port, transport proto &
server domain name

TLSA rrtype



```
_443._tcp.www.example.com. IN TLSA (  
  0 0 1 d2abde240d7cd3ee6b4b28c54df034b9  
  7983a1d16e8a410e4561cb106618e971 )
```

usage

selector

matching
type

certificate association data

TLSA rdata parameters

Usage field:

- 0 CA Constraint
- 1 Service Certificate Constraint
- 2 Trust Anchor Assertion
- 3 Domain Issued Certificate

Selector field:

- 0 Match full certificate
- 1 Match only SubjectPublicKeyInfo

Matching type field:

- 0 Exact match on selected content
- 1 SHA-256 hash of selected content
- 2 SHA-512 hash of selected content

Certificate Association Data: raw certificate data in hex

Questions?