TLS: usage in Russian Domain Space

Dmitry Belyavskiy, TCI
ICANN 58 Tech Day
March 13, 2017
Copenhagen, Denmark
TLS: brief history

- SSLv2 deprecated (RFC 6176)
- SSLv3 deprecated (RFC 7568)
- TLS 1.0 – RFC 2246 (1999)
- TLS 1.1 – RFC 4346 (2006)
- TLS 1.2 – RFC 5246 (2008)

Waiting for TLS 1.3!

Source: https://www.trustworthyinternet.org/ssl-pulse/
Ubiquitous encryption!

- >50% of traffic is encrypted (2016)
- New protocol require encryption by design
- Hosters enable TLS by default
  - Universal SSL
- DNS – the last major unprotected protocol
  - RFC 7626
Russian Domains

- RU (since 1994) – more than 5 500 000
- РФ (since 2010) – more than 900 000
  - The largest IDN domain in the world!
- SU (since 1990) – about 120 000
- New gTLDs: .ДЕТИ, .TATAR
- 3rd-level domains
  - Geographical, generic…
Project of CCTLD .RU and Technical Center of Internet

Based on Registry data

Domains: .RU, .SU, .РФ… http://statdom.ru/

Domain .LV http://tldstat.com/

Public and limited access to data
28 February 2017 (yesterday)

**.RU**

5 509 524  ▼ - 0.02 %
New domains in the current month: 166 408

**.РФ**

900 140  ▼ - 0.38 %
New domains in the current month: 23 158

**.SU**

118 871  ▼ - 0.41 %
New domains in the current month: 2 734

Source: [http://statdom.ru/](http://statdom.ru/)
Powerful reporting tool

Reports

- By region
- By age of the domain
- By registrar
- All you want!
Various forms of visualization

Source: [http://statdom.ru/](http://statdom.ru/)
TLS: methodology

Collecting the TLS statistics

- Process all the domains in .RU
- 443 port
- Collect certificates
- Build chains of trust to browser roots
- Profit!

Full description: http://statdom.ru/about/glossary
Amount of certificates in .RU

- July 2015
- Apr 2016
- Jan 2017

- Self-signed
- Valid
Certificates:

- July 2015: 28 000
- Feb 2017: 226 000

Web-sites:

- July 2015: 34 000
- Feb 2017: 258 000
1. Let’s Encrypt – 46%
2. Cloudflare – 15.5%
3. cPanel – 13.5%
4. Globalsign – 10%

Let’s Encrypt appeared in March 2016 and provided a significant growth
.RU: CA migrations

**Gainers**

1. Let’s Encrypt +3000
2. StartCom +700
3. COMODO (EC+RSA) +300

**Losers**

1. WoSign -900
2. GlobalSign -600

Total migration: 4500 / 45000 (Jan-Aug 2016)

Signed month later – 90%+
.RU: algorithms

- **SHA1**: 13% => 0.05% (116 certs)
- **RSA**: ~85%
- **EC**: ~15%
  - Maximum in March 2016: 32%
Interesting facts

- Almost all EC certificates are from Cloudflare
- ~70% certificates are free or parts of bundle
- ~600 EV certificates
- More at 3rd level
- NO correlation between EV and DNSSec
- MX STARTTLS: 70% IP-addresses
What do users think

- TLS is about encryption
  - No. You should authenticate the 2nd party

- Green locks save
  - No. Domain with similar name + Certificate for free = PHISHING

- Use EV certificates!
  And explain it to your clients…
What are we to worry about

- Mobile applications
  - Certificate validation errors
    - Both on iDevices and Android
  - VPNs for Android are not secure enough

- TLS termination
  - The most protected software are browsers.
  - TLS proxies have a lot of errors
How to protect yourself

Problem: ANY CA can issue a certificate for ANY domain

Solutions:
 DANE
 Certificate transparency
 Certificate pinning
Questions?

Email:

beldmit@tcinet.ru