PRIVACY IN THE DNS: FOR BETTER OR WORSE

Dr. Guillaume-Jean Herbiet
Fondation RESTENA / dns.lu
Data Privacy Day 2019

.lu dns
Service opéré par la Fondation RESTENA
DNS LUXEMBOURG

FONDATION RESTENA AND DNS.LU

- Not-for-profit
- **NREN** for Luxembourg:
  - Higher-education and research network
  - Mail, web hosting
  - Interconnection with GEANT network
- Technical operator **LU-CIX** (Commercial Internet Exchange)
- **CSIRT**: security contact point for the Higher-ed community
- The **registry** for `.lu` domain names
- A **registrar** for `.lu` domain names

Guillaume-Jean Herbiet `<gjherbiet@restena.lu>`
System Engineer

A WORD ABOUT WHOIS AND GDPR

- As a registry, we maintain **WHOIS** for **.lu**
  - public database about domain owners and contacts
    - definitely private information (name, address, ...)
  - ➤ Requirement for cc-TLD delegation by ICANN

- **GDPR impacted all EU cc-TLD operators**
  - different approaches: from all to nothing!
  - **.lu**: personal data is still collected but not public any more

- ICANN is **still discussing a globally applicable model**
  - competing interests: privacy advocates, IP, security analysts

not all TLDs are equal, so chose wisely!

A DEFINITION FOR PRIVACY FROM THE STANDARDS

- RFC 4949 (2007): **Internet Security Glossary, Version 2**
  - *"The **right** of an entity (normally a person)[..] to **determine the degree** to which it [..] is willing to **share** its **personal information** with others."*

- ISO/IEC 7498-2 (1989) : **Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture**
  - *"The **right** of individuals to **control or influence** what **information related to them** may be **collected and stored** and **by whom and to whom** that information **may be disclosed**."*

I shall decide about my data!

THE RATIONALE FOR DOMAIN NAMES AND THE DNS

- The Internet uses **IP addresses** as **technical identifiers**
- Humans prefer unique, memorable **functional identifiers**
  - Would you remember `2a03:2880:f11c:8183:face:b00c::25de` or `www.facebook.com`?
- Domain names are more than functional identifiers:
  - **commercial**: identity vector, brand names
  - **political**: access control to information resources
- **Today's Internet simply wouldn't work without the DNS!**
  - Cloud providers and Content Delivery Networks
    - performance optimisation and fault-tolerance
  - Security certificates use domain names
  - Spam filtering heavily relies on the DNS

The DNS is an **ubiquitous infrastructure technology**

A TENTATIVE DEFINITION OF THE DNS

- The **Domain Name System** is a **distributed database**:
  - **domain name** = query entry-point (*where?*)
  - **query type** = nature of the requested data (*what?*)
    - IP address, mail server, services, certificates, crypto keys, text, ...
- Distribution is achieved using **hierarchical delegation**:
  - from the **root** to the leftmost part of the domain name
  - only have info about the zone you manage (e.g. `.lu`)
  - addresses of the servers managing the below zones (e.g. `uni.lu`, `etat.lu`, ...)

Finding data requires a **recursive resolution** process

RECURSIVE RESOLUTION

www.rtl.lu

1 to 100 ms

x10 to x100/page

?

81.92.238.46

root

Delegation

.lu

Delegation

.rtl

Authoritative DNS servers

root hints

1 IP of www.rtl.lu?

2 IP of www.rtl.lu?

3 IP of .lu DNS servers

4 IP of www.rtl.lu?

5 IP of .lu DNS servers

6 IP of www.rtl.lu?

7 81.92.238.46

8 81.92.238.46

Recursive resolver

DNS PRIVACY THREATS

- **The DNS was designed in a pre-Snowden era**
  - all data is sent in clear-text (eavesdropping)
  - using a connection-less transport protocol (spoofing)
  - without a guarantee on data authenticity (hijacking)
  - meta-data and traffic patterns (identification and profiling)
  - **DNS is often overlooked, so are its security/privacy implications...**

- **The recursive resolver is the cornerstone of the resolution**
  - sees all queries + IP address of the client
  - configured automatically (**by default**):
    - **local network** (corp., univ.): company/school rules
    - **Internet provider** (home): GDPR/Telco rules apply in EU
  - configured manually:
    - **big names** (Google, Cloudflare, ...): privacy policies vary; trust
    - **privacy advocates** (FFDN, CCC): "no log" policy; still trust
    - **local** (on your device): technical knowledge required

IMPROVING DNS SECURITY AND PRIVACY

- **DNSSEC** (2005) introduced zone/replies **signing**:
  - still not widely deployed : 1% of `.com`/`.net`, none in top 20...
  - only provides integrity, not privacy

- **Post-Snowden revelations awakening**
  - "Pervasive Monitoring is an attack" (RFC 7258, 2014):
    - *"Pervasive Monitoring Is a Widespread Attack on Privacy"*
  - DPRIVE WG (2014) formed to improve DNS privacy
    - QNAME minimisation (RFC 7816, 2016)
    - Add an encryption layer to DNS communications:
      - **DNS-over-TLS** (RFC 7858, 2016)
      - **DNS-over-HTTPS** (RFC 8484, 2018)

Focus on the **client to resolver** privacy

DNS-OVER-TLS (DOT)

- **"Simple" encapsulation** of DNS in a TLS tunnel
  - **opportunistic mode**: prevents pervasive monitoring
  - **strict mode** (PKI, DANE): prevents interception

- Uses a **dedicated port** (843/tcp) that can be blocked
  - 443/tcp can be a fallback, but not standard

- **Increasing implementation**:
  - servers: available in all major software + public resolvers
  - clients: additional (stubby) or native (Android Pie)

- **Maintains the traditional DNS architecture**:
  - resolver configuration at system level/system wide
  - assignment via DHCP or user manual configuration

Good ol' DNS with encryption on top

DNS-OVER-HTTPS (DOH)

- Promoted by browser editors, **web-oriented**:
  - (DNS binary format or JSON) + HTTP headers !
  - push mode, sandboxing, pipelining (HTTP/2, QUIC = HTTP/3)

- ***"Everything over port 443"*** approach

- **In-browser implementation** = no system-wide configuration
  - resolver choice is constrained by browser editor
  - configuration option (when existing) is complex to achieve
  - in the future: mandatory for "apps"?

- **Paradigm shift**: "Trusted Recursive Resolver"
  - **Concentration** to a handful of providers **by default**
  - Trust the resolver over the zone owner (DNSSEC deprecation?)

DNS as a new silo for web "giants"

CONCLUSION

- DNS is by design a **decentralised solution**
  - with a **decentralised trust model** (DNSSEC)

- DNS was added a **privacy layer = TLS encryption**
  - client to resolver only
  - reinforces the key role of the **recursive resolver**

- **Privacy solutions may lead to concentration**
  - constrained choice of handful of trusted resolvers
  - run by "big names", **distant** from the end-user

- This is probably not what we want for privacy...

We want our choice back!

WANT TO INCREASE YOUR DNS PRIVACY?

https://dnsprivacy.org

Servers run by the Stubby developers

Hosted by	IP addresses	TLS Ports	Hostname for TLS authentication	Base 64 encoded form of SPKI pin(s) for TLS authentication (RFC7858)	TLSA record published	Logging	Software	Notes
1) The following are currently enabled in the default Stubby config file because they are run by the stubby/getdns developers and have no known issues.								
Surfnet	145.100.185.15 2001:610:1:40ba:145:100:185:15	853 443	dnsovertls.sinodun.com	62lKu9HsDVbyiPenApnc4sfmSYTHOVfFgL3pyB+cBL4=	Y	Traffic volume only	HAProxy + BIND 9.12	
Surfnet	145.100.185.16 2001:610:1:40ba:145:100:185:16	853 443	dnsovertls1.sinodun.com	cE2ecALeE5B+urJhDrJlVFmf38cJLAvqekONvjvpqUA=	Y	Traffic volume only	Nginx + BIND 9.12	
getdnsapi.net	185.49.141.37 2a04:b900:0:100::37	853	getdnsapi.net	foxZRnIh9gZpWnI+zEiKa0EJ2rdCGroMWm02gaxSc9S=	Y	Traffic volume only	Unbound	

Other servers with a 'no logging' policy

Hosted by	IP addresses	TLS Ports	Hostname for TLS authentication	Base 64 encoded form of SPKI pin(s) for TLS authentication (RFC7858)	TLSA record published	Logging	Software	Notes
UncensoredDNS	89.233.43.71	853	unicast.censurfridns.dk	wikE3jYAA6jQmXYTr/rbHeEPmC78dQwZbQp6WdrseEs=	Y	Traffic		See https://blog.uncensoreddns.org/
Fondation RESTENA (NREN for Luxemburg)	158.64.1.29 2001:a18:1::29	853	kaitain.restena.lu	Traffic volume only	Unbound	Configured with qname-minimisation, use-caps-for-id, aggressive-nsec, prefetch, harden-below-nxdomain and the newest auth-zone for local root zone caching.		
						only	9.12	see here for details.
Surfnet	145.100.185.17 2001:610:1:40ba:145:100:185:17	853	dnsovertls2.sinodun.com	NAXBESvpjZMnPWQcrxa2KFIkHV/pDEIjRkA3hLWogSg=	Y	Traffic volume	Knot Resolver	
dkg								e that on e both ccess n TLS LS on separate TLS connections due to some nifty, experimental demultiplexing of traffic, described here.Has some issues with DNSSEC responses - this is under investigation.

+ DNS-over-TLS on RESTENA "community" resolvers (automatically configured at relevant locations)

.lu dns

Service opéré
par la Fondation RESTENA
DNS LUXEMBOURG

QUESTIONS ? DISCUSSION. FEEDBACK!

Thank you