Domain Name System (DNS)

DNS Topics

- Ecosystem
  - You'll notice multiple occurrences of "$"
- Basic Intro (Olaf's slides)
- DNSSEC (Olaf's slides)
- DNSSEC deployment
- DNS privacy

What's the DNS?

- **The** single world-wide distributed database that essentially replaced the host file because that got too big
- Main purpose is to map names to IP addresses
- Also used for many other purposes
  - Mail address right-hand-side to mail server name(s)
  - DNS block lists of spam sources
  - "Passive DNS" for various security purposes
  - Censorship
  - ...

DNS Ecosystem

- The root: “.”
- Top Level Domains (TLDs)
  - Country-code TLDs (ccTLDs): .ie, .uk, .is,...
    - Each more or less do what they want
    - IEDR manage .ie zone, CZ.nic manage .cz, ...
  - Generic TLDs (gTLDs): .com, .org, .net,...
    - Run under ICANN’s oversight (https://icann.org)
    - There are O(1000) of those now (because $$$)
- Second level domains (2LDs)
  - Comply with parental controls (to some extent)
  - Examples: example.com, tcd.ie, amazon.com
  - .com zone has O(100M) names, .ie has O(200k)
- Third level and below: up to 2LD
  - E.g. down.dsg.cs.tcd.ie

Public Suffix List (PSL)

- Some TLDs don't have 2LDs directly below the TLD, e.g. .co.uk, .com.au etc.
- Causes a problem for browsers, when deciding whether to re-tx cookies in HTTP
- Ickky "solution" is the PSL
  - https://publicsuffix.org/
  - Maintained by mozilla and other browser makers
  - A text file with 12,764 lines!
- PSL ideally would be maintained via information in the DNS, but is not, and attempts to do that (IETF DBOUND wg) failed
- Indicative of how DNS can be messy but works despite all

Registry/Registrar/Registrant

- Top Level Domains (TLDs) are operated by registries,
  - IEDR for .ie
  - Affilias operate a whole bunch of ccTLDs and gTLDs
    - https://afilias.info/global-registry-services
  - Public Interest Registry (PIR) operate .org (and feed $$$ to Internet Society, which feeds $$$ to IETF and RFC editor)
- Registrars are accredited by registries and deal with registration of names (and transfer and de-registration)
- Registrant is the entity that wants/has a name registered
  - Per-registry rules may apply, e.g. “connection to Ireland” for .ie
- Registries handle name conflicts, e.g. when trademark issues arise via some dispute resolution process (can involve $$$)
- Registration costs vary from “free” to O($1000), but frequently ($10) per year
  - Some money flows up to registry (ccTLD or gTLD) and to ICANN (for gTLDs)
- ICANN auction new gTLDs now and then
  - Costs O($1M+) to play that game, ICANN have O($150M) resting in account as a result

Registry/Registrar

- Registrar <-> registry protocols vary a lot
  - IEDR have a web console and an “API” that accredited registrars can use
  - Extended Provisionin Protocol (EPP)
  - Registration Data Access Protocol (RDAP)
- whois
  - “Legacy” protocol where registry publishes some registrant data
    - May contain personally identifying information (PII)
  - You can install “whois” on you machine or use via the web
  - Lots of fun with ICANN and whois and GDPR

Olaf’s DNS intro

Olaf’s DNSSEC intro

DNS Root Zone

- The DNS root zone is a speical one that is served by 13 logical servers, operated by different (12) organisations around the world
  - Those are named A-root to M-root
- The root zone is authoritative for the TLDs in the DNS
- Each recursive resolver needs to know (at least one) root zone server address
- IANA (a part of ICANN) maintains the root zone content, which includes addresses for TLD authoritative servers and the root DNSSEC key
  - Resolvers can and do load versions of that locally too sometimes
- Most root server instances are really a cluster of anycast addressable instances, varying between 1 and 150 servers for a total of 446 instances in 2016
  - https://blog.thousandeyes.com/comparing-dns-root-server-performance/
- Other public authoritative and even recursive servers may use anycast for better performance

DNSSEC Deployment

- Dependency on parent (for DS record) makes DNSSEC hard to deploy
- Should registrar or registrant contact parent?
- If registrar, how does zone get signed, or, how does DS/KSK get to registrar? (usually via a crappy web form)
- If registrant, how does registry know it's dealing with the right party (registrant has a/c at registrar, not registry)
- There are also issues with stubs and recursives that don't handle DNSSEC well, or who even strip DNSSEC RRs (typical middlebox issue!)
- There was also lots of delay getting the root zone signed (only happened in 2010)
- Some zone maintainers (say they) cannot sign their zones due to lack of control over names
- Some zone maintainers claim that DNSSEC isn't worthwhile for them
  - But: pentesters may like DNSSEC and some malware distribution vectors can be blocked if DNSSEC is deployed

DNSSEC Deployment

- Result: ~1% of 2LDs signed, maybe 3% of names covered
- Some stats: https://www.statdns.com/
- More stats: https://stats.dnssec-tools.org/
- “Economic incentives on DNSSEC deployment: time to move from quantity to quality”
  - https://ieeexplore.ieee.org/abstract/document/8406223/
  - https://research.tue.nl/en/publications/economic-incentives-on-dnssec-deployment-time-to-move-from-quanti

DNSSEC Deployment

- CDS/CDNSKEY (RFC 8078) provides a way for zone maintainer to publish a “new” DS (CDS) or new KSK (CDKSKEY) in their zone
  - Parent scans children (who are known to do this) and can pick up new DS value that can be used to populate parent zone file (if various conditions met)
  - Hasn’t seen much deployment yet, but should help with ongoing maintainance, allowing much easier changes to KSKs
- Some TLDs are also incentivising registrars (via discounts of maybe 10% of $) to deploy DNSSEC for new domains
  - Leads to more deployment, not clear if more security

DNS Privacy

- All data published in DNS is public, so there was little/no interest in confidentiality when DNSSEC was defined
- But the fact of access to DNS data can be sensitive, e.g. if you access https://www.aa.org/ that may say something about your life
- RFC7626 is a problem statement for DNS privacy
  - Names, timing, IP addresses (e.g. if local recursive), client-subnet
- Mitigations:
  - Use Tor browser bundle
  - QNAME minimisation (RFC7816)
  - Define ways to provide confidentiality for DNS traffic
  - Don’t (always) send EDNS(0) client subnet

DNS over TLS (DoT)

- IETF “DPRIVE” working group has defined how to run DNS over TLS (DoT, RFC7858)
- DoT is usable today between stub and recursive
- Generally, you’d replace your system stub resolver (e.g. dnsmasq) with something that can do DoT (e.g. stubby)
  - https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Daemon+-+Stubby
- There are recursives now who offer that kind of “DNS privacy service”, e.g. 9.9.9.9, 1.1.1.1, ...

DoT with padding

- DNS query or answer lengths may leak information about names
- RFC 7830 describes an EDNS(0) padding option
- Responders MUST pad if requesters do (and MAY in any case)
- RFC8467 describes ways in which one might use padding and recommends:
  - Pad queries to block lengths of N x 128 octets
  - Pad responses to block lengths of N x 468 octets
  - Don’t do random stuff (signal leaks), maximal-length is wasteful (esp if we go > MTU)

Recursive <->Authoritative

- Today, DoT is usable for stub <-> recusive
- Would like to also secure recursive <-> authoritative
- Can’t amortise TLS state so much so needs lots of performance testing, esp., if done near root
- Not clear if/how to authenticate authoritative (various proposal being considered)
- Might get deployed in medium term, but not clear

DNS over HTTPS (DoH)

- Browsers and some JS code however can't easily tell if DoT is being used
- So DNS over HTTPS (DoH, RFC8484) describes how to encapsulate DNS traffic in HTTPS
- Supported today in FF nightly with their "Trusted Recursive Resolver" (TRR) concept, with exactly one TRR instance (Cloudflare)
- Has lead to a **major** fuss – the move from a system/OS stub, to an in-browser stub causes many changes and people fear/dislike such changes

Anti-DoH!

- Various operator-like folks have described issues with DoH (or more correctly with the mozilla/CF deployment that may eventually happen)
  - https://tools.ietf.org/html/draft-bertola-bcp-doh-clients
  - https://tools.ietf.org/html/draft-reid-doh-operator
  - https://tools.ietf.org/html/draft-livingood-doh-implementation-risks-issues
- None of those are objective analyses, but work will likely happen to do that analysis, because there are some real issues (if DoH gets widely deployed in applications):
  - Split horizon
  - Loss of enterprise control for BYOD
  - Passive DNS
- Mozilla statements on their TRR plans:
  - https://mailarchive.ietf.org/arch/msg/doh/po6GCAJ52BAKuyL-dZiU91v6hLw
  - https://wiki.mozilla.org/Security/DOH-resolver-policy

DNS Privacy enables ESNI

- Once/if we get deployment of DNS privacy (whether via DoT or DoH) then we can try to tackle SNI encryption as part of the TLS handshake
  - https://tools.ietf.org/html/draft-ietf-tls-esni
- Idea: publish a new DH public share in DNS (ESNIKeys RR) and use that to encrypt SNI in the TLS ClientHello
- Issue: multi-CDN switching causes possible mismatch between A/AAAA and ESNIKeys
  - Needs more testing to find out how big a deal this may be (currently: seems a non-deal for clients, but a sometimes-major deal for web sites when/if switching CDN)
- Current CDN-friendly proposal: include A/AAAA values inside the ESNIKeys RR structure!
  - If that lasts, there'll be an even bigger fuss with operators:-)
  - Personally: I'd prefer ESNIKeys contain prefixes but not full /32's or /128's to remove duplication, test results will be interesting

DNS Conclusions

- DNS is sort-of criticial infrastructure that (sometimes amazingly) works well
- DNSSEC deployment is currently woeful
  - Contrast with DKIM
- DNS privacy is starting to be addressed but in the presence of real tussles