

# DNS team

DNS/DNSSEC/DNS Privacy

IETF 98 Hackathon  
Chicago

# Projects

- DNS Privacy
  - Monitoring plug-in for DNS-over-TLS servers
  - Performance of DNS-over-TLS servers
  - Implementation of DNS Padding
  - Implementation of new forwarder
- DNSSEC: Zero configuration DNSSEC in getdns

[github code](#)

Stephane  
Borztmeyer

# DNS-over-TLS

## Monitoring plug-in

- Based on Nagios API - tests for:
  - DNS response on port 853 over TLS
  - Server authenticated (hostname/pinset)
  - Checks if certificate is about to expire
  - FUTURE - QNAME MIN, Keepalive

**RFC 7858 (DNS-over-TLS), RFC 7766 (DNS-over-TCP), RFC7815 (QNAME-MIN), RFC7858 (Keepalive), draft-ietf-dprive-dtls-and-tls-profiles**

# DNS-over-TLS Monitoring plug-in

The screenshot shows the Icinga monitoring dashboard. The left sidebar contains navigation links: Dashboard, Problems (5), Overview, History, System, Configuration, and icinga. The main content area is divided into three sections: 'Current Incidents' (with sub-tabs for Overdue and Muted), 'Service Problems', and 'Services'.

**Service Problems:**

Severity	Time	Service	Description
CRITICAL	16:11	surfnet-1-v6: dns-tls	GETDNS CRITICAL - Certificate will expire in 14 days
CRITICAL	16:05	getdns-v6: dns-tls	GETDNS CRITICAL - Certificate will expire in 14 days
CRITICAL	16:05	surfnet-1-v4: dns-tls	GETDNS CRITICAL - Certificate will expire in 14 days
CRITICAL	16:05	surfnet-2-v4: dns-tls	GETDNS CRITICAL - Certificate will expire in 14 days
CRITICAL	16:05	surfnet-2-v6: dns-tls	GETDNS CRITICAL - Certificate will expire in 14 days
WARNING	16:05	getdns-v4: dns-tls	GETDNS WARNING - Certificate will expire in 28 days

**Services:**

Service	Status	Time	Description
cmrg: dns-tls	OK	14m 11s	GETDNS OK - 181 ms, expiration date 2017-05-30, auth. Success: Address 2400:cb00:2048:1::6814:55 Address 2400:cb00:2048:1::6814:155 Address 104.20.0.85 Address 104.20.1.85
getdns-v4: dns-tls	WARNING	16:05	GETDNS WARNING - Certificate will expire in 28 days
getdns-v6: dns-tls	CRITICAL	16:05	GETDNS CRITICAL - Certificate will expire in 14 days
lorraine: dns-tls	OK	16:10	GETDNS OK - 256 ms, expiration date 2018-09-26, auth. Failed: Address 2400:cb00:2048:1::6814:55 Address 2400:cb00:2048:1::6814:155 Address 104.20.1.85 Address 104.20.0.85
oarc-v4: dns-tls	OK	16:22	GETDNS OK - 222 ms, expiration date 2027-08-25, auth. Success: Address 2400:cb00:2048:1::6814:55 Address 2400:cb00:2048:1::6814:155 Address 104.20.0.85 Address 104.20.1.85
oarc-v6: dns-tls	OK	16:13	GETDNS OK - 218 ms, expiration date 2027-08-25, auth. Success: Address 2400:cb00:2048:1::6814:55 Address 2400:cb00:2048:1::6814:155 Address 104.20.0.85 Address 104.20.1.85

**CRITICAL**  
16:05

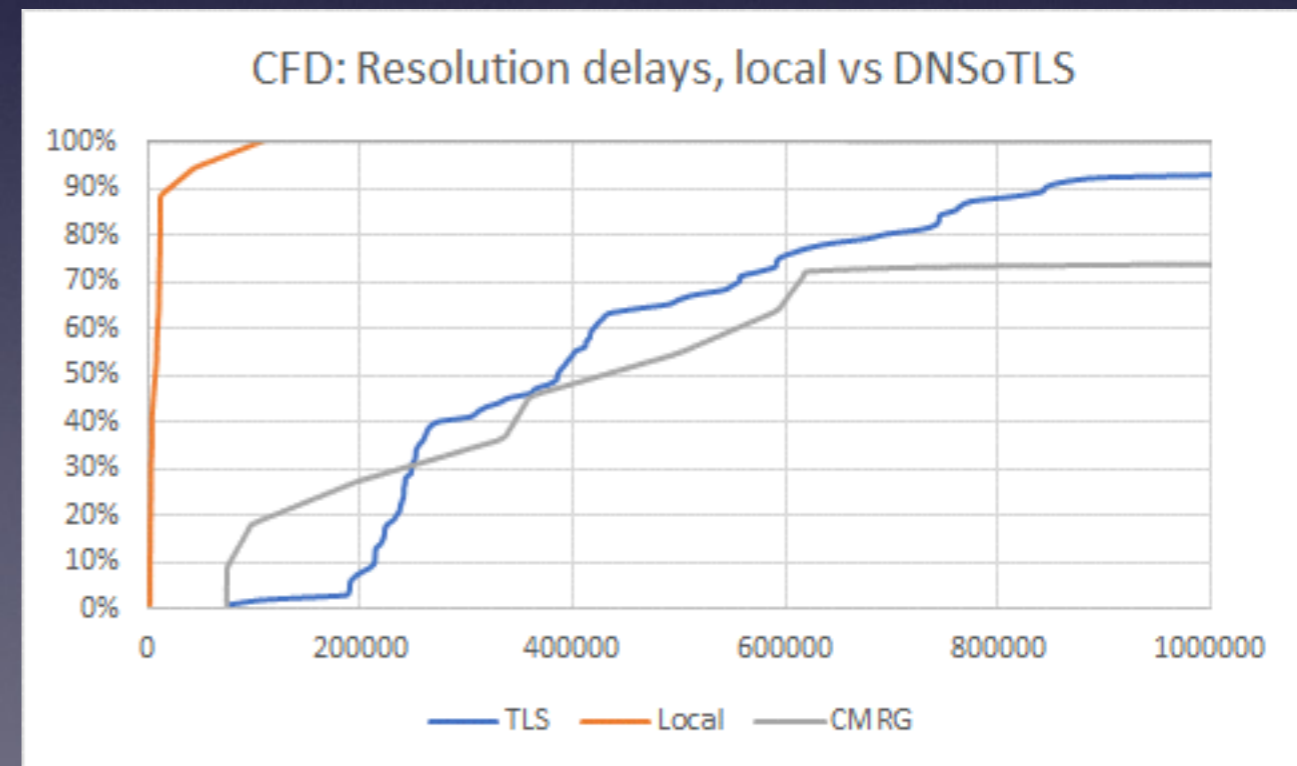
**surfnet-2-v4: dns-tls**

GETDNS CRITICAL - Certificate will expire in 14 days



# Performance of DNS-over-TLS servers

- Implementation of test script comparing local resolver to existing DNS-over-TLS servers
- “Interesting” results
- Basis for much more in depth investigation



patches  
submitted to  
[Knot Auth](#) and  
[Knot Resolver](#)

dkg

# DNS Padding

- draft-mayrhofer-dprive-padding-profile =>  
**Default policy to pad queries to mult of 128 octets, responses to mult of 468**
- Implementation (patches submitted)
  - `libknot` - new API with 'sensible' default padding policy
  - `kdig` uses this by default for TLS queries
  - `kresd` - makes use of `libknot` API
  - Plan is for `getdns` + Unbound

**RFC7830 + draft-mayrhofer-dprive-padding-profile + [dkg paper](#)**

# *kresd* as a DNS-over-TLS forwarder

- Client side DNS-over-TSL - Already have Stubby, Unbound
- `kresd` implementation in progress
  - basic implementation + config done
  - but... still debugging

# Zero configuration DNSSEC in getdns

- Root KSK is rolling! New key is public, roll will happen Oct 2017
- Some DNS implementations use static config of root trust anchor and rely on RFC5011 but...
- `getdns` would like to implement purely dynamic key management (RFC7958)



# Team

- Willem Toorop
- Daniel Kahn Gillmor
- John Dickinson
- Sara Dickinson
- Ondrey Sury
- Melinda Shore
- Alison Mankin
- Benno Overeinder
- Shumon Huque
- David Lawrence
- *Christian Huitema*
- *Stephane Bortzmeyer*