UNIVERSITÄT DUISBURG ESSEN

Measurement Survey of Server-Side DNSSEC Adoption

Matthäus Wander

<matthaeus.wander@uni-due.de>

ICANN 56

Helsinki, June 27, 2016

Version: 2016-06-22

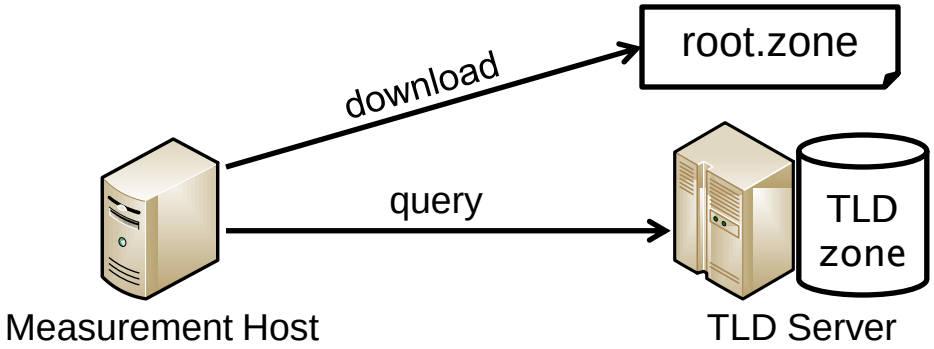
Outline

1. DNSSEC signing at top-level domains
2. Quantification of **all** signed second-level domains (5.1 million)
3. Analysis of 3.4 million signed second-level domains

- Datasets acquired in **February/March 2015**
  - Partial update on signing algorithms from **June 2016**

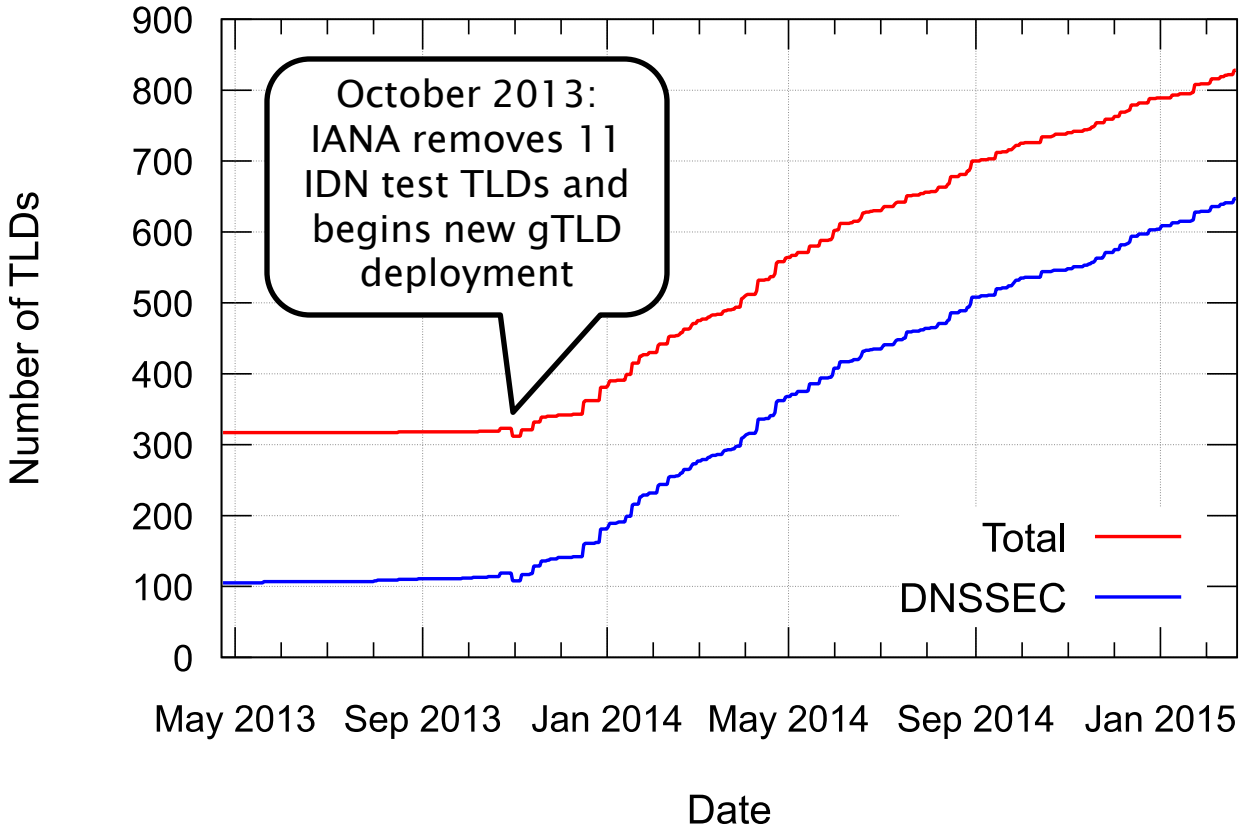
TOP-LEVEL DOMAINS

Signed Top-Level Domains



- Method:
  - Download and parse IANA root zone file daily
  - Probe TLD servers daily for various records
  - 22-month observation from Apr 2013 to Feb 2015

Timeline


900
800
700
600
500
400
300
200
100
0
Number of TLDs
October 2013:
IANA removes 11
IDN test TLDs and
begins new gTLD
deployment
Total
DNSSEC
May 2013
Sep 2013
Jan 2014
May 2014
Sep 2014
Jan 2015
Date

Public Keys

- **647** TLDs (**100%**) use RSA as signing algorithm
  - All with separate KSK/ZSK

KSK

Key Length	Count
1024	1
1280	4
2048	772
2056	1
4096	5

Feb 2015

Most frequent: 2048-bit KSK

ZSK

Key Length	Count
1024	594
1032	1
1048	2
1152	3
1280	225
2048	32

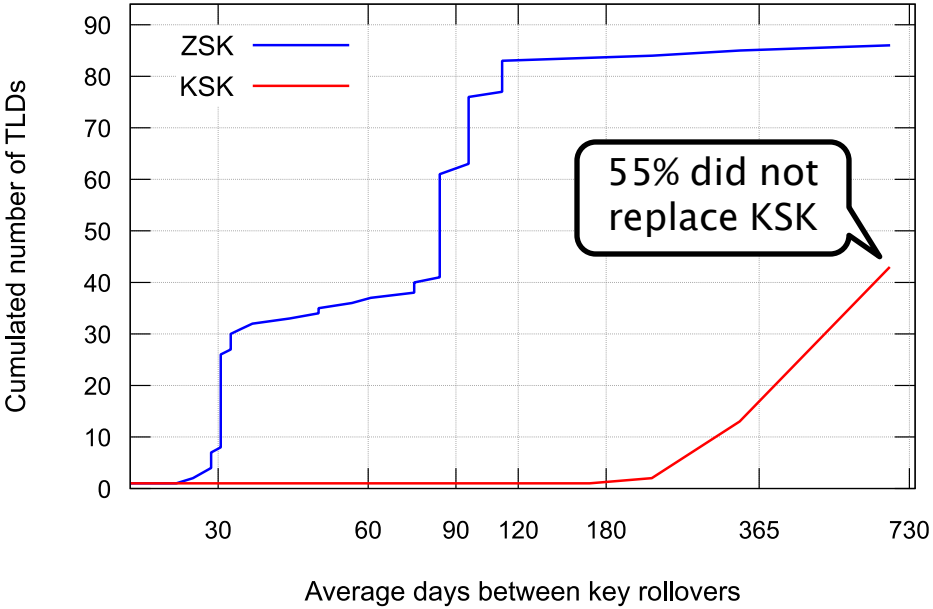
Feb 2015

Most frequent: 1024-bit ZSK

ARI Registry Services uses 1280-bit ZSK for new gTLDs

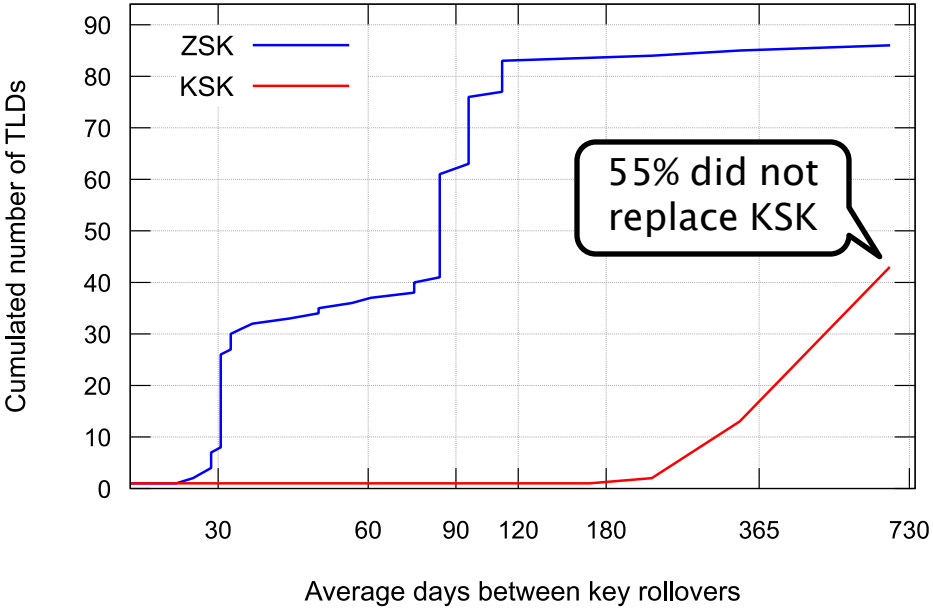
Key Rollover Intervals

94 TLDs signed for the whole period

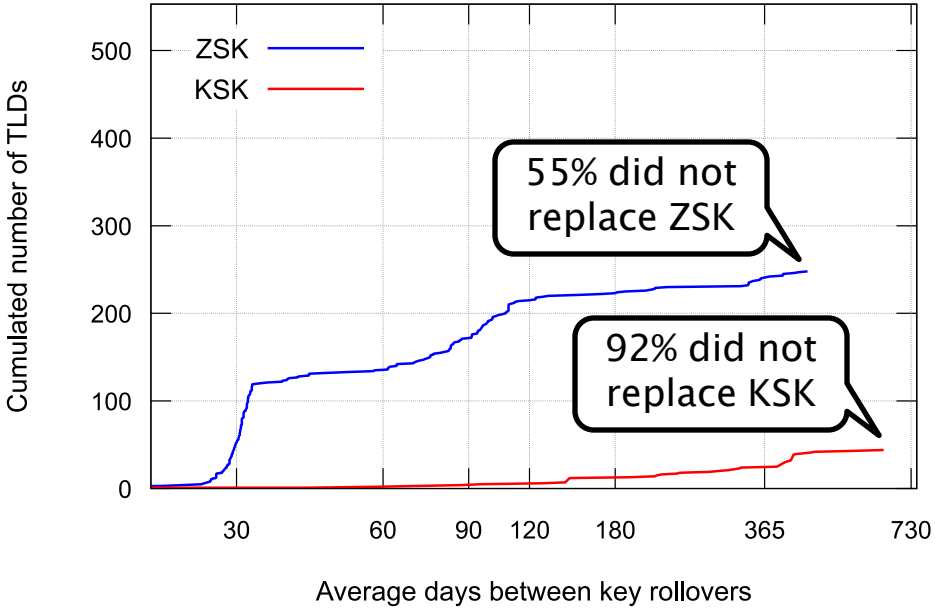


Key Rollover Intervals

94 TLDs signed for the whole period



553 newly signed TLDs



RSA Public Exponent

- Choice of *e* determines verification performance
  - Guideline: small value, low hamming weight

KSK

Exponent	Count
3	15
$2^{16} + 1$	762
$2^{32} + 1$	6

Feb 2015

e.g. by Verisign

ZSK

Exponent	Count
3	15
$2^{16} + 1$	834
$2^{32} + 1$	8

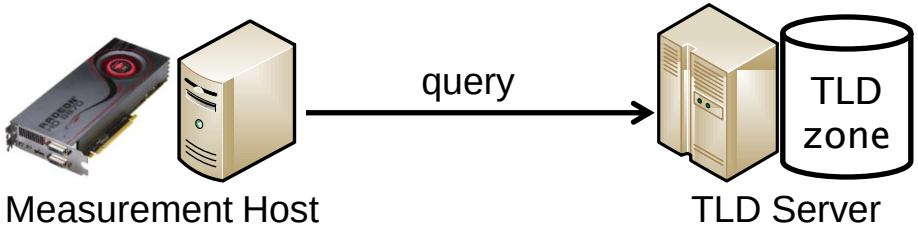
Feb 2015

Most frequent: *e*=65,537

- Above choices are fine (safe and fast)

QUANTIFICATION OF SIGNED SECOND-LEVEL DOMAINS

DNSSEC at Second-Level Domains



- Method:
  - Perform NSEC & NSEC3 zone enumeration on all TLDs
  - Includes 26 SLDs like `com.br`, `co.kr`, `com.tw`, `co.uk`
  - NSEC: `ldns-walk` [http://www.nlnetlabs.nl/projects/ldns/]
  - NSEC3: `nsec3breaker` [http://dnssec.vs.uni-due.de/nsec3]

Zone Enumeration Results

- Duration: about 3–4 days in March 2015
- 107 TLDs with NSEC: 7.99 million names
- 540 TLDs with NSEC3: 7.49 million hash values
  - Most TLDs use opt-out, thus fewer NSEC3 records
  - CPU fast enough to retrieve most NSEC3 hash values
  - Switched to GPU to close the last few gaps (~100) for large zones ⇨ yields complete NSEC3 chain

TLDs with most Secure Delegations

	TLD	NSEC(3)	DS	Address	Empty	Other
1.	nl	NSEC3, opt-out, i=5	2,279,702	5	1	1
2.	br	subject to subdomain	566,694	0	0	34,625
3.	cz	NSEC3, i=10	448,984	0	0	717,267
4.	com	NSEC3, opt-out, i=0	426,182	0	0	1
5.	se	NSEC	349,514	9	0	940,946
6.	eu	NSEC3, opt-out, i=1	320,311	7	1	1
7.	fr	NSEC3, opt-out, i=1	205,662	0	6	3
8.	no	NSEC3, opt-out, i=5	119,759	4	2	2
9.	be	NSEC3, opt-out, i=5	92,385	0	1	2
10.	net	NSEC3, opt-out, i=0	81,391	0	0	1
	[637 others omitted]					
		Total:	**5,146,705**	**926,279**	**131,610**	**9,272,944**

TLDs with most Secure Delegations

	TLD	NSEC(3)	DS	Address	Empty	Other
1.	nl	NSEC3, opt-out, i=5	2,279,702	5	1	1
2.	br	subject to subdomain	566,694	0	0	34,625
3.	cz	NSEC3, i=10	448,984	0	0	717,267
4.	com	NSEC3, opt-out, i=0	426,182	0	0	1
5.	se	NSEC	349,514	9	0	940,946
6.	eu	NSEC3, opt-out, i=1	320,311	7	1	1
7.	fr	NSEC3, o			0	
8.	no	NSEC3, o			4	2
9.	be	NSEC3, opt-out, i=5	92,3			
1			81,391			
			37 others omitted]			
		Total:	**5,146,705**	**926,279**	**131,610**	**9,272,944**

A or AAAA records (plus a few CNAME or MX records)

Insecure delegations or other records

Empty non-terminals

Total number of securely delegated registered domains

Address Records

	TLD	NSEC(3)	DS	Address	Empty	Other
11.	org	NSEC3, opt-out, i=1	46,382	10,737	4,976	448
12.	ovh	NSEC3, opt-out, i=1	29,372	0	0	1
13.	nu	NSEC3, i=5	21,126	0	0	235,308
14.	de	NSEC3, opt-out, i=15	20,004	185,107	89,689	2
15.	pl	NSEC3, opt-out, i=12	18,110	7	0	1

- Some TLDs allow to put addresses directly into the TLD zone instead of delegations
  - Causes empty non-terminals when e.g. record for `www.example.de` exists but `example.de` is empty

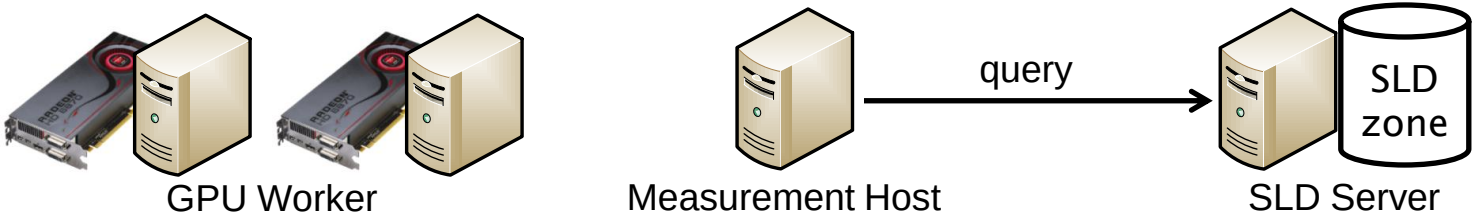
Dangling Glue Records

	TLD	NSEC(3)	DS	Address	Empty	Other
11.	org	NSEC3, opt-out, i=1	46,382	10,737	4,976	448
12.	ovh	NSEC3, opt-out, i=1	29,372	0	0	1
13.	nu	NSEC3, i=5	21,126	0	0	235,308
14.	de	NSEC3, opt-out, i=15	20,004	185,107	89,689	2
15.	pl	NSEC3, opt-out, i=12	18,110	7	0	1

- Some TLDs do not enforce removal of glue records after a delegation has been removed
  - Former glue record like `ns1.example.org` becomes authoritative and causes empty non-terminal

ANALYSIS OF SIGNED SECOND-LEVEL DOMAINS

Algorithms and Keys at Second-Level Domains



- Method:
  - Break NSEC3 hash values with `nsec3breaker`
  - Query for DS and DNSKEY records for known second-level domains

NSEC3 Hash Breaking

- NSEC3: 7.49 million hash values from 540 TLDs
  - 4.65 million (62%) broken after 3 weeks of computing
  - 4 graphic cards (AMD HD 7970, AMD HD 6970, 2x NVIDIA GTX 690)
  - 22 CPU cores (contribute 2% of total computing power)

Method	Names tested	Names found
Brute-force	5.2×10^{14}	1,353,657
Dictionary	3.2×10^{14}	3,198,966
Markov	1.1×10^{13}	96,817
Total	**8.4×10^{14}**	**4,649,424**

NSEC3 attack details: [https://www.vs.uni-due.de/paper/2014_Wander_NSEC3.pdf]

Signing Algorithms and Public Keys

- 3.4 million domains with DS (67% out of 5.1M)
  - 89% of them appear to use a KSK/ZSK scheme

Zero RSA/MD5

Few DSA keys

Algorithm	Key SEP=1	Key SEP=0
RSA/MD5	0	0
DSA/SHA-1	2,176	2,279
RSA/SHA-1	1,550,859	1,848,283
RSA/SHA-256	1,875,294	2,785,784
RSA/SHA-512	1,220	1,158
GOST R 34.10-2001	30	30
ECDSA P-256/SHA-256	27	25
ECDSA P-384/SHA-384	21	17
Total	**3,429,630**	**4,637,576**

March 2015

Most frequent: RSA (>99%)

ECDSA rarely (in **2015**)

Signing Algorithms and Public Keys (2016)

- 2.6 out of the 3.4 million domains still there
  - Some domains have ceased to exist in the meantime

Algorithm	Key SEP=1	Key SEP=0	Key SEP=1	Key SEP=0
RSA/MD5	0	0	0	0
DSA/SHA-1	2,176	2,279	1,256	1,289
RSA/SHA-1	1,550,859	1,848,283	1,057,868	1,365,548
RSA/SHA-256	1,875,294	2,785,784	1,442,347	2,131,923
RSA/SHA-512	1,220	1,158	26,285	51,409
GOST R 34.10-2001	30	30	34	34
ECDSA P-256/SHA-256	27	25	707	551
ECDSA P-384/SHA-384	21	17	44	36
Total	**3,429,630**	**4,637,576**	**2,528,542**	**3,550,790**
	March 2015		*June 2016*	

DSA declining

Most frequent: RSA (>99%)

ECDSA growing

RSA Key Lengths

- 0.4% of domains have an insufficient key length

Key Length	Key SEP=1	Key SEP=0
512	8,704	14,416
1024	724,324	4,333,715
1280	878	214,944
1536	154,748	123
2048	2,454,645	64,947
4096	83,602	5,142
Other	472	925
Total	**3,427,373**	**4,635,221**

March 2015

Insecure

Most frequent: 1024-bit ZSK

Most frequent: 2048-bit KSK

2016 shifts slightly to longer keys but no major change yet

RSA Public Exponent

Exponent	Key SEP=1	Key SEP=0
3	202	252
65,337	26	60
65,535	124	288
$2^{16} + 1$	3,421,138	4,629,425
$2^{30} + 3$	38	51
$2^{32} + 1$	5,845	5,145
Total	**3,427,373**	**4,635,221**

March 2015

Most frequent: e=65,537

Not $2^{16} + 1$ ☺

- Some strange values for e occur: probably typos
  - Not a problem if basic RSA properties are met: e must be coprime with $\theta(n)$

DSA Key Lengths

- DSA keys in DNSSEC are specified for group sizes up to 1024 bit
  - Note: a 1024-bit DSA key is about 3x larger in wire format than a 1024-bit RSA key

Key Length	Key SEP=1	Key SEP=0
512	3	5
768	2	3
1024	2,173	2,271
Total	**2,178**	**2,279**

March 2015

Most frequent: 1024-bit KSK

Most frequent: 1024-bit ZSK

Validation Result

- All 3.4 million domains ought to be signed
  - 0.6% (2015) respectively 1.3% (2016) fail validation

Most frequent error: DNSKEY response contains no key

Validation Result	Domains		Domains
No DNSKEY (dangling DS)	17,751		31,642
No trusted DNSKEY (dangling DS)	1,066		1,278
No RRSIG for trusted DNSKEY	238		153
Signature expired	2,138		668
Signature verify failure	5		5
Validation failure	**21,198**		**33,746**
Validation success	**3,416,700**		**2,520,610**
	March 2015		*June 2016*

Recommendations

- Deprecate DSA
  - Large DNSKEY records, insufficient key length
- If using RSA, use keys with ≥2048 bits
  - If stuck with 1024 bit, replace them every few weeks
- Consider using ECDSA with 256-bit keys
- Consider using a combined signing key unless KSK/ZSK are stored at separate places

Conclusions

- More than 5 million domains use DNSSEC
  - Around 1% of signed domains show validation errors
- RSA is the dominant signing algorithm
  - A few domains switched to ECDSA
- Future work: how many **newly signed** domains use elliptic curve cryptosystems?