DNS-over-HTTPS and DNS-over-TLS

SSAC & ccNSO | ICANN65 | June 2019

Agenda

1. Session Goals and Introductions
2. Technical Overview
3. Q & A
4. Potential Deployment Concerns
5. Q & A
6. Panel Discussion on Deployment Considerations

Session Goals and Introductions

- **Goals of this session**
  - Clarify DoH and DoT for a non-technical audience
  - Discuss deployment concerns with the community

- **Chairperson:** Alejandra Reynoso
- **Presenters:** Danny McPherson, Peter Koch
- **Moderators:** Barry Leiba, Alyssa Moore
- **Panelists:** Tim April, Vittorio Bertola, Michele Neylon

Technical Overview

Danny McPherson

Technical Overview

- DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) are two new protocols for transporting DNS data
- Both protocols support encrypting DNS data in transport
  - Traditional DNS queries and responses are unencrypted
- DNS data integrity is unrelated to DoH and DoT
  - The need for DNSSEC has not changed
- Standardization on how DoH and DoT resolvers are configured in applications and operating systems is still ongoing
  - DoH and DoT implementations are still developing and current deployments are limited

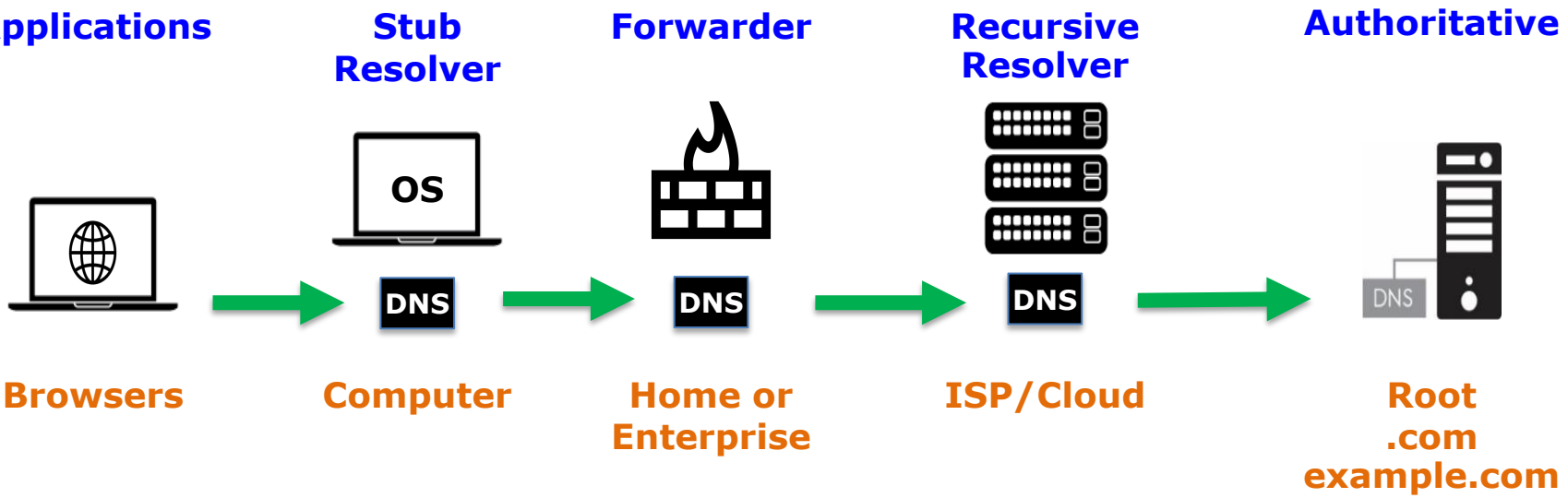
Why DoH / DoT ?

- Traditional DNS transport is unencrypted
  - Can cause users to leak confidential information (surveillance)
  - DNS responses can be tampered with (censorship)
- DoH and DoT provide channel **confidentiality** while DNSSEC provides response **integrity** when validation is performed
- Technologies such as QNAME Minimization may also be effective at preserving user privacy

Traditional DNS

- Resolution path has changed little since the dawn of the Internet
- Queries and Responses sent in plaintext (unencrypted)
- Operating system stub cannot authenticate the resolver
- RFC 1034 and RFC 1035

Traditional DNS



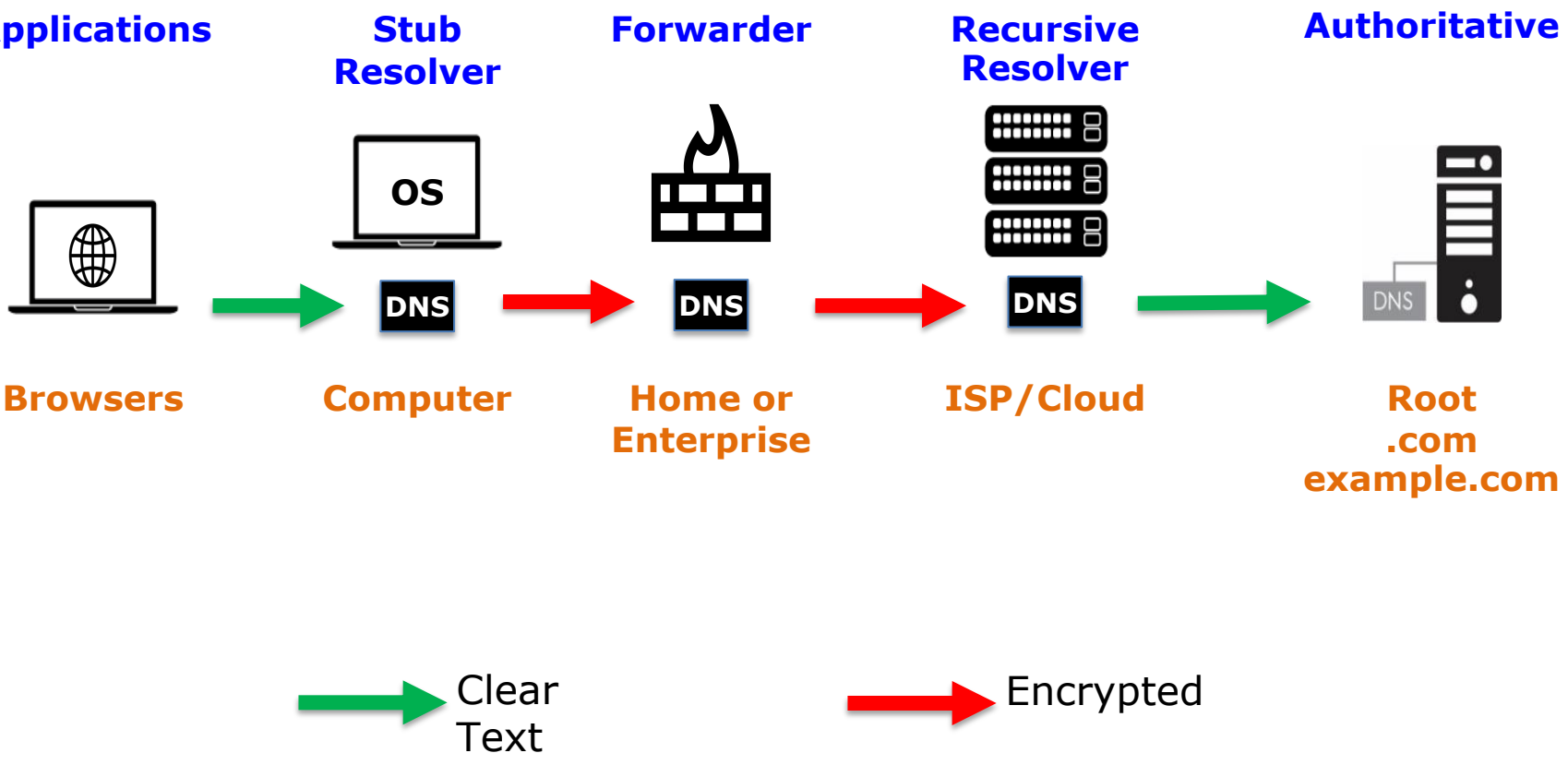
Clear Text

Encrypted

DNS-over-TLS (DoT)

- Uses Transport Layer Security (TLS) for DNS queries and responses
- All traffic is encrypted between the stub and recursive resolver
- Stub able to authenticate the resolver
- Requires support in stub and recursive resolver
- RFC 7858 and RFC 8310

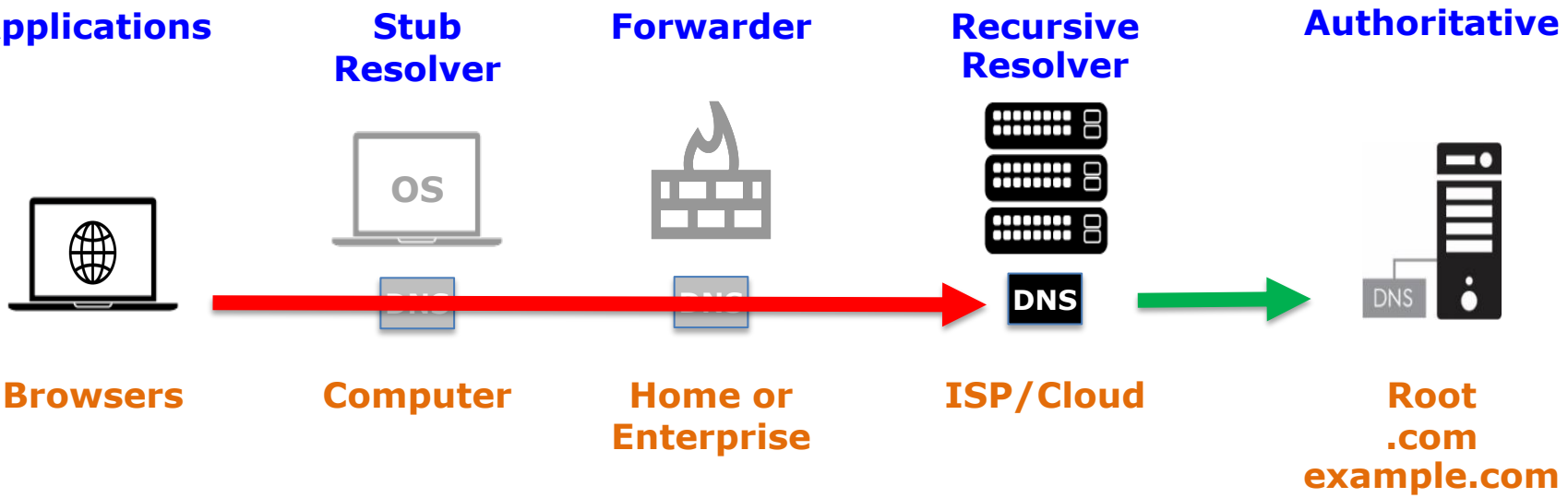
DNS over TLS (DoT) Possible Deployment



DNS-over-HTTPS (DoH)

- Uses the Hypertext Transfer Protocol Secure (HTTPS) protocol for DNS queries and responses
- All traffic is encrypted between the application and recursive resolver, bypassing the operating system stub
- Application able to authenticate the resolver
- Requires support in application and recursive resolver
- RFC 8484

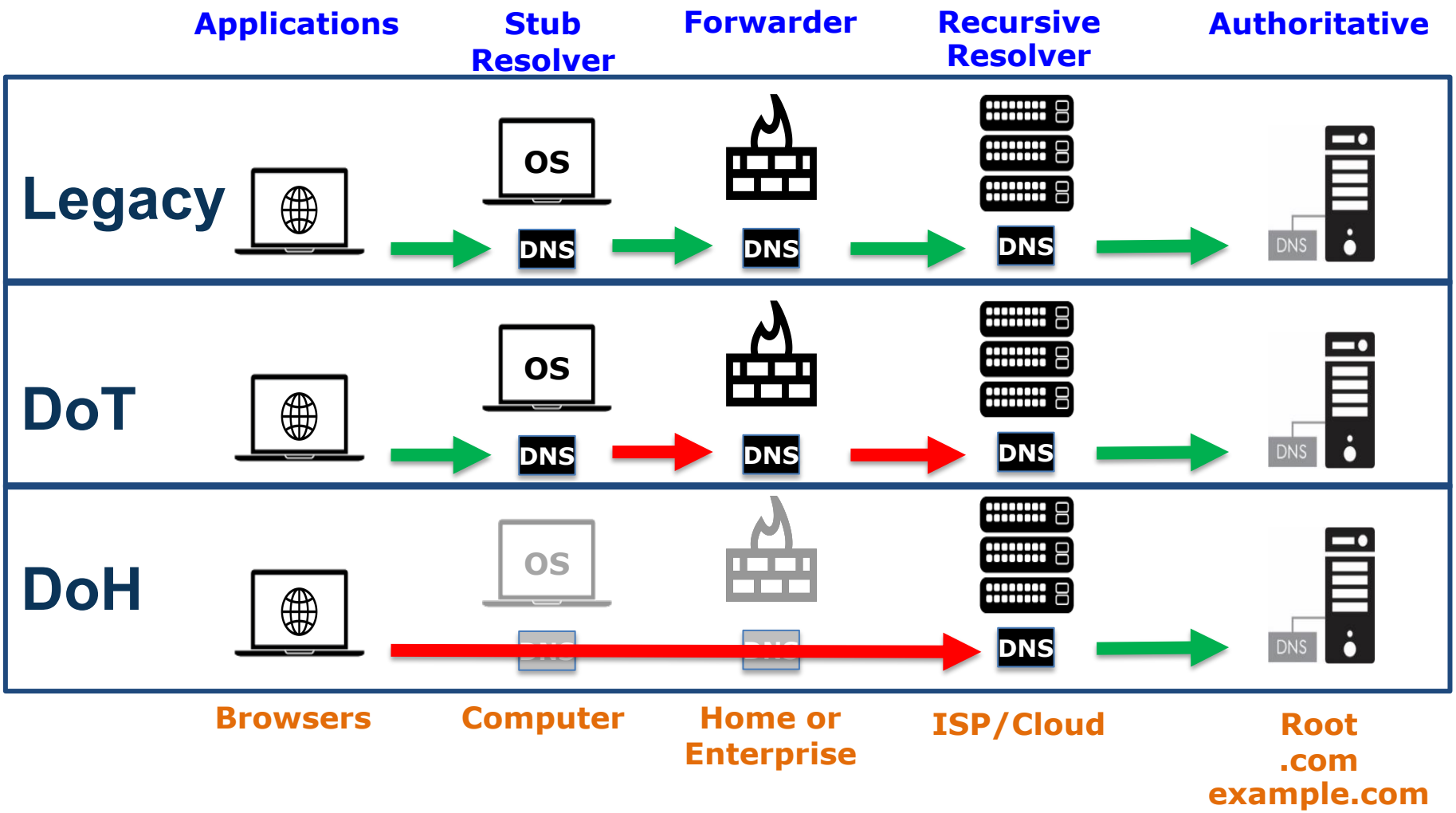
DNS over HTTPS (DoH) Possible Deployment



Clear Text

Encrypted

Q & A

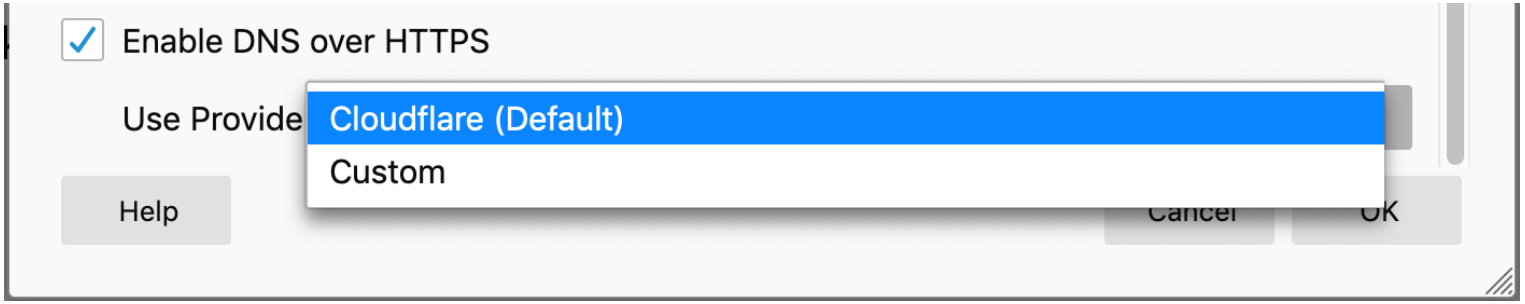

Applications
Stub Resolver
Forwarder
Recursive Resolver
Authoritative
Legacy
DoT
DoH
OS
DNS
Browsers
Computer
Home or Enterprise
ISP/Cloud
Root
.com
example.com

Potential Deployment Concerns

Peter Koch

Potential Deployment Concerns of DoT/DoH

- Standardization around how DoT and DoH will be deployed is still in development
  - Currently there is no standard way for an application to learn which resolvers support DoH, and therefore, which resolver can be used
  - Automatic configuration (e.g., DHCP, IPv6 RA) has typically been used by network managers to determine which DNS servers are learned by the operating system
  - There have always been some users who manually configured DNS servers for their operating system
- One web browser enabled for DoH contains a hardcoded URL for DoH resolvers that overrides the operating system's configured resolvers
  - Bypassing the operating system's configured resolver for web browser DNS lookups
  - This can interfere with how some network managers deploy DNS security



Potential Deployment Concerns of DoT/DoH (cont)

- DoT and DoH may make it harder to distinguish DNS queries from other traffic
  - DoH cannot be blocked without blocking other important HTTPS traffic
  - It may be possible to masquerade DoT traffic as generic TLS traffic, but further research is needed
- Network managers may be unable to block DoH traffic without decrypting all HTTPS traffic
  - Interferes with popular information security practices
  - Can interfere with regulatory requirements in some jurisdictions
  - This kind of blocking has never been perfect (e.g., VPNs, BYOD)
- Masquerading DNS queries as generic HTTPS may help users circumvent DNS based filtering (e.g., censorship, blocking malware)

Policy Questions - The Bigger Picture

- DoH does not prescribe a certain deployment model
- … but we can observe developments towards concentration/consolidation
- DNS name resolution used to be highly decentralized
- DNS name resolution “as a service“ appeared prior to DoH
  - the "quads": 1.1.1.1, 8.8.8.8, 9.9.9.9, …
- This in addition to choice of resolution path per application, rather than per system/ISP/enterprise, leads to increased concentration of (increasingly "large") resolvers

Policy Questions - The Bigger Picture

- DoH and DoT provide privacy on the wire
- DNS Resolvers still see users‘ requests, at varying levels of detail
  - still not reliably able to identify individuals
- DNS Resolver Policy (what happens to the query data?)
- NB: some scenarios depend on optimizing network traffic by giving different responses based on knowledge of the users‘ "location" (but that‘s not in the original DNS textbook)

Policy Questions - DoH Resolvers

- How to select DoH Resolvers?
- How to hold operators of DoH resolvers accountable?
- Who determines which policies are acceptable?

Policy Questions - The Namespace

- Assume a group of (cooperating) DoH Resolution Providers
- Further assume a dominant Internet service
  - For example, the Web
- Interest in additional name resolution paths
  - For example, .onion
- Who would be in a position to practically open the new paths?
- What would that mean for ICANN‘s role with regards to the DNS root zone?

Conclusions

- Some potential deployments of DoH and DoT may impact traditional policy control points in DNS resolution
- Standardization on how DoH and DoT resolvers are configured in applications and operating systems is still ongoing
- For registry and registrar operators there is **currently** little impact from DoH and DoT
- It is **too early** to say what the impact of DoH and DoT on users will be
- The need for DNSSEC and QNAME Minimization has not changed

Q&A

Panel Discussion on Deployment Considerations

Questions to the Audience

- Do you foresee any impact from deploying DoH and/or DoT on your operations?
- Are there any issues with DoH / DoT that fall within ICANN's mission?
- How do you think DoH should be implemented in applications such as web browsers?
- What concerns do you have about DoH and/or DoT?

- The IETF has been discussing these topics extensively on the <add@ietf.org> mailing list
- At the upcoming IETF 105 meeting in Montreal, there will be a related Birds-of-a-Feather session

Thank you