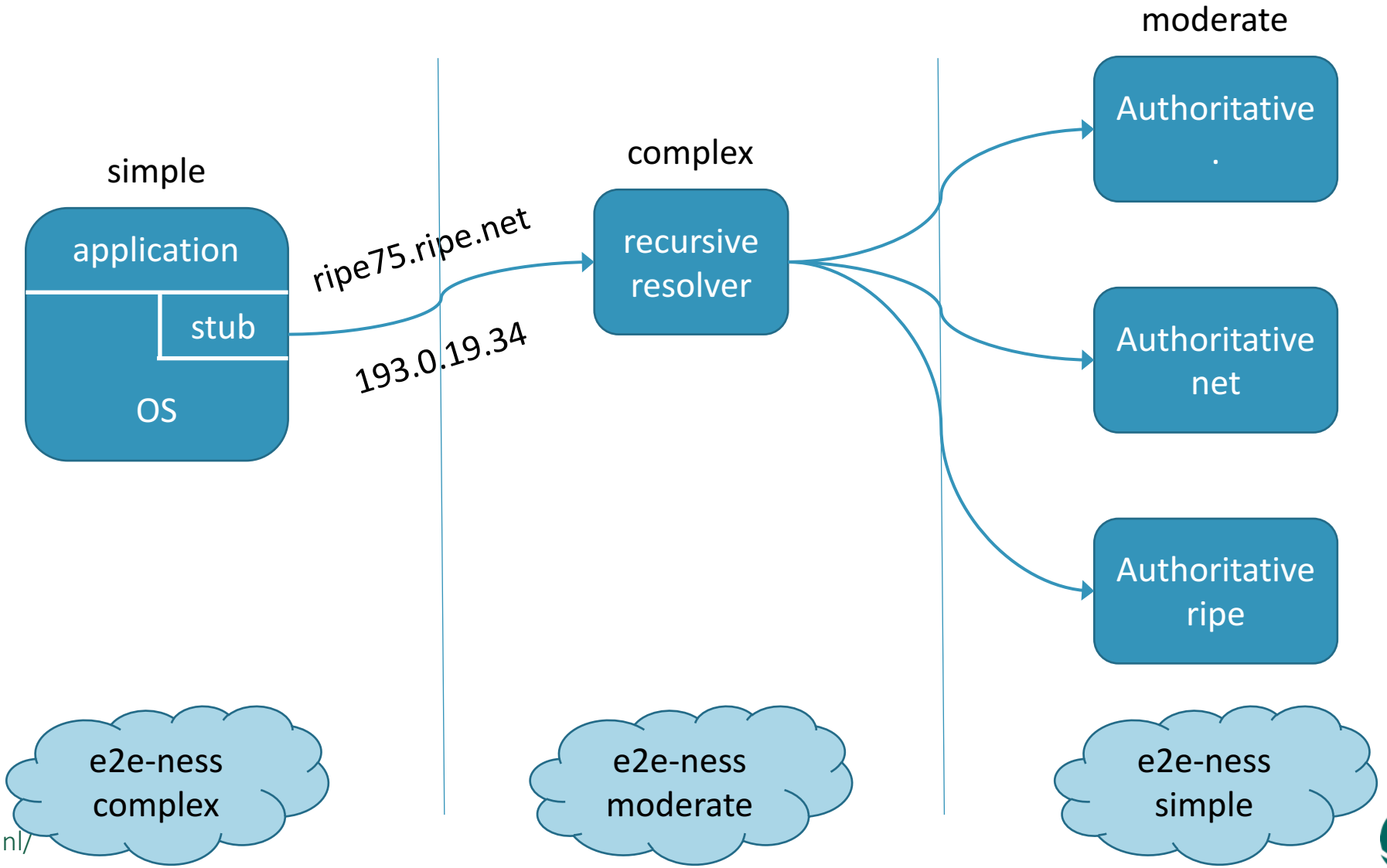
Living on the Edge: (Re)focus DNS Efforts on the End-Points

Benno Overeinder
NLnet Labs

RIPE 75, Dubai, UAE

NLNETLABS

Complexity at Core-Middle-Edge

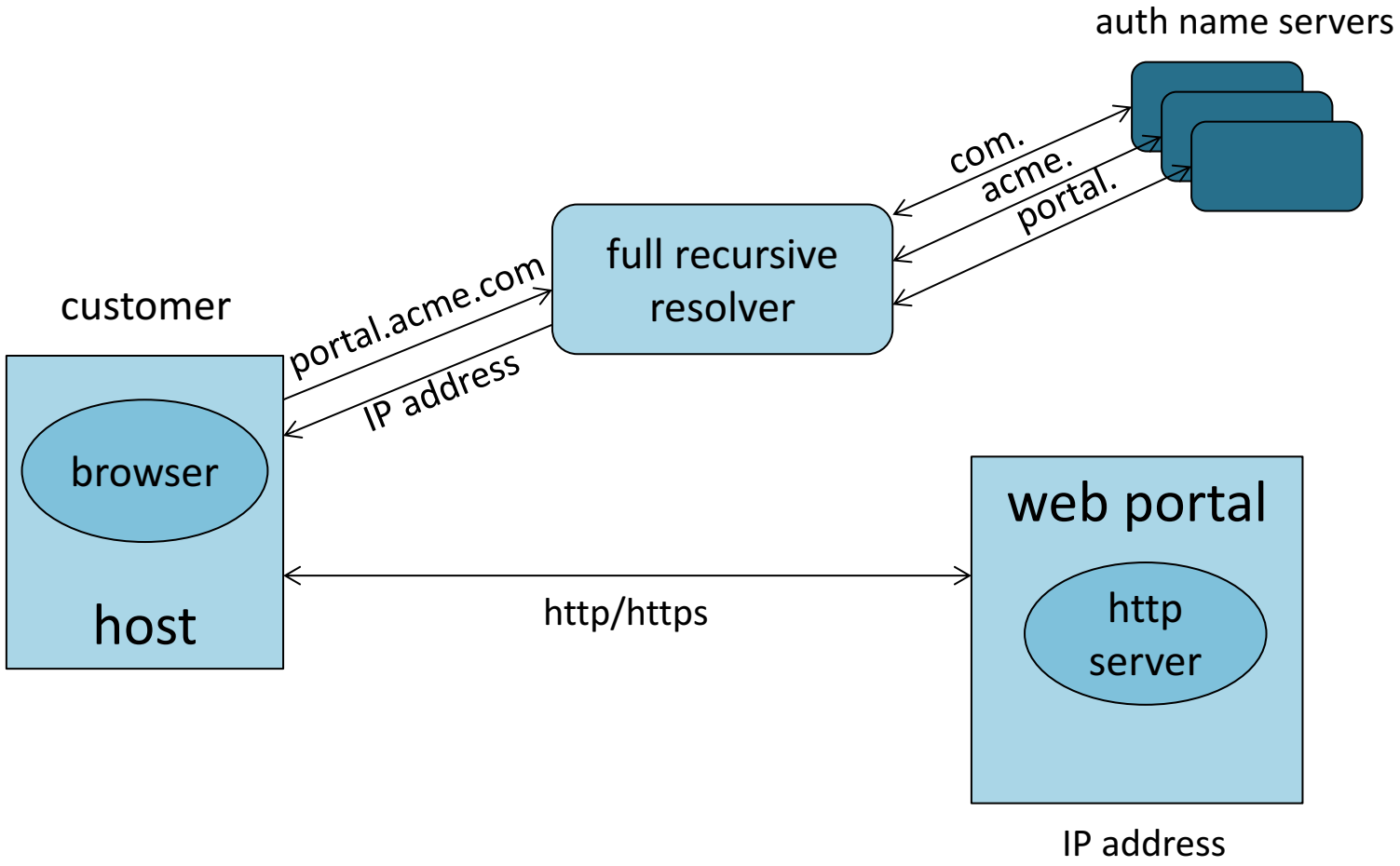


NLNETLABS

From the ground-up security

… and now for something completely different

Customer–Web Portal Interaction

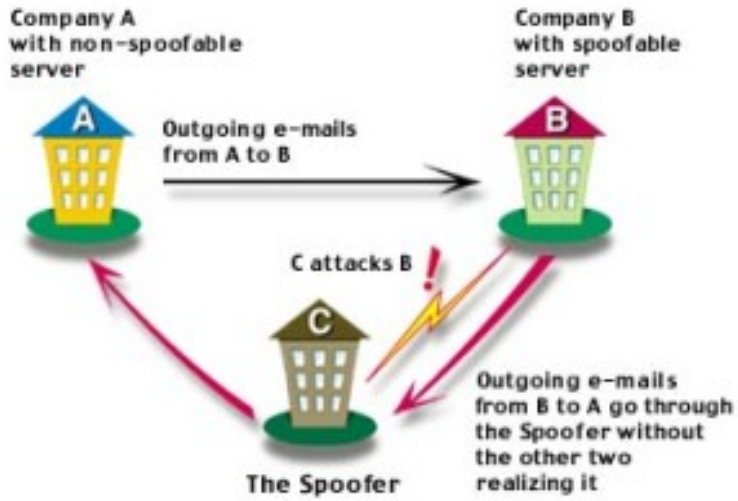


NLNETLABS

DNS Spoofing

- DNS Spoofing by cache poisoning
  - attacker flood a DNS resolver with phony information with bogus DNS results
  - by the law of large numbers, these attacks get a match and plant a bogus result into the cache

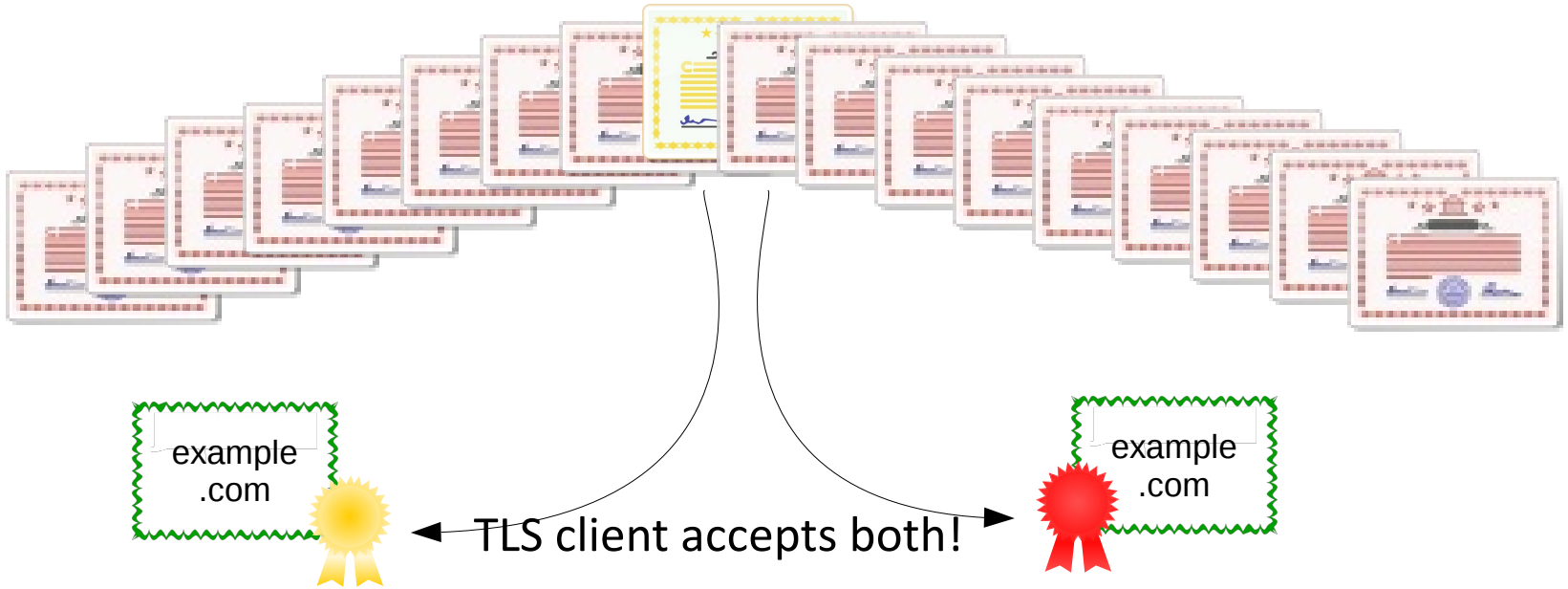
- Man-in-the-middle attacks
  - redirect to wrong Internet sites
  - email to non-authorized email server



NLNETLABS

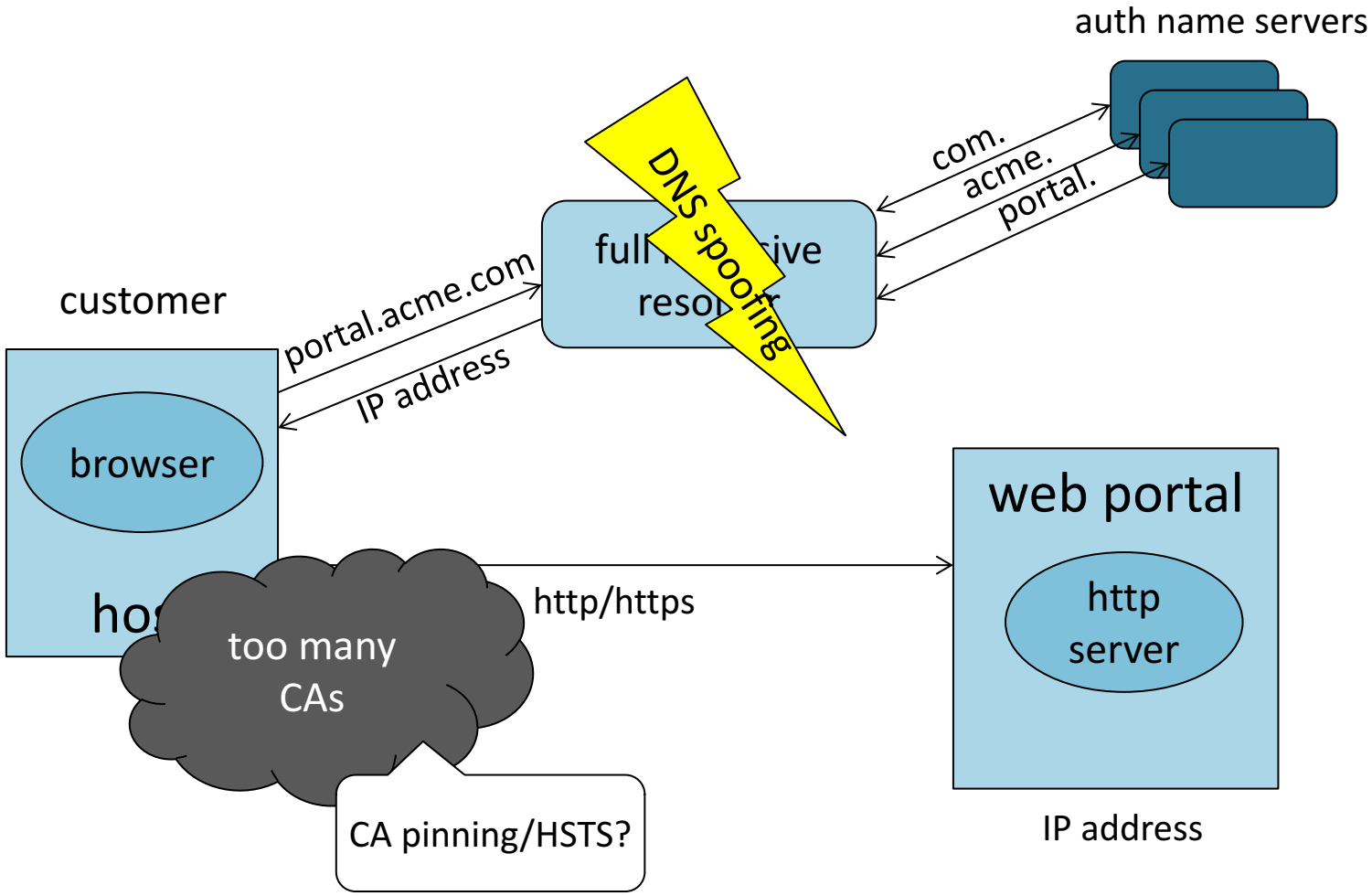
The “Too Many CAs” Problem

- TLS clients have abundance of TAs
  - modern web browsers have 1300+ TAs
  - any of them can issue certificate for example.com

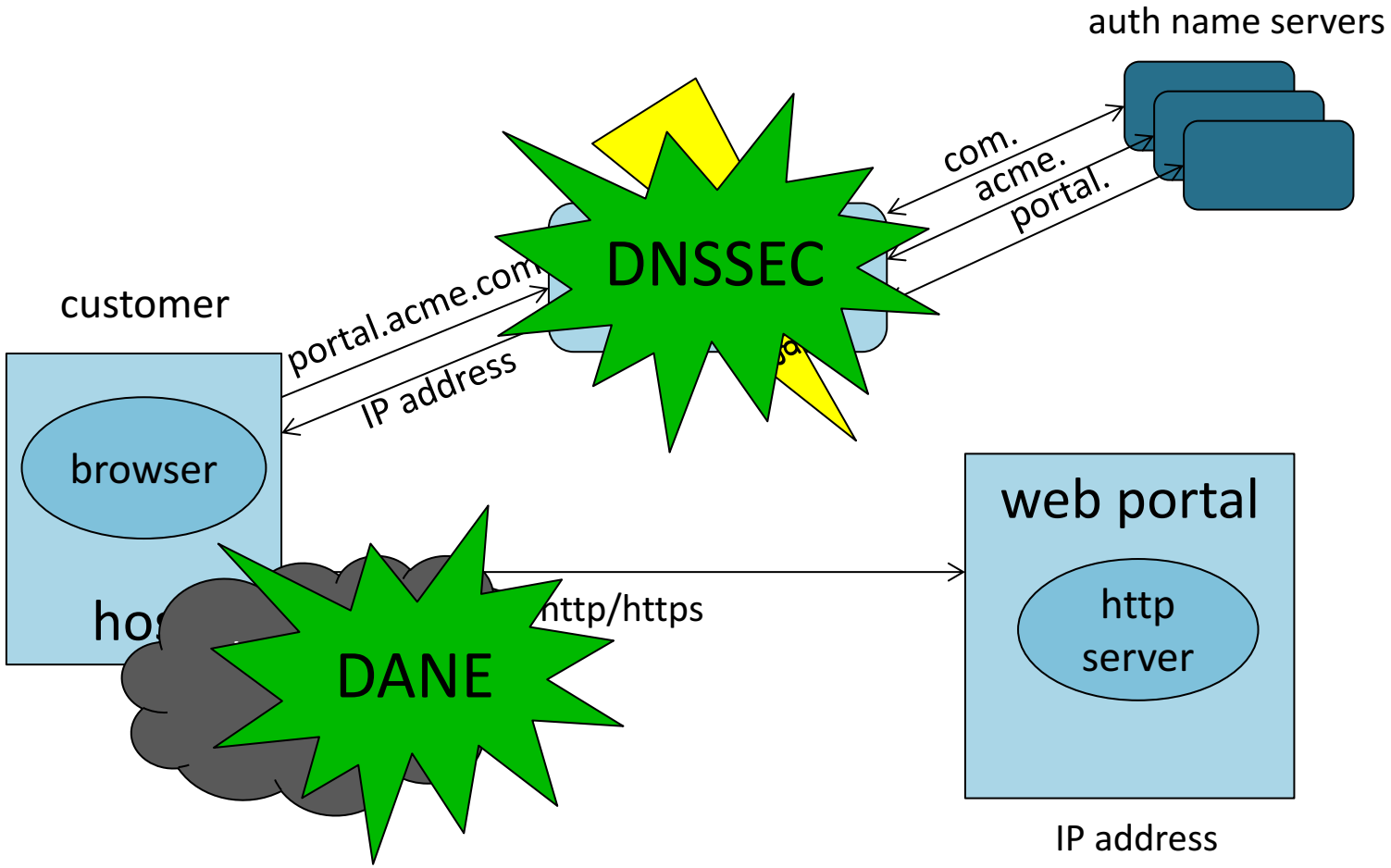


credits wes.hardaker@parsons.com

Customer–Web Portal Interaction

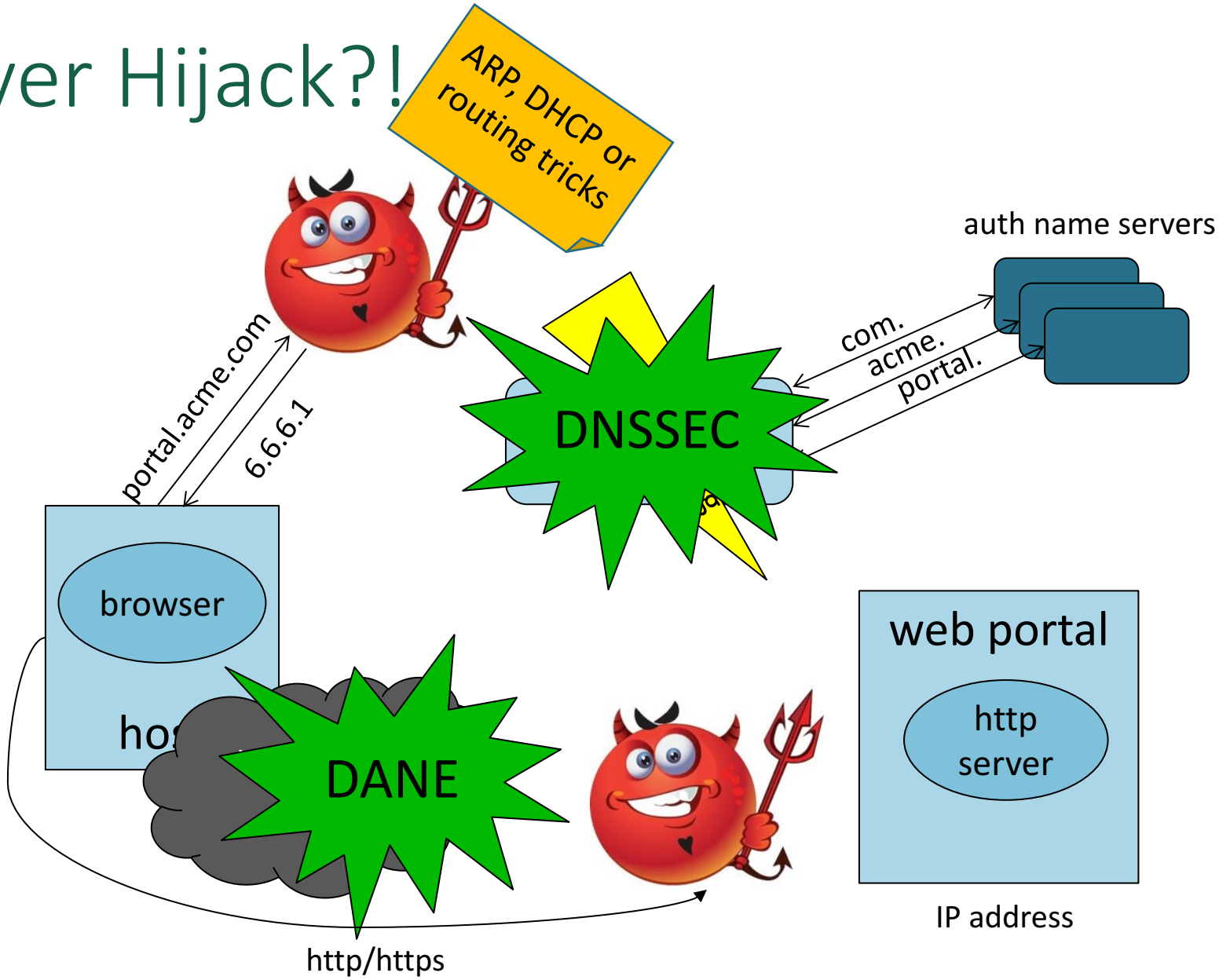


DNSSEC-Based Secure Customer–Web Portal Interaction



NLNETLABS

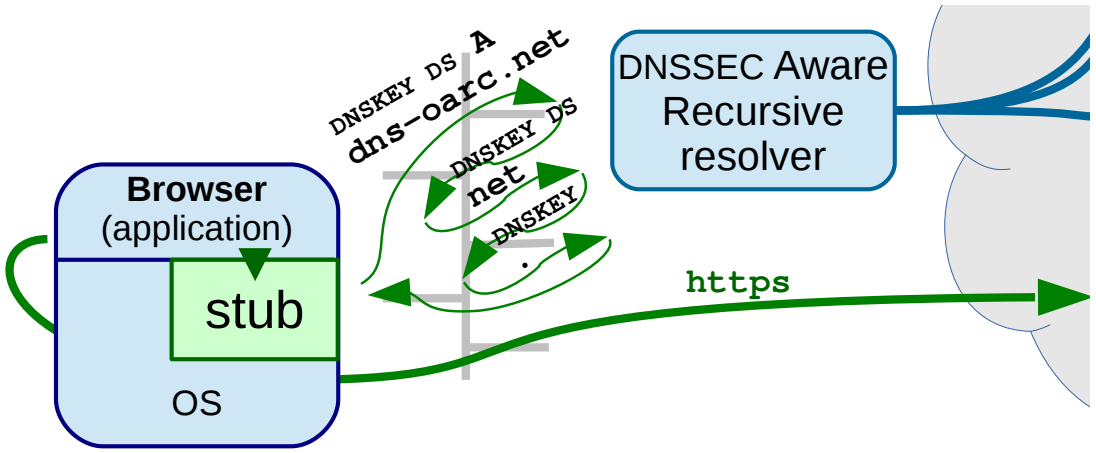
Resolver Hijack?!



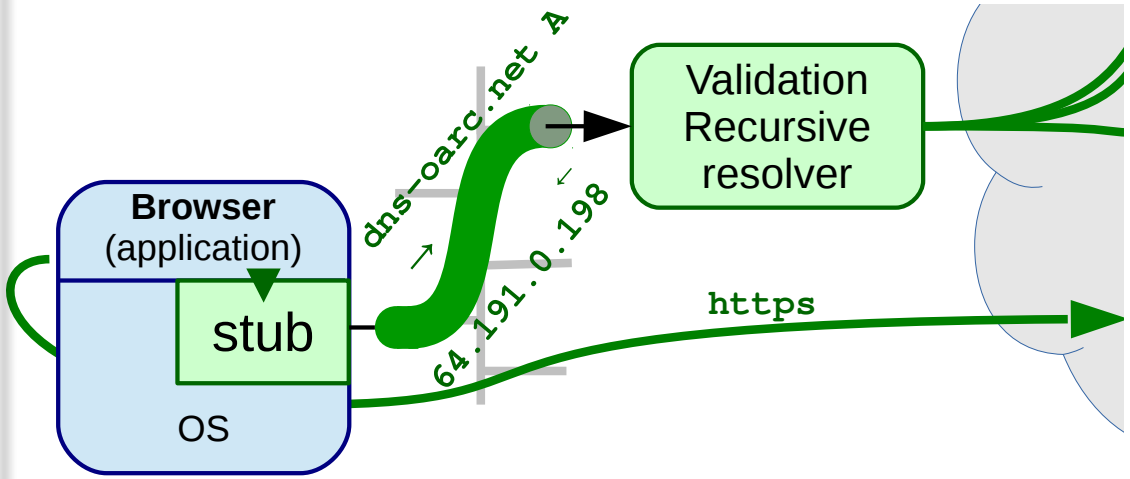
NLNETLABS

Countering Resolver Hijack

- DNSSEC on the stub



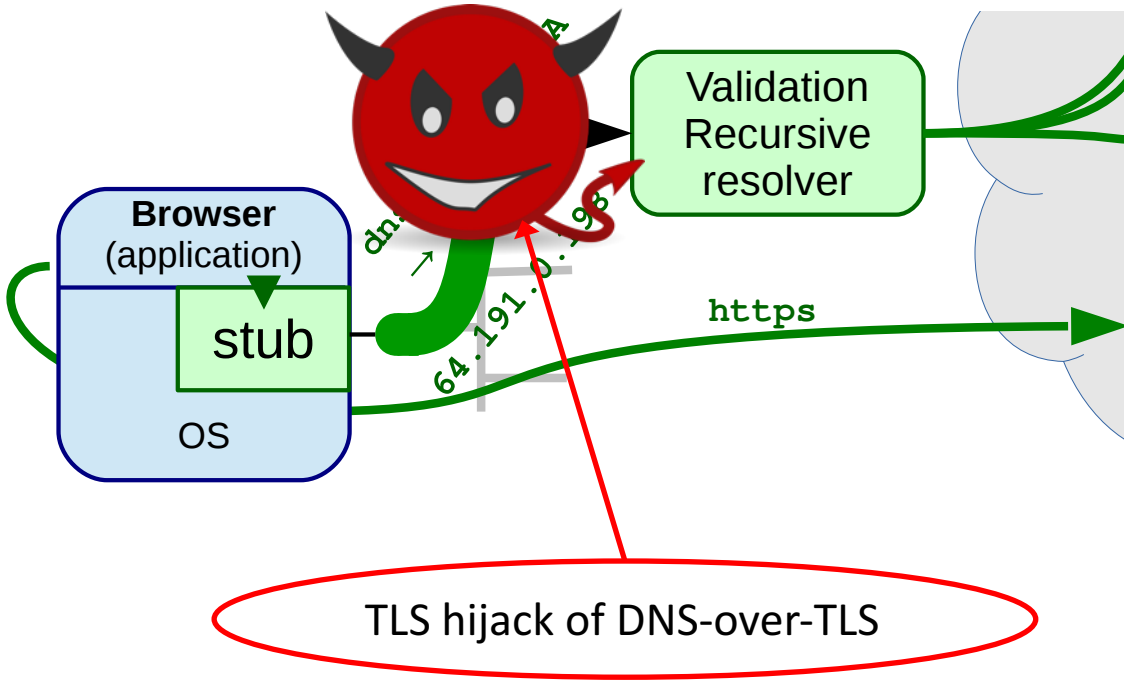
- DNS-over-TLS



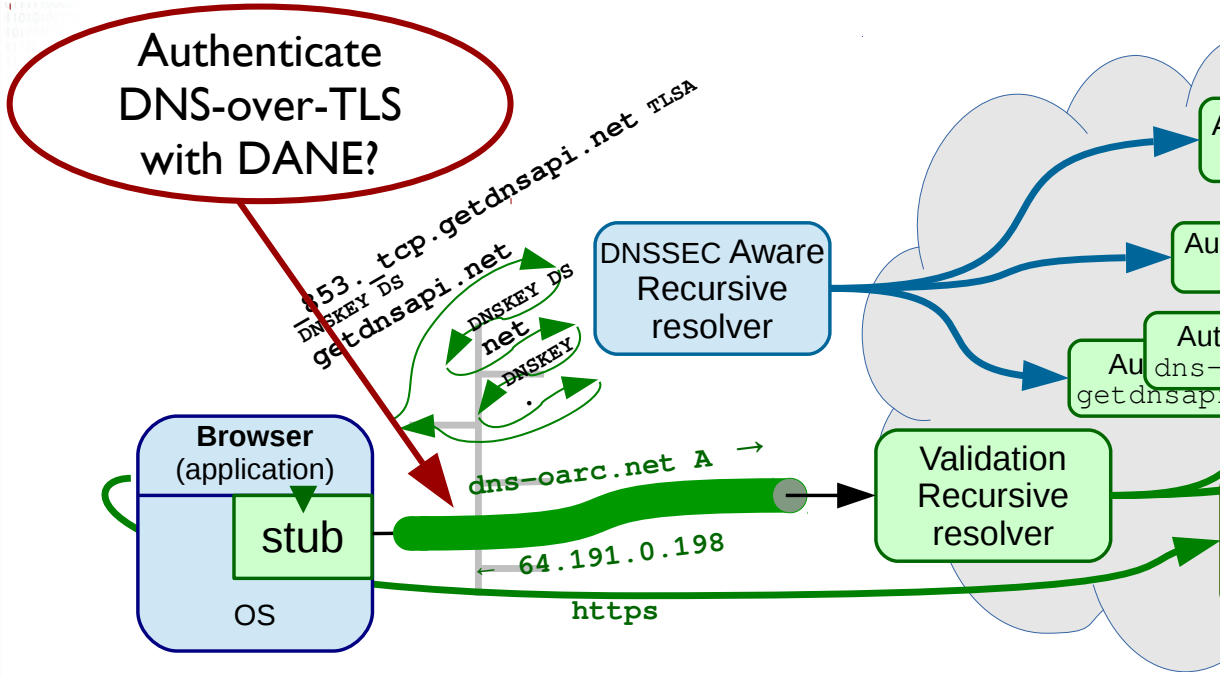
NLNETLABS

Countering Resolver Hijack (cont'd)

- DNS-over-TLS



- DNS-over-TLS



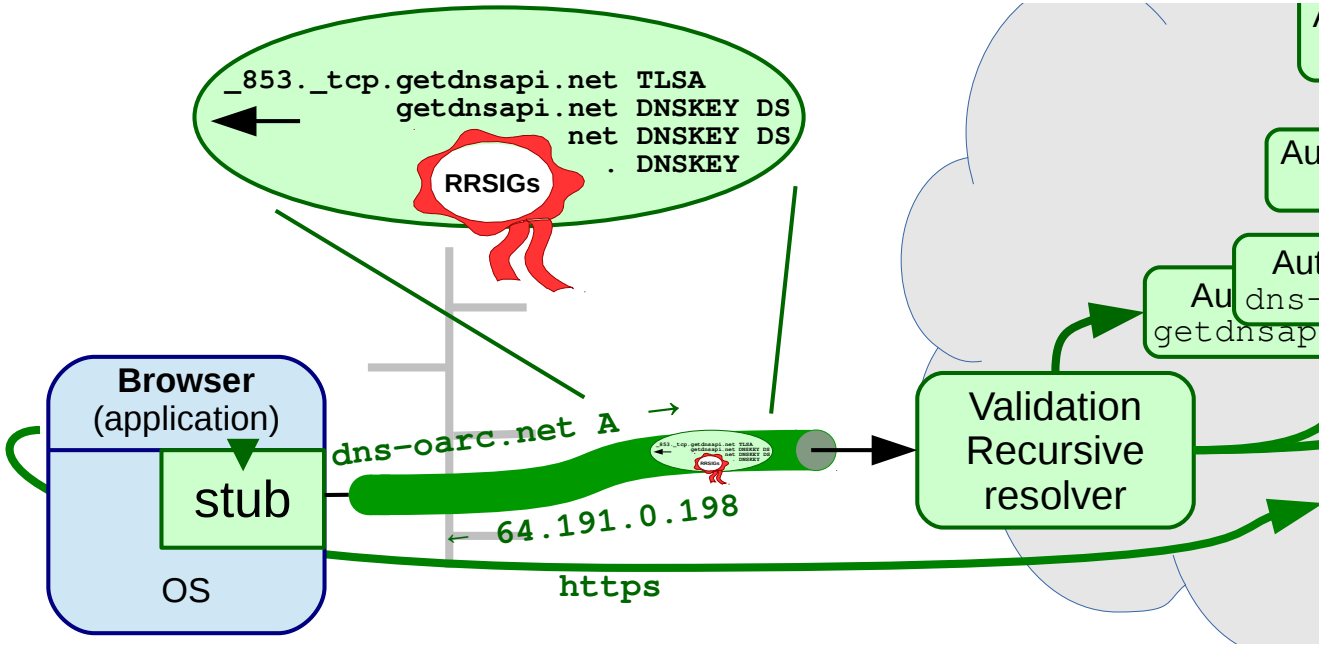
Bootstrap the TLSA lookup with regular DNS?

Chicken and egg problem.

NLNETLABS

DNSSEC Data Blob-over-TLS

- TLSA record + the complete DNSSEC authentication chain embedded in a TLS extension
  - TLS DNSSEC authentication to prevent “Too many CA’s” problem
  - https://tools.ietf.org/html/draft-ietf-tls-dnssec-chain-extension



NLNETLABS

DNS Privacy and Standards

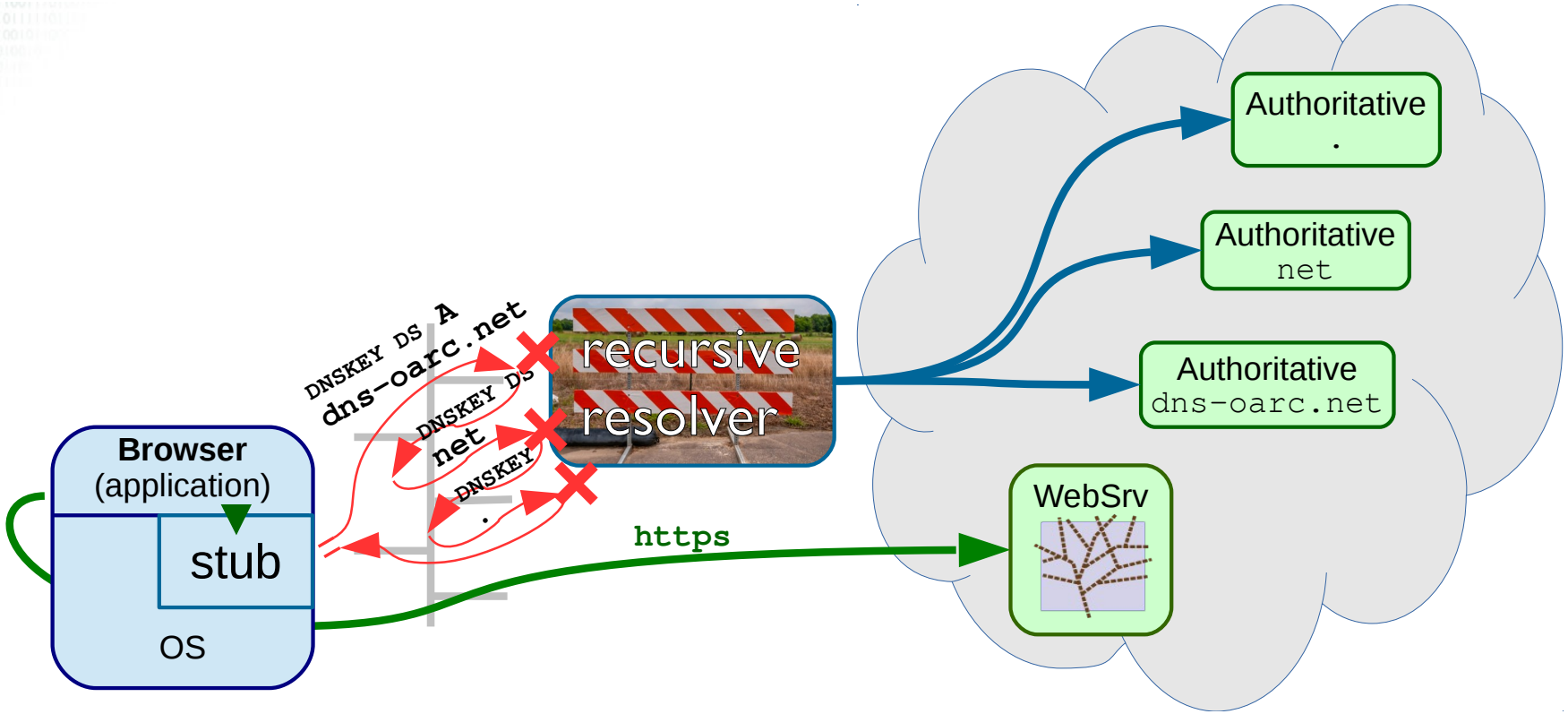
- DNS privacy requirements

Capability	Standard
DNS-over-TLS	RFC7858
Reuse/pipelining/OOOP	RFC7766
TCP fast open	RFC7413
ENDS0 keep alive	RFC7828
ENDS0 padding	RFC7830
PKIX support for authentication	*(various)*
DNSSEC support *(for address lookup and authentication)*	*(various)*

DNSSEC Roadblocks

Consequences of living on the edge

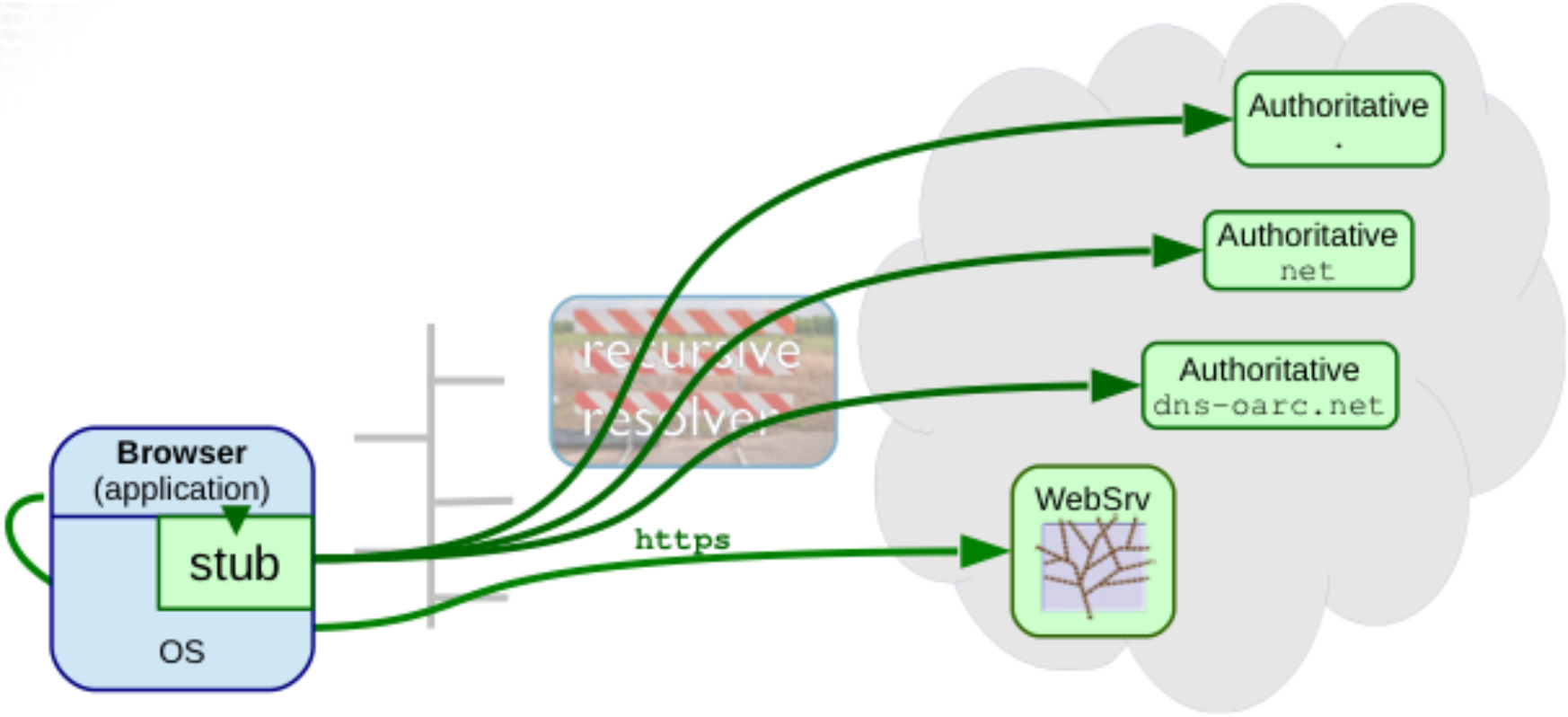
DNSSEC Roadblocks



- Resolving DNSSEC (to cross the first mile) needs DNSSEC aware recursive resolver

NLNETLABS

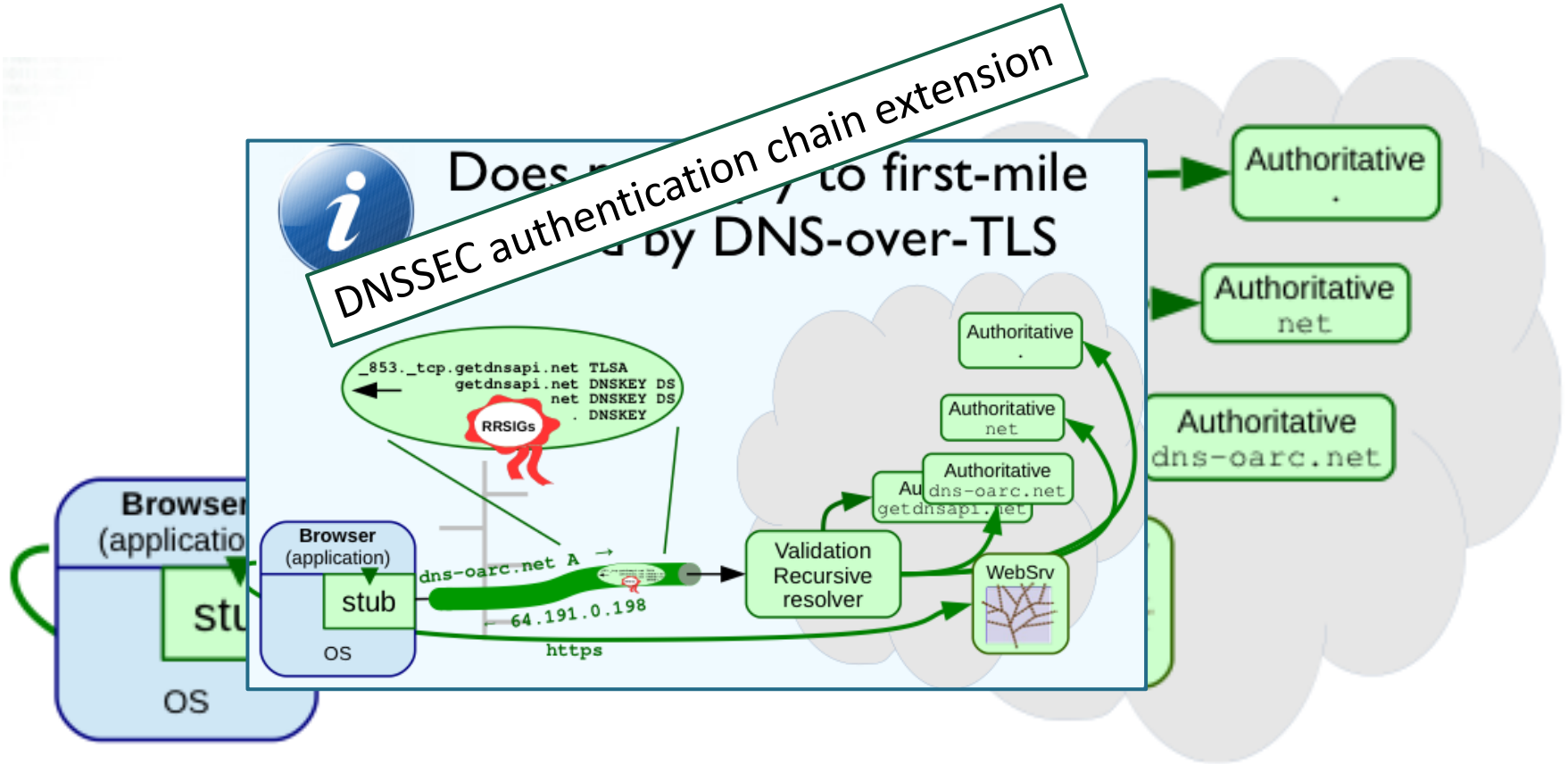
DNSSEC Roadblock Avoidance



- DNSSEC roadblock avoidance + full recursion capability
  - https://tools.ietf.org/html/rfc8027

NLNETLABS

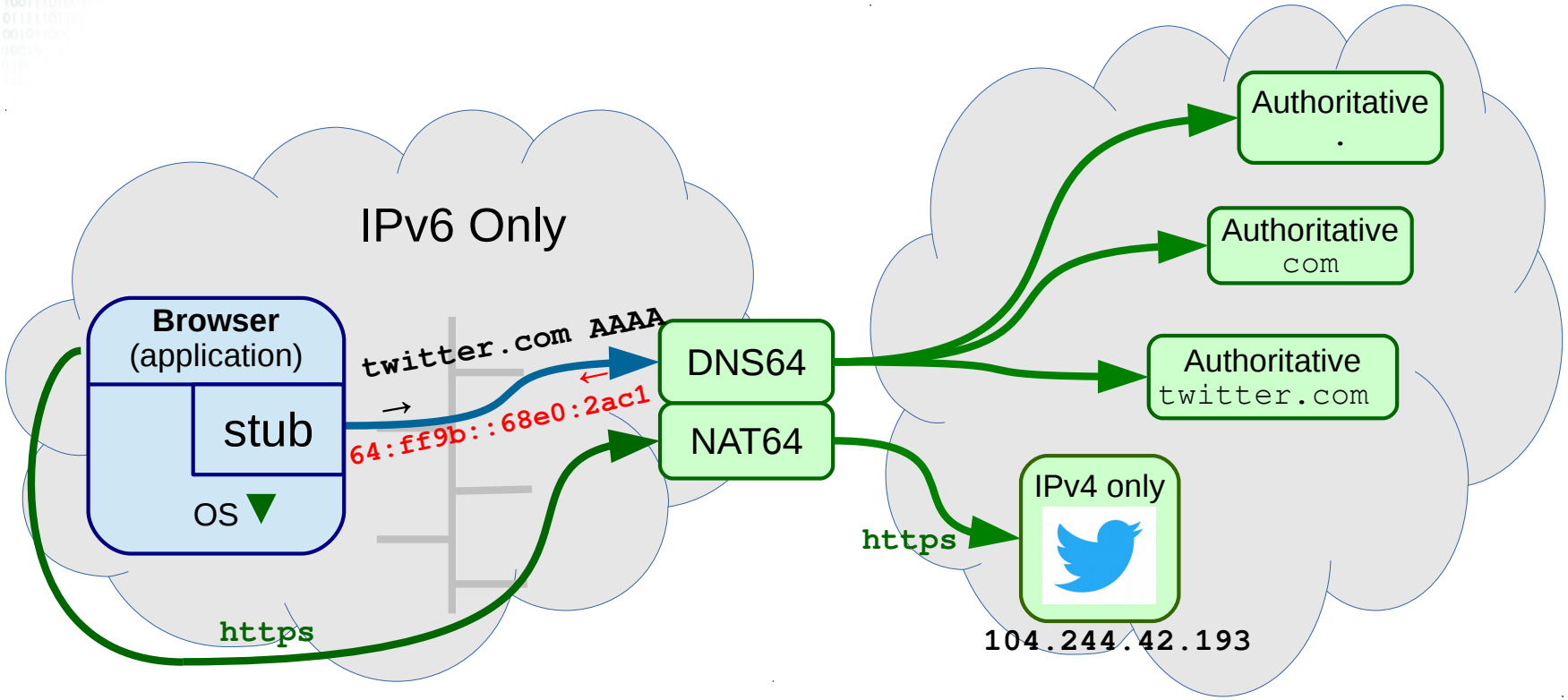
DNSSEC Roadblock Avoidance



- DNSSEC roadblock avoidance + full recursion capability
  - https://tools.ietf.org/html/rfc8027

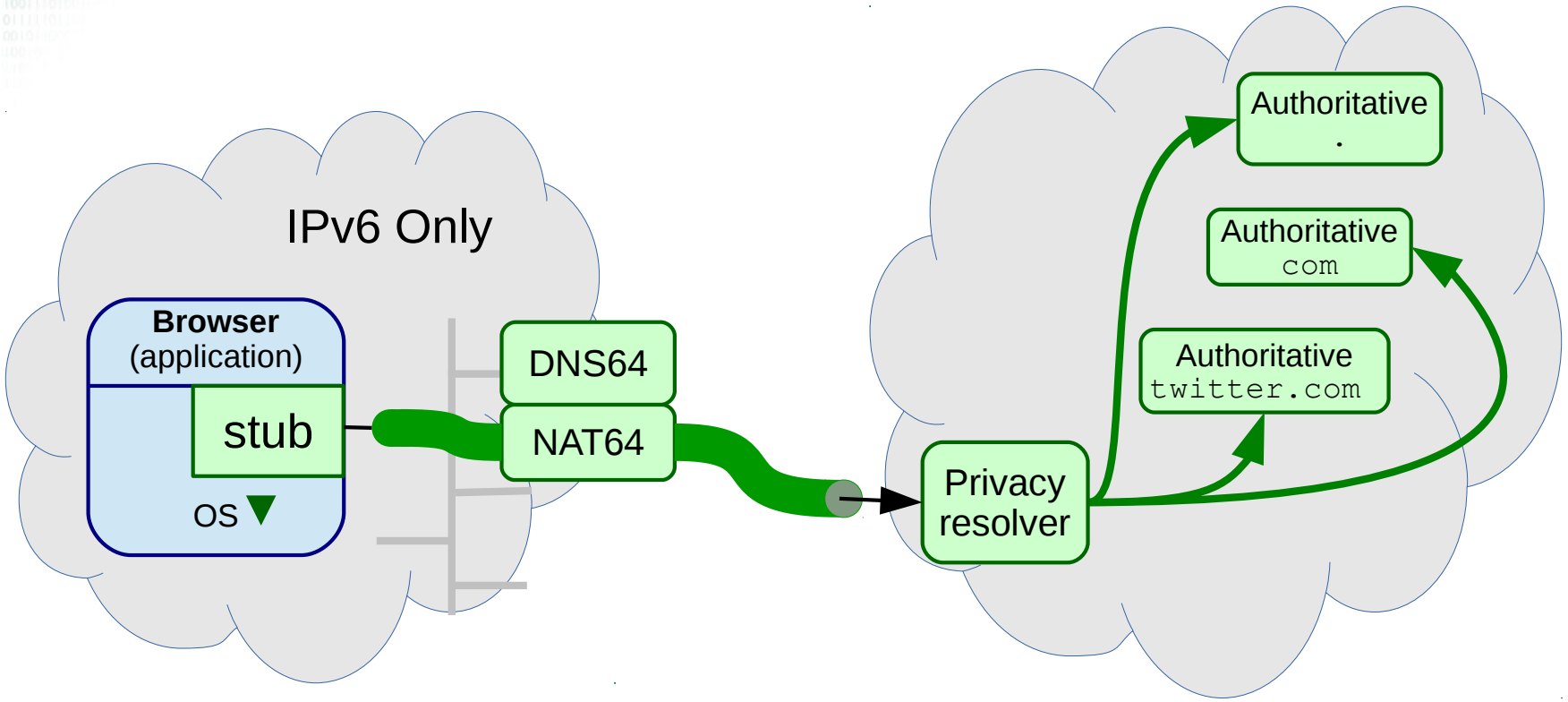
NLNETLABS

DNSSEC with DNS64 & NAT64



- Jen Linkova's "Let's talk about IPv6 DNS64 & DNSSEC"
  - https://blog.apnic.net/2016/06/09/lets-talk-ipv6-dns64-dnssec/
- With IPv6 prefix discovery, stub can do DNSSEC validation of A RR itself

DNSSEC with DNS64 & NAT64



- IPv6 address synthesis prefix discovery + DNS64 capability
  - https://tools.ietf.org/html/rfc7050
  - https://tools.ietf.org/html/rfc6147

NLNETLABS

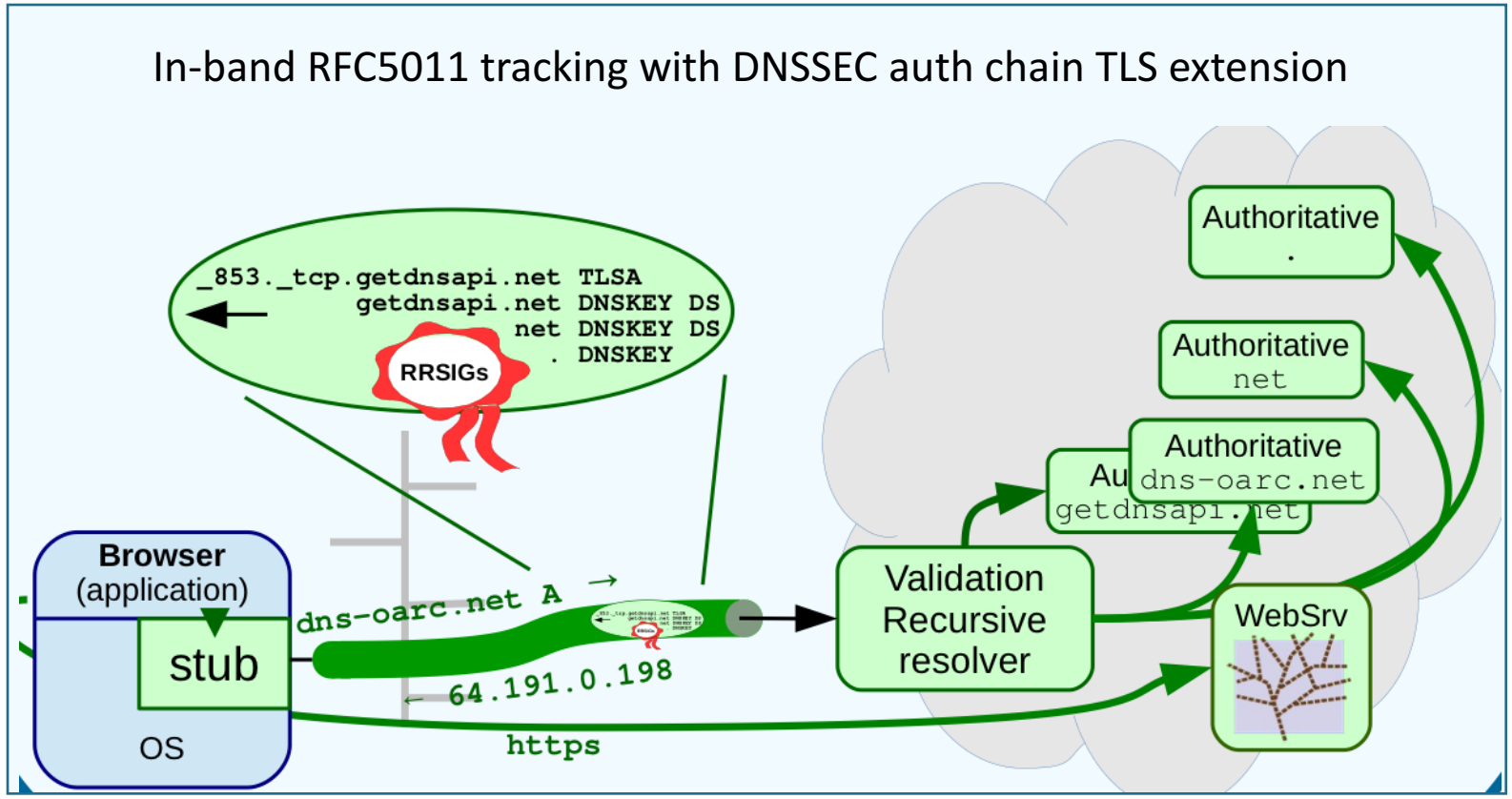
KSK Root Rollover

More roadblocks ahead

NLNETLABS

RFC5011 for DNSSEC Validating Stubs

- DNSSEC validating stub **must** do RFC5011



NLNETLABS

KSK Root Rollover for Stub Library

- A stub library for DANE
  - runs with user's privileges
  - no system config
  - bootstrap DNSSEC capabilities
    - https://tools.ietf.org/html/rfc7958
    - unbound-anchor functionality

DNSSEC Roadblocks and Standards

- DNSSEC stubs capability requirements

Capability	Standard
DNSSEC validation	*(various)*
DNSSEC roadblock avoidance	RFC8027
IPv6 prefix discovery	RFC7050
IPv6 address synthesis	RFC6147
Automated trust anchor updates	RFC5011
Automated initial trust anchor retrieval	RFC7958

Living on the Edge

"Final Thoughts"

Wrapping Up

- Stub resolver/library experience complex e2e-ness
  - at the edge of the network many kinds of roadblocks/brokenness
- DNS-based security from the ground up
  - bootstraps with the stub
- Closing the gap in the last mile with ongoing work
  - overview of RFCs and drafts
  - most of discussed work is implemented in **getdns** and its stub resolver **Stubby**
- DNSSEC Authentication Chain Extension
  - https://tools.ietf.org/html/draft-ietf-tls-dnssec-chain-extension