DNS Privacy

Current State and Development

Tim Wicinski tjw.ietf@gmail.com
IETF Technical Liaison Group

ICANN 61
San Juan, March 2018

Overview

- Problem: Why Internet privacy and DNS Privacy are important (DNS leakage)
- Current state of technical solutions/standards
- Implementation status of current solutions
- Operational deployment
- Future Directions

DNS Privacy

DNS Privacy: Problem

- DNS was designed 30 years ago
  - RFC 1034/1035 1987
- Too much information
  - DNS Requests are sent in the clear
  - The Fully Qualified Domain Name (FQDN) sent to root name servers
- Some requests expose too much
  - DNS Lookup for 'twicinski-laptop.internal.salesforce.com'
  - EDNS Client Subnet

DNS Privacy: History

- July 2013 - "Summer of Snowden"
    - IETF published RFC 7258 (July 2013)

  "Pervasive Monitoring is an attack on Internet users and organizations"

- April 2016 - GDPR Approved
- May 2018 - GDPR Compliance

Technical Standards

Technical Standards: DNSSEC

- RFC 2065 published in March 1999
  - Authentication (or non-existence) of DNS records
- Two Part Deployment
  - Signing of DNS Zones and Records
  - Validation of Signed Zones and Records
- Lacking a "Must Have"
  - DNS Authentication of Named Entities (DANE)

DNSSEC Zone Signing

- Deployment still limited to Internet Infrastructure
- ICANN drives this
- Government Requirements
  - US Government Federal Requirements
  - Germany and Netherlands Regulations
- DNSSEC not always an option
  - Amazon AWS does not deploy
  - DNS Vendors limited support
- Enterprise Adoption at Scale lacking
  - Cloudflare

DNSSEC Validation

- Done at DNS Resolver stage
- Research shows 15% of user population
  - Google DNS ("DNS on at 8's") does
  - Quad 9 ("Now DNS on the 9's!") also
- Peak DNSSEC?
- Business Constituency avoids problem
  - "Behind Firewalls, No One Can See Your Dirty Laundry"

DNS Privacy: Other Work

- DNSCurve
  - Initial interest but no real adoption
- DNSCrypt
  - OpenDNS
- DNSSEC-Trigger
  - Unbound used DNS-over-TLS
- .ONION
  - Defined as Special-Use Name
  - All for an SSL Certificate

Technical Standards: DNS Privacy

- RFC 7816 - DNS Query Name Minimisation (March 2016)
  - Stop sending FQDN to root name servers
  - Great in the GDPR situation
- RFC 7858 - DNS over TLS (May 2016)
  - Uses a different Internet Port (853 instead of 53)
  - TCP Based
  - Lacks the TLS Authentication piece
- DPRIVE Working Group of IETF (September 2014)
  - Focused on this problem

DPRIVE

- Focus on Stepwise Solutions
  - No Ocean Boiling
- DNS Stub Resolver to Recursive Resolver
  - Technical Solution
  - Reveals the most information
- Harder Problem: Recursive to Authoritative
  - Non-Technical Solution
- Tracking Implementations and Usage

Implementation Status

Current Implementation Status

- DNS Privacy Deployment
  - DNS-over-TLS Clients
  - **Trustworthy** DNS-over-TLS Recursive servers
  - Mobile
- DNS-over-TLS Clients/Forwarders
  - Several exist
- DNS-over-TLS Servers
  - Knot/Unbound/Stubby leading the way
- Mobile
  - DNS-over-TLS on Android committed but not released
- See Charts at dnsprivacy.org

Operational Deployment

Operational Deployment: DNS Privacy

- "The sound of an IETF standard that no one uses"
- User Awareness of the issue
- Mobile **will** be the driver for User Community
- Tangible Benefit for Business Constituency
  - Use of Shared Internet Server Infrastructure
- Quad9 only really deployment at scale

Future Directions

Future Directions: DNS Privacy

- GDPR is Happening
- Lots of areas of DNS data leakage
  - EDNS client subnet
  - DNS logs
  - Certificate Transparency

Future Directions: Standards

- Authentication of DNS-over-TLS resolvers
  - Not part of original DNS-over-TLS standard
- DNS-over-HTTPS
  - Middleboxes/China/etc
- DNS-over-QUIC
  - Yet Another Internet Transport
- IETF starting work on resolver to authoritative portion
  - Root servers only part of the solution

Future Directions: Implementations

- Integration into Client Operating Systems
    - Mobile
    - Laptops
- Increased Resolver software deployment
    - Built-in and turned on
    - ...And it can't break anything

Future Directions: Deployment

- ICANN has limited scope in deployment
  - TLDs (and mostly gTLDs)
  - "We Need Bigger Carrots"
- Need to show deployment at scale
  - Tendency to avoid possible traps
  - Look at IPv6 Deployment
- Mobile Clients will drive this