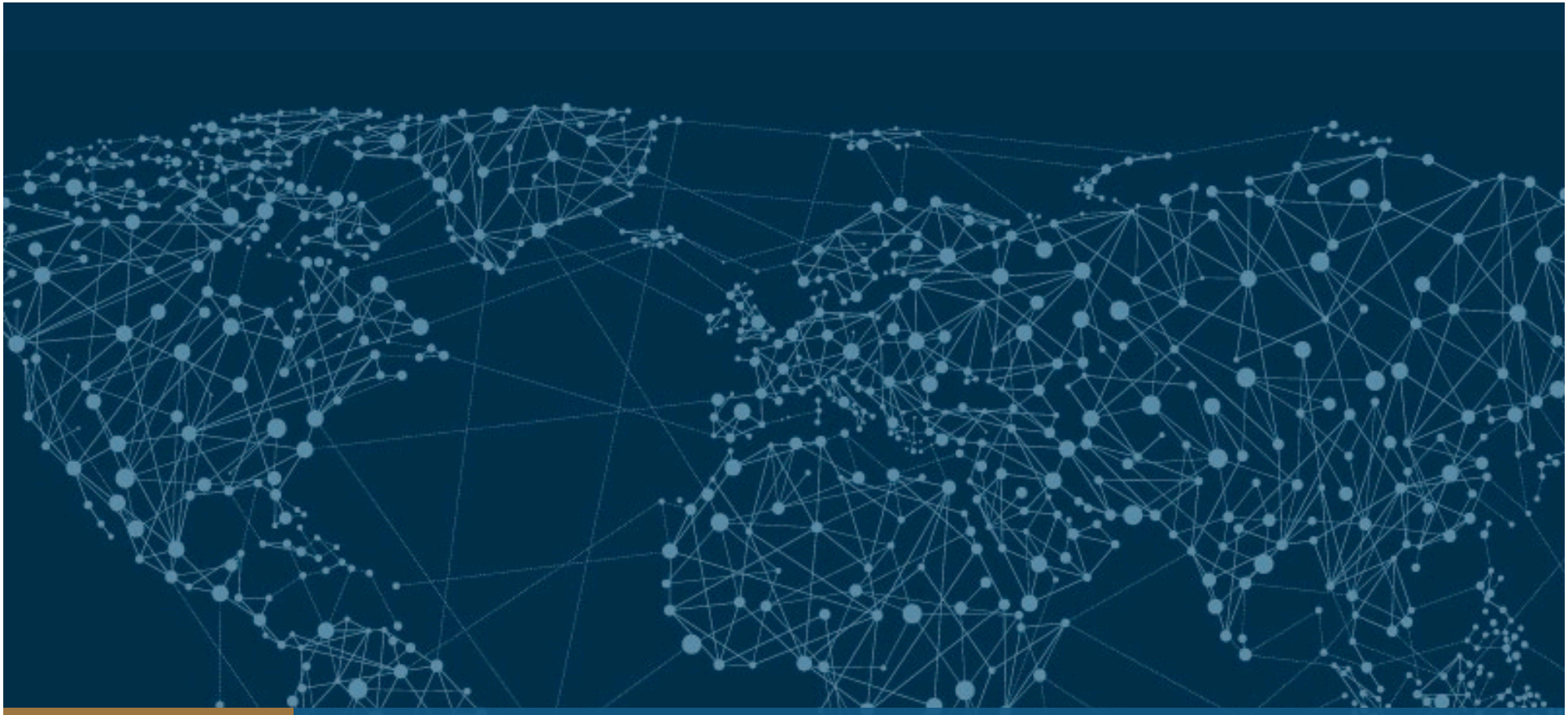

DNSSEC Cryptographic Habits of the gTLD Second Level Zones

Edward Lewis | ICANN DNS Symposium | 13 May 2017

Data Source(s)

- May 1, 2017, zone files reported to ICANN according to registry agreements plus queries across the DNS that day
- A similar presentation, given two years ago, is used as a comparison, based on May 4, 2015 data
  - This data may over count certain results, use for "magnitude" comparisons
- A note on precision: "millions" "thousands" "ones" are used to reduce numerical clutter
  - May 1, 2017 data take still has 2% bad responses that need to be ironed out

TLDs Studied, then and now

Statistic	May 4, 2015	May 1, 2017
Total zones (root+TLDs) - Live	948	1532
DNSKEYs in root+TLD - Live	778	1387
DS records - Live	767	1379
Zones studied - Reported	655 (69%)	1234* (80%)
DNSKEY'd Zones studied	647 (83%)	1233* (88%)
Class-of-2012 TLDs (studied)	635	1214*
Pre-Class of 2012 with DS (")	11	18
Without DS (")	8	1

* - One zone is in a statistical "limbo". No longer delegated but...

Coverage of SLDs

Statistic	May 4, 2015	May 1, 2017
Total names	155 million	186 million
Names with DS records	688 thousand	993 thousand
Percentage of names	0-point-44%	0-point-53%

Hash Algorithms in DS records

Statistic	May 1, 2017
Total DS records in zone files	1 million
Names with DS records	993 thousand
Names with SHA-1 DS hashes in set	275 thousand
Names with only SHA-1 DS hashes (solo)	*227 thousand*
Names with SHA-256 DS hashes in set	765 thousand
Names with only SHA-256 DS hashes (solo)	*717 thousand*
Names with GOST DS hashes in set	335 (*20 "flying solo"*)
Names with SHA-384 DS hashes in set	402 (*60 "flying solo"*)
Names with SHA-1 and SHA-256	48 thousand
With GOST/SHA-384, no SHA-1/-256	81

DNSSEC Security Algorithms in DS records

Algorithm Name	Count
RSA-SHA1	712 thousand
RSA-SHA256	189 thousand
EC-SHA256T	153 thousand
RSA-SHA512	2 thousand

Less than 1 thousand: "Delete", Private DNS, Private OID, Diffie-Hellman, GOST, DSA-SHA-1(NSEC3), RSA-MD5, EC-SHA384T

DNSKEY Flags

Statistic	May 4, 2015	May 1, 2017
Names with DS records	688 thousand	993 thousand
Names with collected DS	682 thousand	- (N/A)
Names owning KSK	666 thousand	968 thousand
Names owning ZSK	672 thousand	965 thousand
Names owning revoked KSK	41	23
Names owning revoked ZSK	5	9

Keys by Algorithm (counting names)

Statistic	May 4, 2015	May 4, 2017
RSA-SHA1	573 thousand	679 thousand
RSA-SHA256	146 thousand (*)	142 thousand
EC-SHA256T	38 ones	147 thousand
RSA-SHA512	453	1015
GOST	16	19
EC-384T	14	176
DSA-SHA1	6	10
"0" (Delete)	0	1

* - Strongly suspect this is an over count

Keys by Size and Algorithm

Statistic	May 4, 2015	May 1, 2017
Total Keys	----	2.2 million
RSA-SHA1 @ 1024b	1 million	1.3 million
EC-256T	80 (ones)	335 thousand
RSA-SHA1 @ 2048b	164 thousand	217 thousand
RSA-SHA256 @1024b	208 thousand (*)	186 thousand
RSA-SHA256 @2048b	152 thousand	152 thousand
RSA-SHA256 @1280b	1 thousand	5 thousand
RSA-SHA1 @ 4096b	1-2 thousand	3 thousand
RSA-SHA256 @ 4096b	761 ones	1 thousand
RSA-SHA512 @ 2048b	none reported	1 thousand

* - Strongly suspect this is an over count

Engage with ICANN

Thank You and Questions

Reach us at:
Email: engagement@icann.org
Website: icann.org

twitter.com/icann

soundcloud.com/icann

facebook.com/icannorg

weibo.com/ICANNorg

youtube.com/user/icannnews

flickr.com/photos/icann

linkedin.com/company/icann

slideshare.net/icannpresentations