Elliptic Curves in .CZ

Where no TLD has gone before

Ondřej Surý • ondrej.sury@nic.cz • 15. 10. 2016

CZ.NIC | SPRÁVCE DOMÉNY CZ

Why?

Motivation

- Response sizes
  - Lower fragmentation
  - Lower reflection attack (DDoS) ratios
- Zone size
  - 21% decrease in zone size
- Testing the rollover process
  - Rolling RSA → ECDSA in TLD for the first time
  - What challenges we will meet?
- Push the “deployment base”
  - DNS deployment tends to get stale
  - Get the DNS deployment base to update

The ~~Plan~~Wall

The Plan

- Measure everything
- Transition all CZ.NIC domains to ECDSA
- Inform and work with the public
- Transition .CZ to ECDSA

What?

Obstacles

- Validating resolver deployment base
  - Czech Republic
  - Global
- Key Algorithm Rollover
  - Double signing
  - IANA update

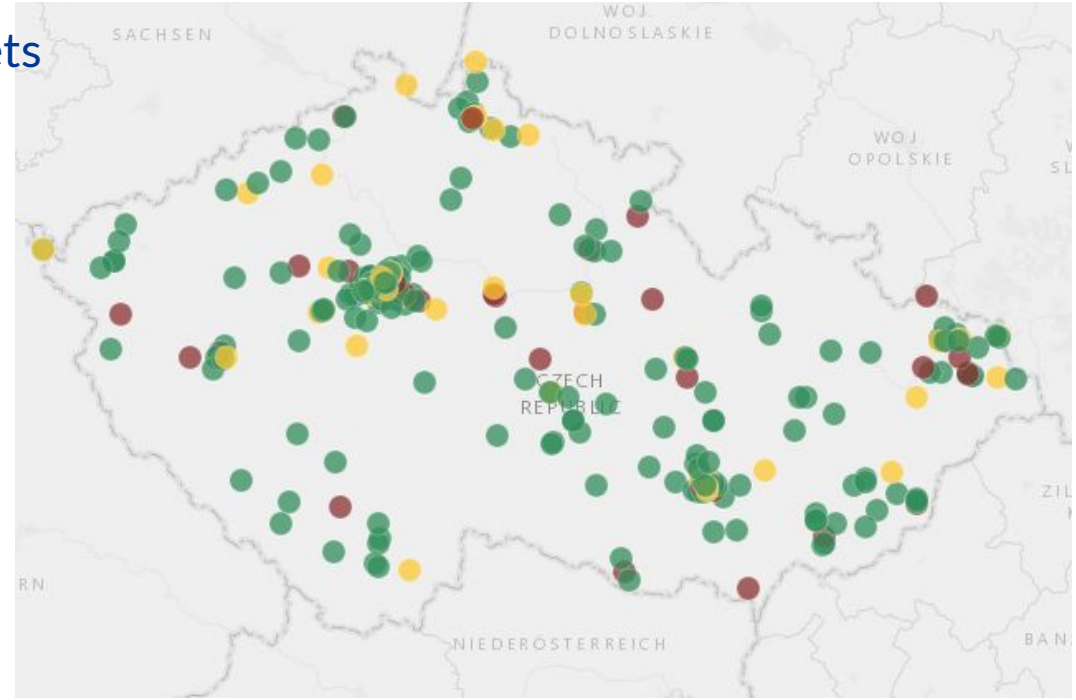
Who?

Data, data, data...

- Focus mostly on Czech Republic
- RIPE Atlas probes
- Turris 1.x
- APNIC survey (thanks!)

RIPE Atlas Methodology

- Secure/bogus/insecure triplets
  - ECC → {good,bad,no}.ecdsa.cz
  - RSA → {good,bad,no}.udp53.cz
- Use RIPE Atlas DNS test
  - ✓ Use the Probe's Resolver(s)
  - ✓ Set DO bit
  - ✓ Skip DNS check
  - ✓ / ✕ Set CD bit



RIPE Atlas Results

N = 453			BOGUS		SECURE		
	CD	ANCOUNT	ECDSA	RSA	ECDSA	RSA	δ
Supports DNSSEC-ECDSA		0	258	277	1	1	-19 (4%)
General error		-1	70	70	54	57	~
No RRSIG → No DNSSEC at all		1	50	52	53	55	~
A+RRSIG		2	75	54	345	340	21
Confused by CD?	✓	0	19	19	1	1	~
General error	✓	-1	62	62	52	53	~
No RRSIG → No DNSSEC at all	✓	1	49	48	53	52	~
A+RRSIG without validation	✓	2	323	324	347	345	~

Use of DNSSEC-ECDSA Validation for Czech Republic (CZ)

Courtesy of APNIC – http://stats.labs.apnic.net/ecdsa/CZ

Use of DNSSEC-ECDSA Validation for Czech Republic (CZ)

	Czechia (N=3714)	Global
Does not perform any validation	2440 (66%)	3,441,624 (76%)
Performs BOTH ECDSA and RSA validation	**839 (23%)**	482,833 (11%)
Performs RSA but does not appear to be supporting ECDSA	**210 (6%)**	173,383 (4%)

Transition CZ.NIC domains to ECDSA

- All but nic.cz signed with ECDSAP256SHA256
- nic.cz (contains NS for .cz) rolls in October 2016
  - Doesn’t affect other paths under .cz

How?

Inform the public

- Articles in (web) magazines / press releases
- Blogposts
- Direct contact via IXP
- Indirect contact via users

Web tool for users – “IPv6” widget

- Embeddable HTML/CSS/JS widget
  - https://labs.nic.cz/en/ipv6-widget.html
- Components can be turned on/off
- Tests for:
  - IPv6
  - DNSSEC – now with ECDSA
  - FENIX – NIX.CZ secure VLAN
- Speed measurement

Key Algorithm Update

- We still need double sign whole zone with RSA and ECDSAP256SHA256
  - Including double-ZSK
- Why?
  - BIND is fine
  - Knot Resolver is fine
  - Unbound is fine
- But…
  - Unbound 1.5.5 harden-algo-downgrade finally defaults to ‘no’ in October 2015
  - That’s like yesterday in DNS deployment world

DS update in the root

- RFC 6605 is April 2012
  - That's like last week in Groot's time…
- IANA is not yet ready :(
- IANA Transition is over now, yay!

When?

When?

- The longer of:
  - When IANA can update the DS with ECDSAP256SHA256
  - After a public has been sufficiently informed
- Somewhere sometime next year

Questions?

Ondřej Surý • ondrej.sury@nic.cz • 15. 10. 2014