DNS Privacy
Implementation and Deployment

ICANN 58 TechDay

Benno Overeinder
NLnet Labs

http://www.nlnetlabs.nl/
Why DNS Privacy?

• IAB published RFC 6473: “Privacy Considerations for Internet Protocols”, July 2013
• Snowden revelations, June 2013
• RFC 7258: “Pervasive Monitoring is an Attack”, May 2014

http://www.nlnetlabs.nl/
But Wait... DNS and Privacy?
But Wait... DNS and Privacy?

• RFC 7626: “DNS Privacy Considerations”, August 2015

• Debunk “the alleged public nature of DNS data”

• Data might be public, but a DNS transaction is not (or should not be)
ATTACKS
The First/Last Mile

stub resolvers → resolver → authoritative name servers

icann.org?
ietf.org?
klm.com?
DNS Information Leakage

stub resolver → resolver → authoritative name servers

 leaks information

schedule.icann.org?

root

.org

.authoritative name servers

.schedule.icann.org?

.org

.schedule.icann.org?

.icann.org

.schedule.icann.org?
Etc. and More Information

- Excellent IETF tutorial by Sara Dickinson (Sinodun)
  - Background information
  - Other attack or DNS disclosure scenarios
  - Recent IETF RFCs and IETF WG activities
  - https://www.ietf.org/meeting/97/tutorials/dns-privacy.html
IMPLEMENTATION
Protecting the First/Last Mile

- Encrypt your DNS traffic
  - STARTTLS
  - TLS
  - DTLS
  - Confidential DNS draft
  - DNSCurve and DNSCrypt (not in IETF)
DNS over TLS

- DNS queries to resolver via (authenticated) TLS connections

- Requires “fixing” DNS over TCP/TLS
  - optimise session setup & resumption
    - TCP Fast Open and TLS session resumption
  - pipelining & out-of-order processing
    - see next slide
  - robust TCP management of many connections
    - learn from HTTP servers & proxies
Out-of-Order Processing

Without OOOP

With OOOP!
Reducing DNS Leakage: QNAME Minimisation
DEPLOYMENT
Deployment of DNS Privacy Enhanced DNS services

stub resolver

DNS over TLS

resolver

QNAME Minimisation

.org?

.org?

.icann.org?

.icann.org?

.root

authoritative name servers

schedule.icann.org?
Deployment of DNS Over TLS

• getdns as stub
  – act as stub and full recursive
  – DNSSEC as a stub
    • even without validating upstreams
  – avoid DNSSEC roadblocks
    • works around upstreams that hamper DNSSEC
• DNS64
  • signed IPv4 can be validated
• DNS Privacy
  • DNS over TLS

• **Stubby** is getdns stub resolver with all privacy options enabled
DNS Privacy Enhanced Resolvers

• Available implementations
  – Unbound
  – Knot Resolver
  – Bind + TLS proxy (nginx, HAProxy)

• DNS-over-TLS test resolvers (see dnsprivacy.net)
  – NLnet Labs and OARC: Unbound
  – SURFnet/Sinodun: Bind + HAProxy/nginx
  – dkg: Knot Resolver

http://www.nlnetlabs.nl/
QNAME Minimisation
Enabled Resolvers

• Implemented
  – Unbound
  – Knot Resolver

• In future release
  – Bind
WRAPPING-UP
Resources

• IETF DPRIVE Tutorial by Sara Dickinson and Daniel Kahn Gillmor

• DNS Privacy websites
  – Community, non-technical: [dnsprivacy.org](http://dnsprivacy.org)
  – Enterprise/corporate users: [dnsprivacy.net](http://dnsprivacy.net)

• getdns project website
  – [getdnsapi.net](http://getdnsapi.net)
Acknowledgements & Questions?

• Acknowledgements
  – Sara Dickinson
  – Allison Mankin
  – Willem Toorop
  – getdns team