A Balanced DNS Information Protection Strategy: Minimize at Root and TLD, Encrypt When Needed Elsewhere

ICANN-70 DNSSEC Workshop

March 24, 2021

Scott Hollenbeck <shollenbeck@verisign.com>

Burt Kaliski <bkaliski@verisign.com>

VERISIGN

Overview

The Domain Name System (DNS) protocol is in a new era of change, with increasing focus on confidentiality protections

Different approaches, including DNS encryption and minimization techniques, fit different parts of the DNS ecosystem

Verisign's recommendation: "Minimize at root and TLD, encrypt when needed elsewhere"

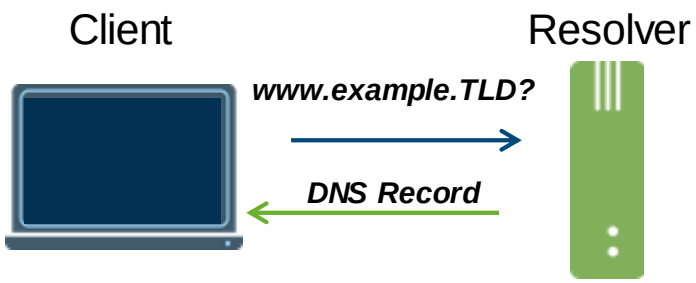
Factoring in Operational Risk

Protocol changes, such as DNS encryption, create new operational challenges, expand the attack surface, and impair DNS monitoring and protection services

Name server availability affects navigation to the entire DNS hierarchy below it

Disclosure risk must be balanced with operational risk

Client-to-Resolver



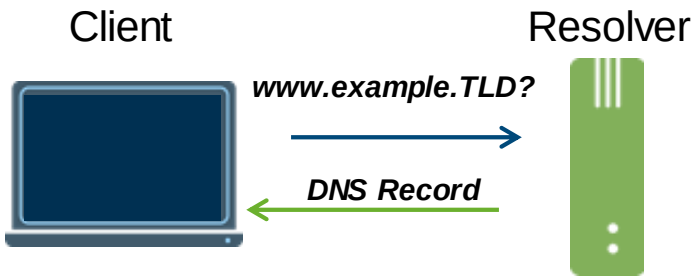
Client-to-Resolver

Client-specific information, by definition

Full domain names

All domain names of interest to client, if only one resolver

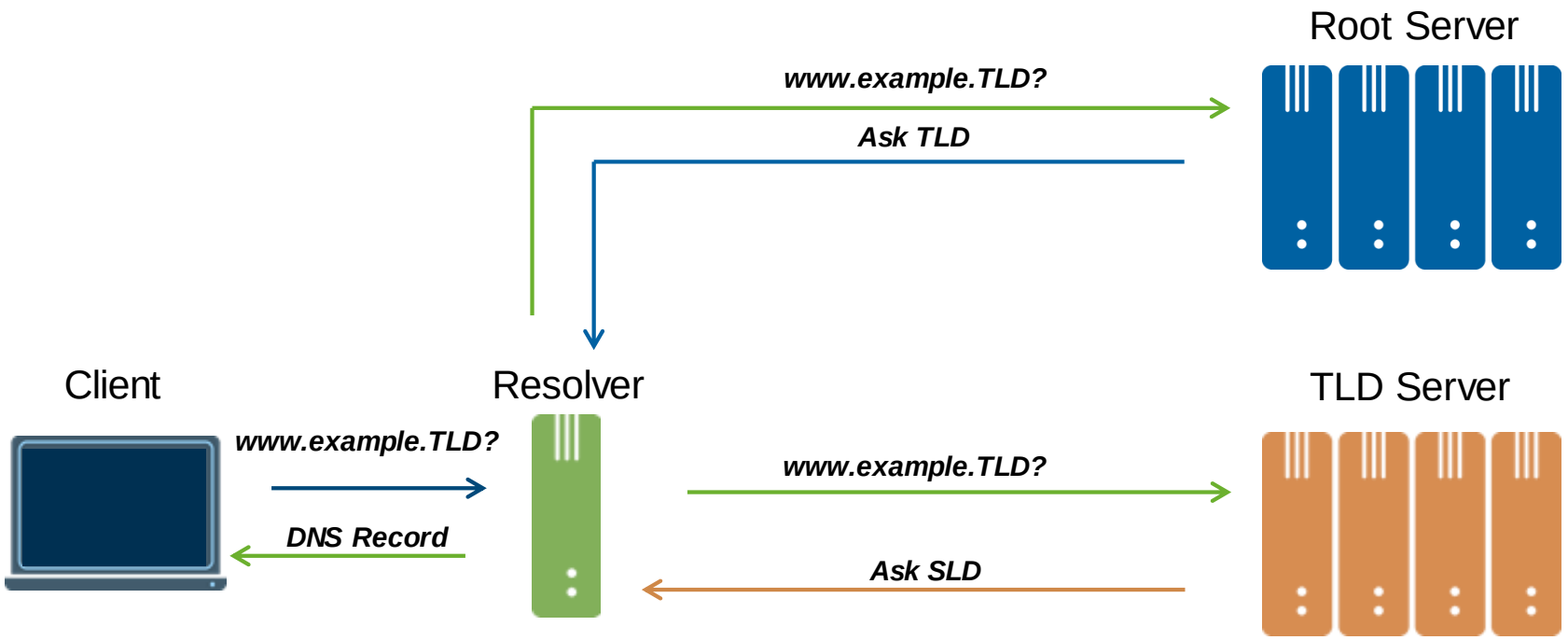
Client-to-Resolver: Encryption Recommended



Client-to-Resolver

Clients and resolvers should implement DNS encryption unless adequate protection is otherwise provided, e.g., as part of a network connection

Resolver-to-Root and TLD



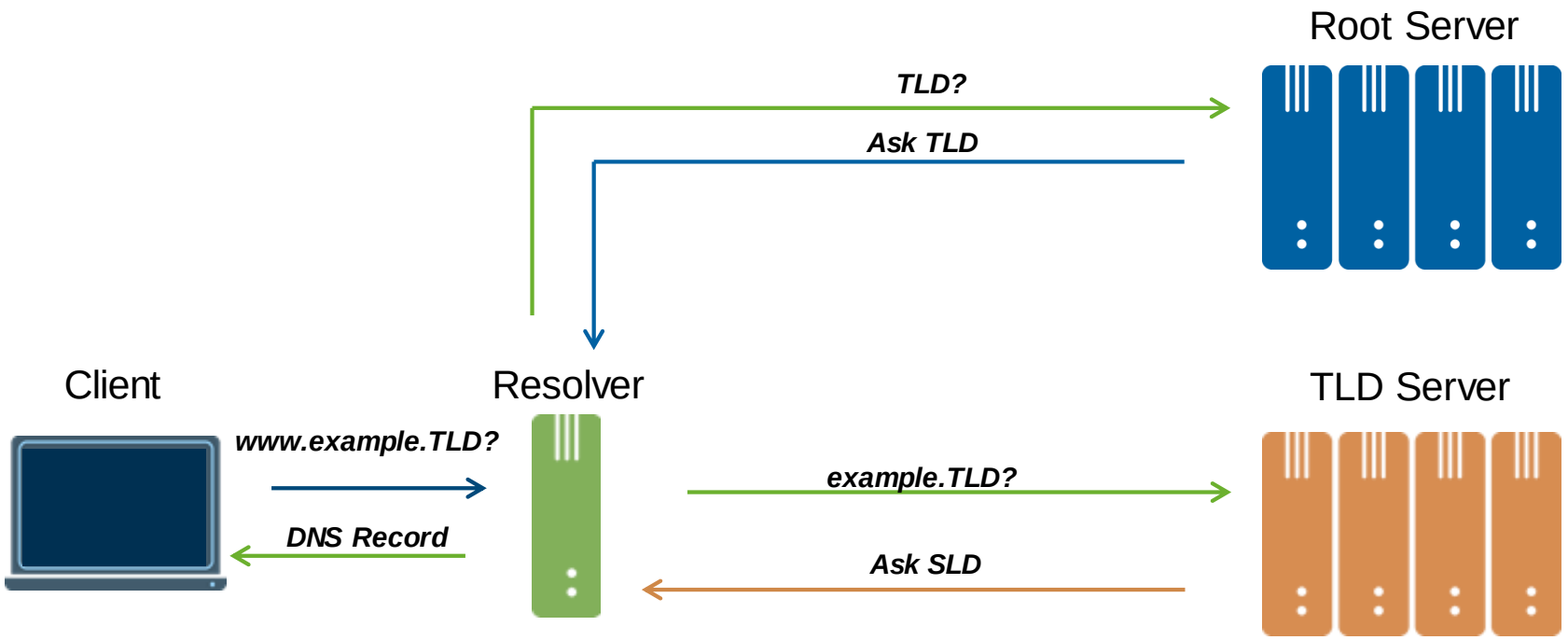
Resolver-to-Root and TLD

Aggregate interests of resolver's clients — not interests of specific clients

In traditional DNS resolution, full domain name of interest — more than "need to know"

With qname minimization, only aggregate interests in TLDs and SLDs

Resolver-to-Root and TLD: Minimize



Resolver-to-Root and TLD

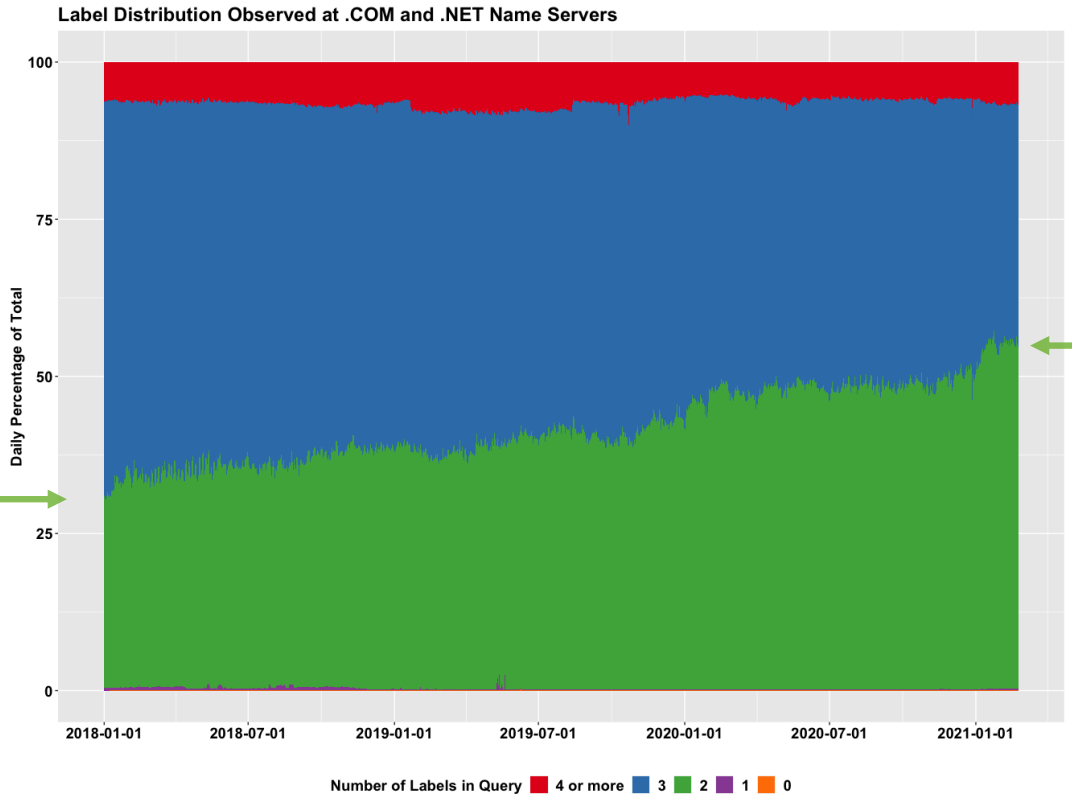
Resolvers should apply minimization techniques

QNAME Minimization: Deployment Statistics

Queries Received at the .COM and .NET Name Servers Consisting of Only Two Labels

Jan 2018

32%

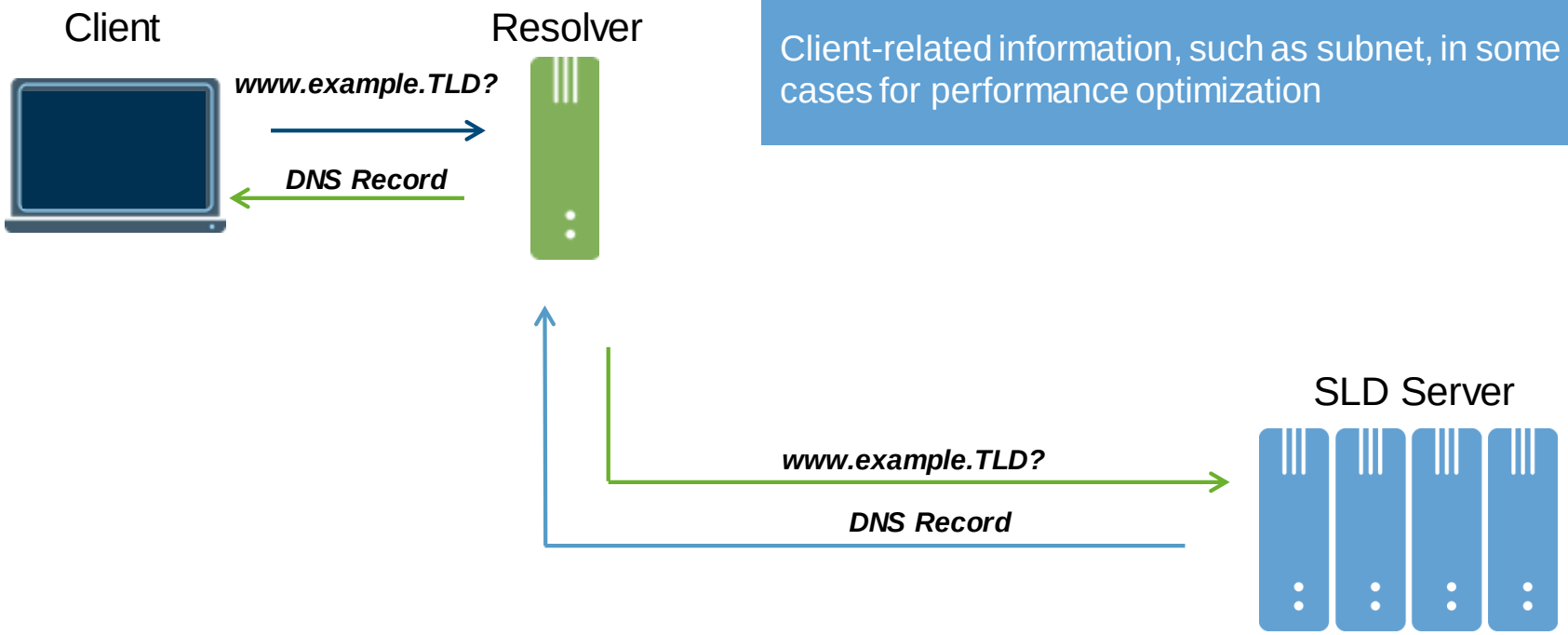


Feb 2021

55%

Some minimized queries may be indistinguishable from 3+ label queries in this analysis, depending on minimization technique employed

Resolver-to-SLD and Below



Resolver-to-SLD and Below

Aggregate interests of resolver's clients

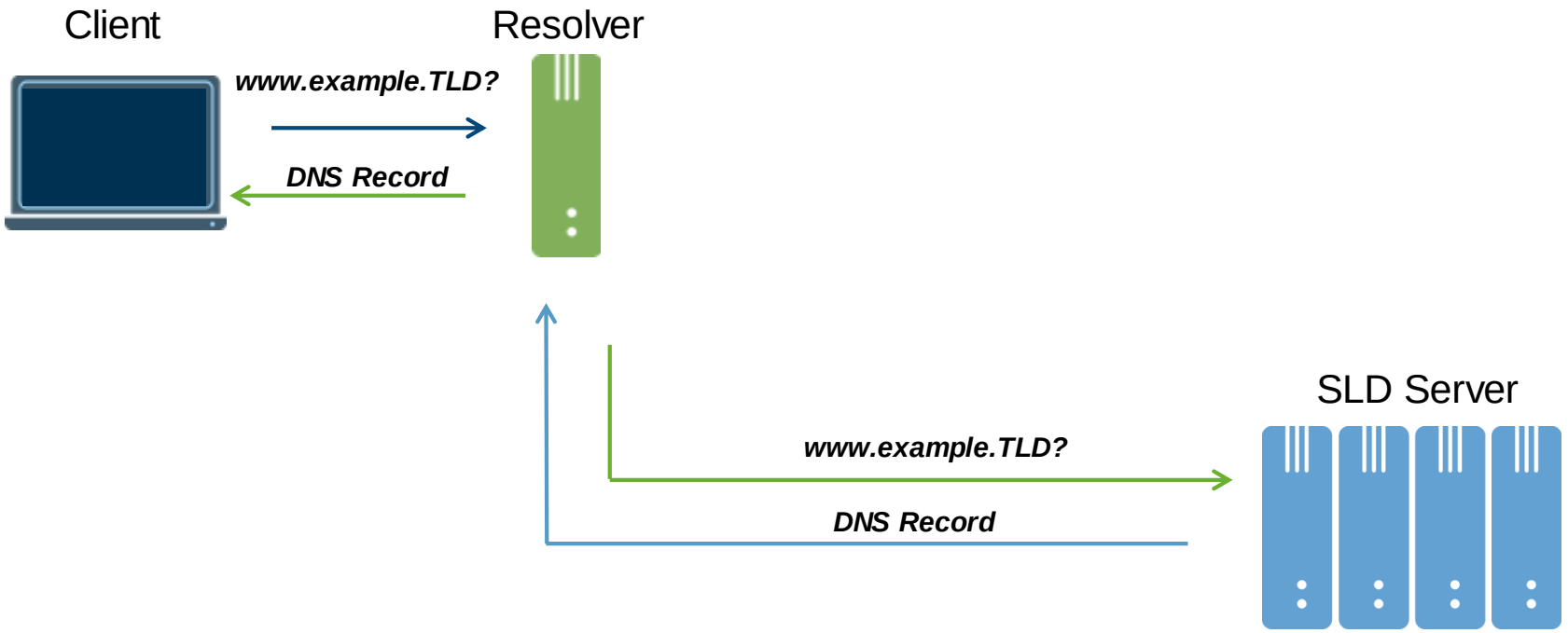
Full domain name needed to complete resolution

Client-related information, such as subnet, in some cases for performance optimization

Resolver-to-SLD and Below: Encrypt When Needed

Resolver-to-SLD and Below

Resolvers and SLD servers should implement DNS encryption on their exchanges if sending sensitive full domain names, client-specific information



DNS Confidentiality Protection Techniques: Encryption and Minimization

Encryption techniques

cryptographically conceal information, reducing risk of disclosure to outside parties

Bilateral: both parties on exchange implement, operational impact on both

Examples:

DNS-over-TLS (DOT), DNS-over-HTTPS (DoH)

Minimization techniques

decrease sensitivity of information, reducing risk of disclosure to both outside and *inside* parties

Unilateral: only sender implements, no operational impact on receiver

Examples:

query name (qname) minimization, NXDOMAIN cut processing, aggressive DNSSEC caching

Conclusion

DNS encryption and various minimization techniques all have a place in protecting different DNS exchanges

Verisign's recommendation: "Minimize at root and TLD, encrypt when needed elsewhere"