DNS over HTTPS & DNS over TLS

Barry Leiba / Suzanne Woolf | ICANN67 | March 2020

Agenda

1 SSAC Overview

2 Overview of SAC1XX: Implications of DoH & DoT

3 Comparisons of the Technologies

4 Perspectives on DoH & DoT

5 Implications to the Namespace

6 Q & A

Security and Stability Advisory Committee (SSAC)

Who We Are

- **34** Members
- Appointed by the ICANN Board

What We Do

Role: Advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.

What is Our Expertise

- Addressing and Routing
- Domain Name System (DNS)
- DNS Security Extensions (DNSSEC)
- Domain Registry/Registrar Operations
- DNS Abuse & Cybercrime
- Internationalization (Domain Names and Data)
- Internet Service/Access Provider
- ICANN Policy and Operations

How We Advise

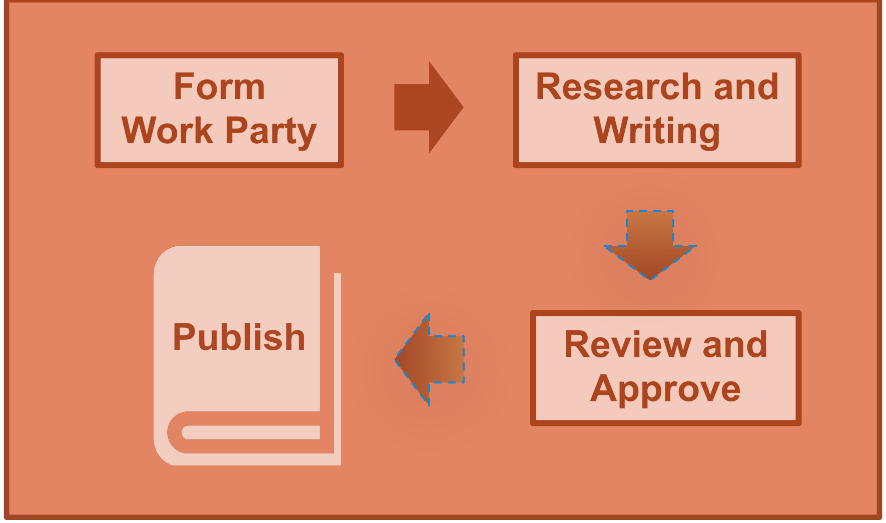
108 Publications since 2002

Security and Stability Advisory Committee (SSAC)

ICANN's Mission & Commitments

- To ensure the stable and secure operation of the Internet's unique identifier systems.
- Preserving and enhancing the operational stability, reliability, security and global interoperability, resilience, and openness of the DNS and the Internet.

SSAC Publication Process



Form Work Party

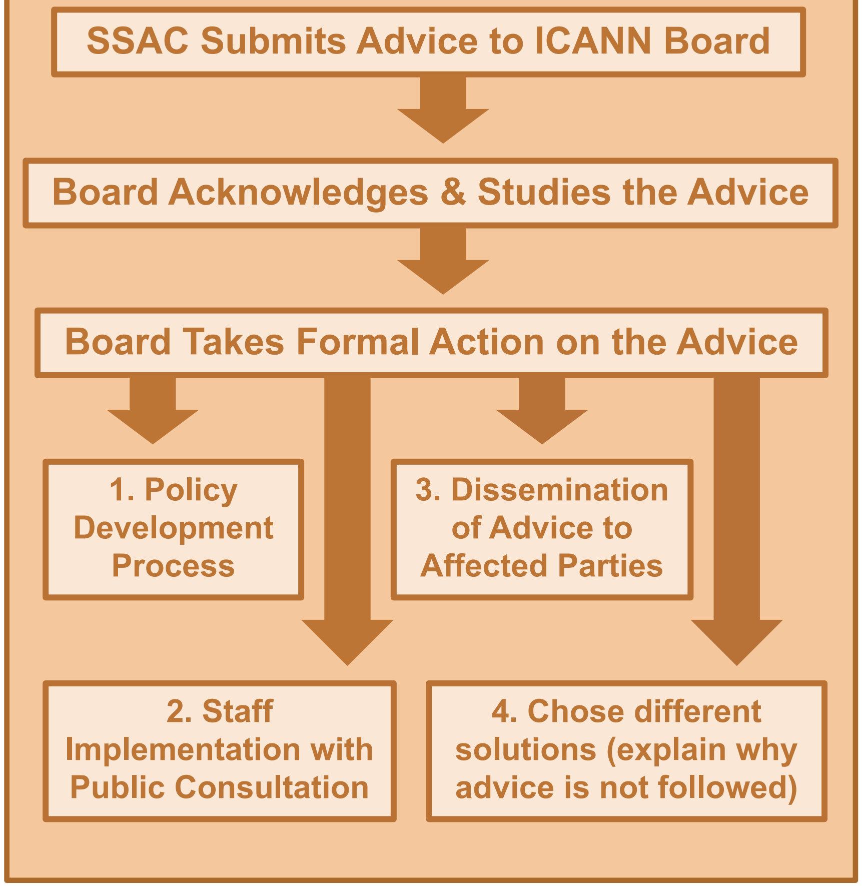
Research and Writing

Review and Approve

Publish

Consideration of SSAC Advice

(to the ICANN Board)



SSAC Submits Advice to ICANN Board

Board Acknowledges & Studies the Advice

Board Takes Formal Action on the Advice

1. Policy Development Process

2. Staff Implementation with Public Consultation

3. Dissemination of Advice to Affected Parties

4. Chose different solutions (explain why advice is not followed)

SAC1XX: The Implications of DNS over HTTPS and DNS over TLS

SAC1XX: Implications of DNS over HTTPS and DNS over TLS

- Explanation and comparison of DNS over HTTPS (DoH) and DNS over TLS (DoT), focusing on the standardization and deployment status
- Exploration of the effects on and perspectives of several different groups of stakeholders: parents, enterprise network managers, dissidents and protesters, and Internet service providers
- Examination of application resolver choice and what implications arise from these decisions
- Potential implications on the namespace due to DNS stub resolution moving to applications

SAC1XX: What NOT to expect

- Declaration of universally agreed-upon “right” and “wrong” labels with respect to DoH and DoT, their implementation, and deployment choices
- Strong statements such as, “More privacy is always better,” or “More encryption is always better”
- Strong statements about trust models that we cannot all all agree with, because we all have different perspectives
- Recommendations to the ICANN Board

SAC1XX: Conclusions

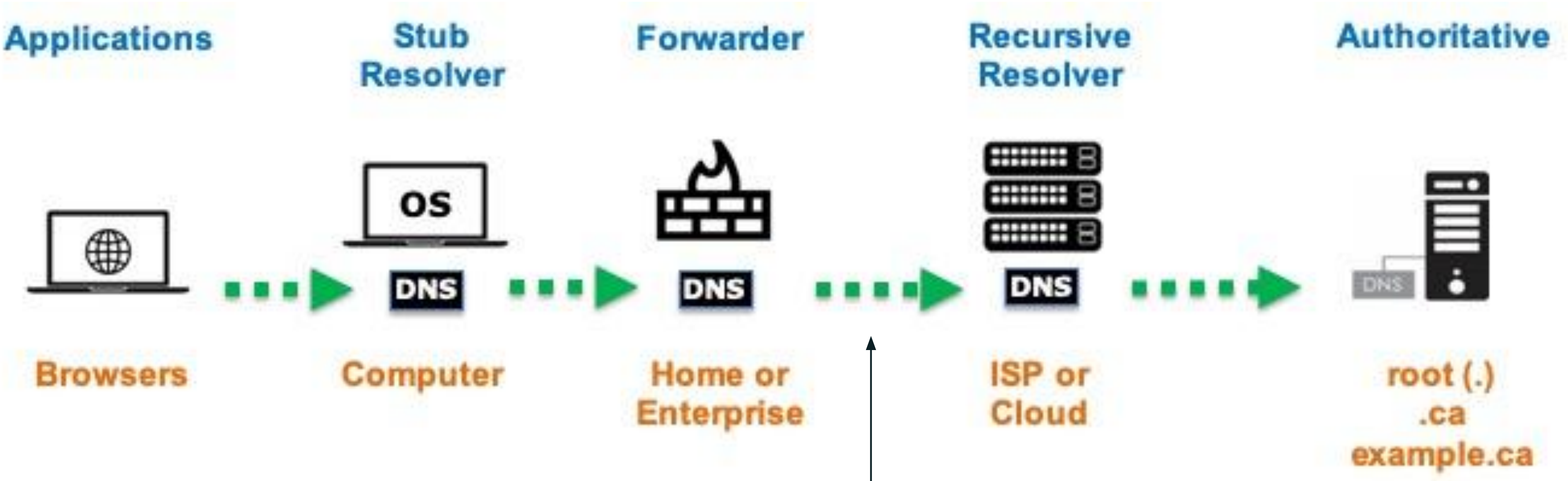
- Evaluations of DoH or DoT rely on the perspective of the evaluator.
  - How they are implemented, how they are deployed, what default settings are configured, and who uses them, are the questions that this report focuses on.
- Regardless of perspective, the deployment of DoT and DoH will be disruptive, mainly in the implementation and deployment of the technology.
- Application-specific DNS resolution via DoH and DoT presents a host of challenges:
  - How networks and endpoints work.
  - Who has access to DNS query data.
  - How to protect and manage networks in this new model.

Comparison of DNS over HTTPS and DNS over TLS

Three Technologies

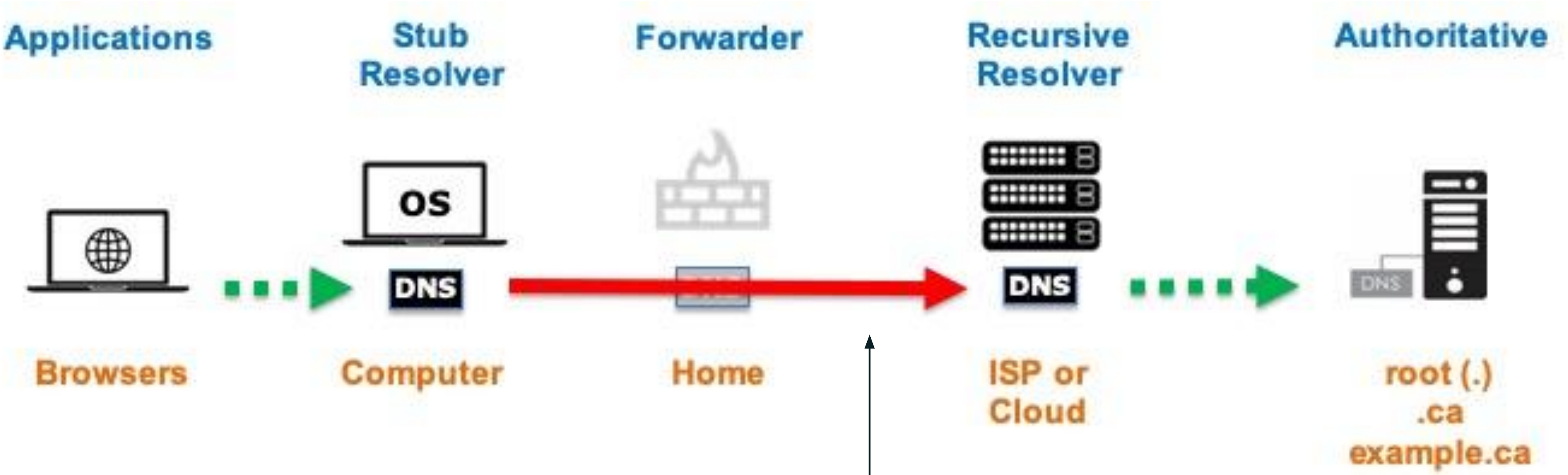
- Traditional DNS
  - Unencrypted transport using UDP / TCP port 53
- DNS over HTTPS
  - Encrypted transport of DNS traffic over Secure Hyper Text Transfer Protocol (HTTPS)
  - Uses TCP port 443, the same as other HTTPS traffic
  - Only used for stub to recursive queries
- DNS over TLS
  - Encrypted transport of DNS queries over Transport Layer Security (TLS)
  - Uses TCP port 853, unique port reserved for this purpose
  - Only used for stub to recursive queries

Possible Traditional DNS Deployment



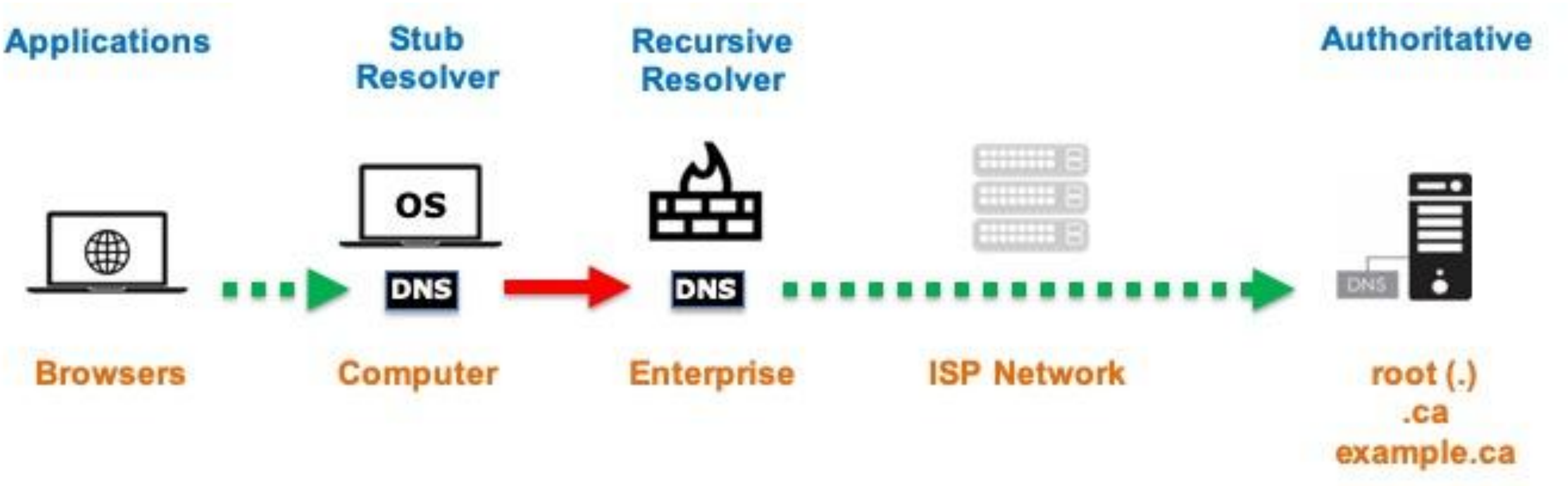
(green dashes show unencrypted paths)

Possible DNS over TLS Deployment in a Home Network

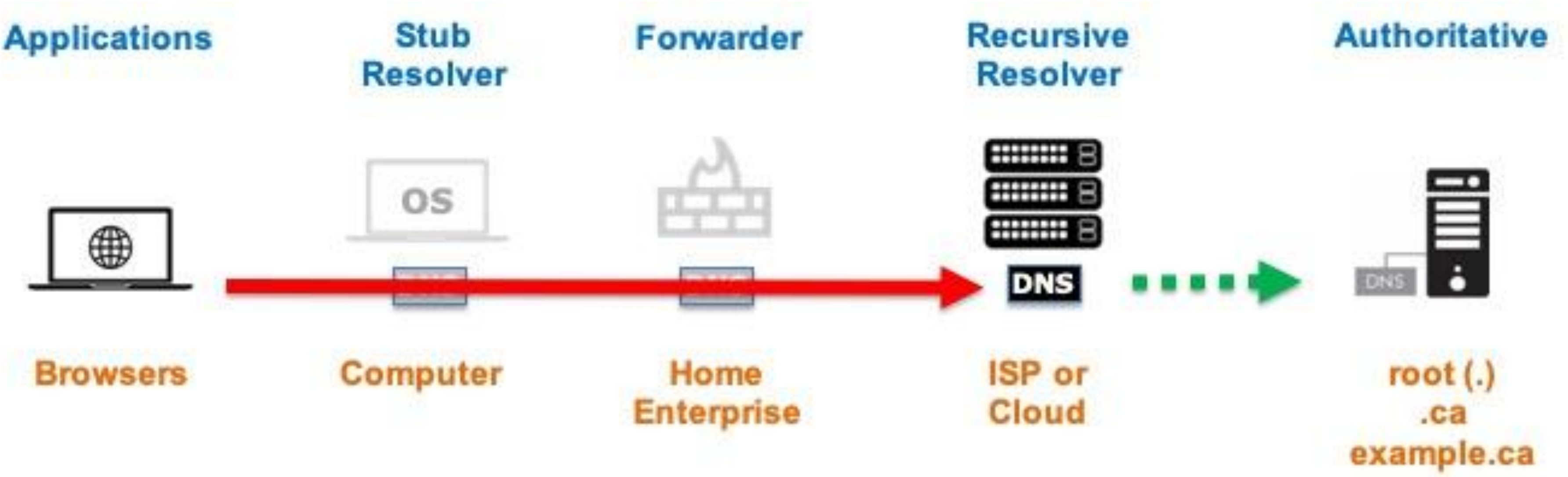


(red solids show encrypted paths)

Possible DNS over TLS Deployment in an Enterprise Network



Possible DNS over HTTPS Deployment



Different Perspectives on DNS over HTTPS and DNS over TLS

Parents

- Some parents may wish to control their children’s access to the Internet, and the DNS can be an effective control point for this.
- Services have always existed to provide this type of blocking.
- Just as children have often been skilled enough to work around them.
- DoH will make this kind of blocking more difficult.

Enterprise Network Managers

- Many different types of organizations can be considered enterprise networks:
    - corporations, municipalities, university campuses, hospitals, military bases
- Often have a positive obligation to understand and control the traffic on their networks for regulatory or security reasons.
- DNS is an important control point for enterprise network control.
- The introduction of new DNS transports, and DoH in particular, threatens to upend this model of network control and management.

Dissidents, Protesters, and Others

- The Internet is an important vehicle for dissidents and protesters to spread alternative views, critique politics, and shed light on corruption and human rights abuses.
- By encrypting DNS queries and resolution, DoH and DoT can help shield users from being tracked by their ISPs or governments.
- There has always been Virtual Private Network (VPN) software, and ToR.
- Not a panacea. Even with DoH or DoT, the ability of citizens to express political dissent without reprisal is greatly influenced by their governments.

Internet Service Providers (ISPs)

- Many governments obligate ISPs to block traffic using DNS as a control point.
- The introduction of DoH and DoT may mean that ISPs now become obligated to block traffic using other means.
- Some ISPs may resort to blocking all DoT traffic or offer their own DoH or DoT services.
- ISPs may blacklist known DoH servers based on known IP addresses, but this will not work 100%.

Implications to the Namespace

Implications to the Namespace

- Applications performing DNS functions themselves may cause other disruptions which may or may not be visible to users of those applications.
- One industry concern with respect to applications providing DNS functionality is that they will undermine the usefulness of DNS as a generic, protocol-neutral naming system for the Internet.
- Namespaces may become tailored to the requirements of a particular application.
- Web browsers have begun to cache web content per-origin.
    - In practice, this means each browser tab now has its own cached versions of content.

Thank you