# 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

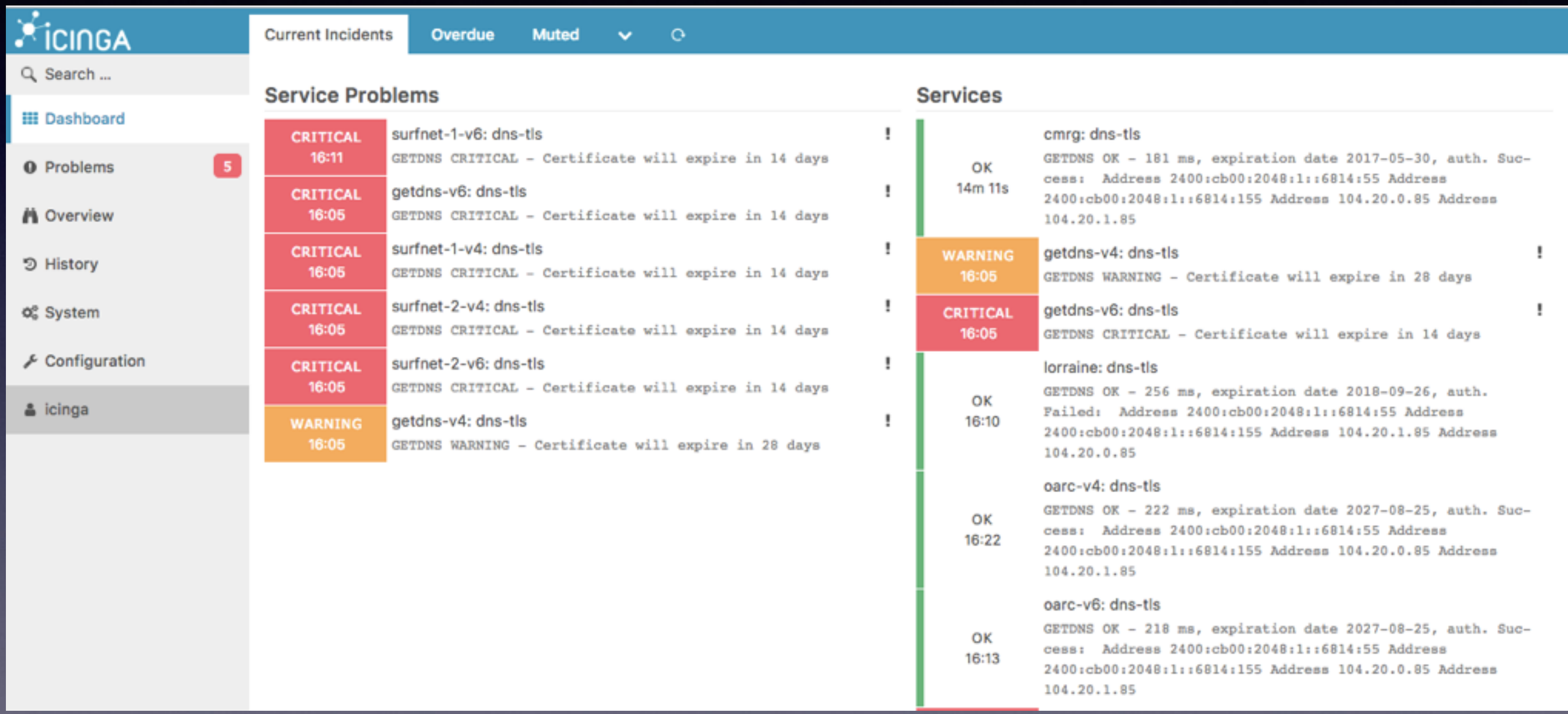
# DNS-over-TLS Monitoring plug-in

Stephane Borztmeyer

- 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

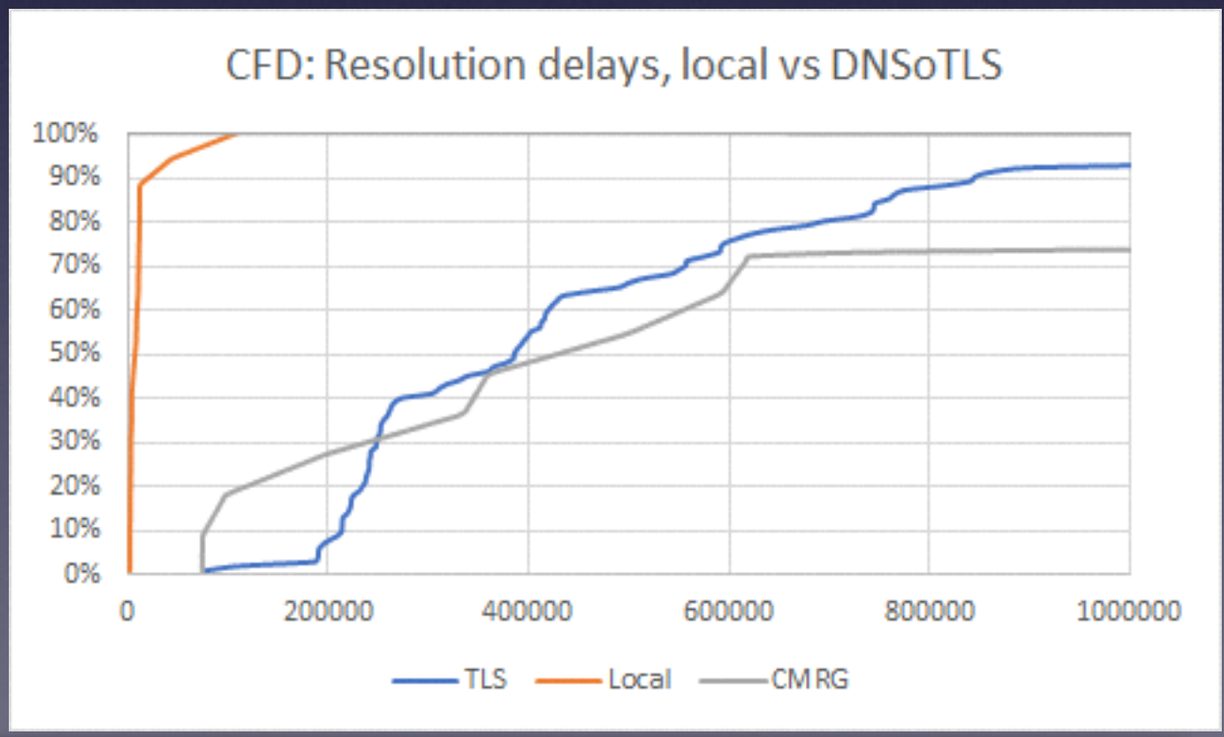



github code

# Performance of DNS-over-TLS servers

Christian Huitema

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




**RFC 7858 (DNS-over-TLS), RFC 7766 (DNS-over-TCP),**

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**

Work in to Knot Resolver

Ondrej Sury

# ***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

**RFC 7858 (DNS-over-TLS), RFC 7766 (DNS-over-TCP), draft-ietf-dprive-dtls-and-tls-profiles**

Work in to getdns

# Zero configuration DNSSEC in getdns

Willem Toorop

- 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)

**RFC 7958**

# Team

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