From the Ground Up Security

DNS-based Security of the Internet Infrastructure

Benno Overeinder

NLnet Labs

INTRO

About NLnet Labs

- Not-for-profit R&D company
  - open standards
  - open source software
  - innovation & expertise for benefit of open Internet
- Mission & goal
  - contribute to bridge gap between research and practical deployments

    https://www.nlnetlabs.nl/labs/mission/

About NLnet Labs cont'd

- Open source software
  - infrastructure: NSD, Unbound
  - provisioning: OpenDNSSEC, …
  - libraries: getdns API, ldns
- Community activities
  - standards: IETF (drafts and RFCs)
  - research & operational insights: RIPE, NANOG, …
  - policy and governance: ICANN, ...

How DNS(SEC) provides building blocks for security and privacy

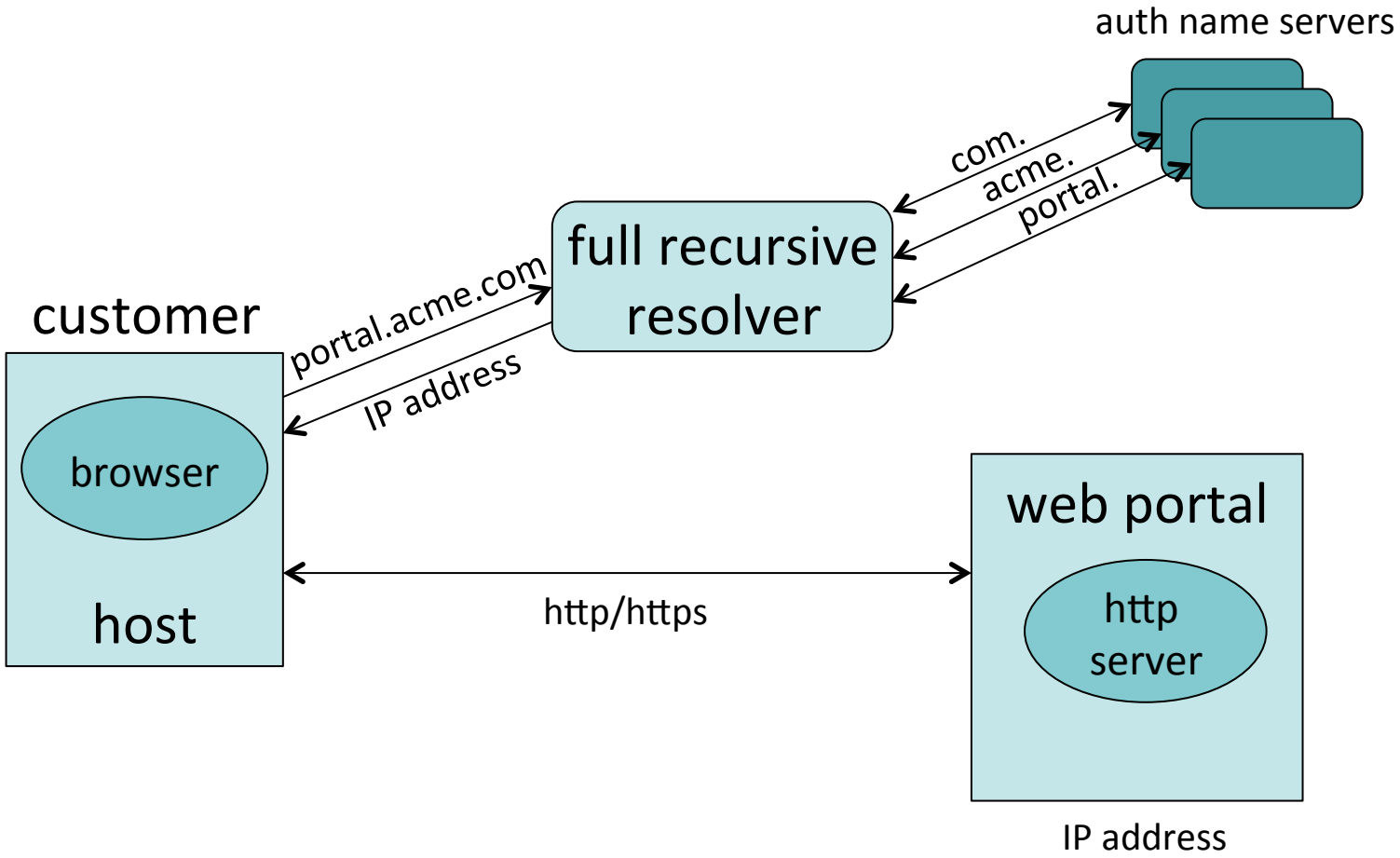
FROM THE GROUND UP SECURITY

Use-/Showcase Scenarios

End-to-end authenticated and secured/ encrypted communication

- Secure customer interaction in web portal
- Secure email
- Instant messages/chat with OTR
- …

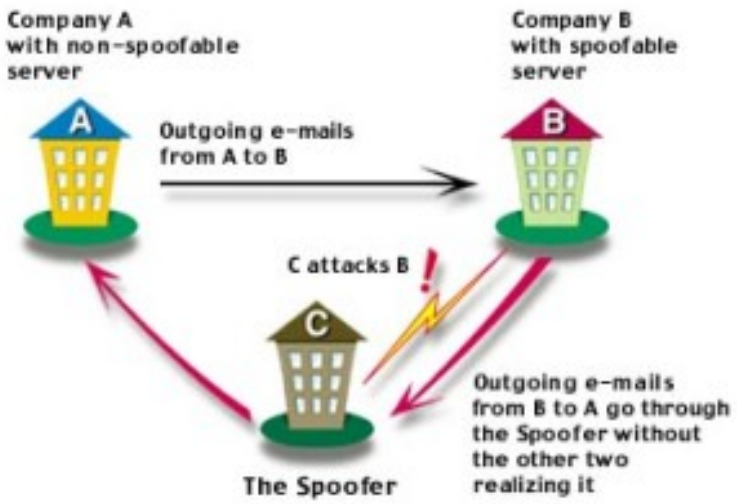
Customer–Web Portal Interaction



DNS Spoofing

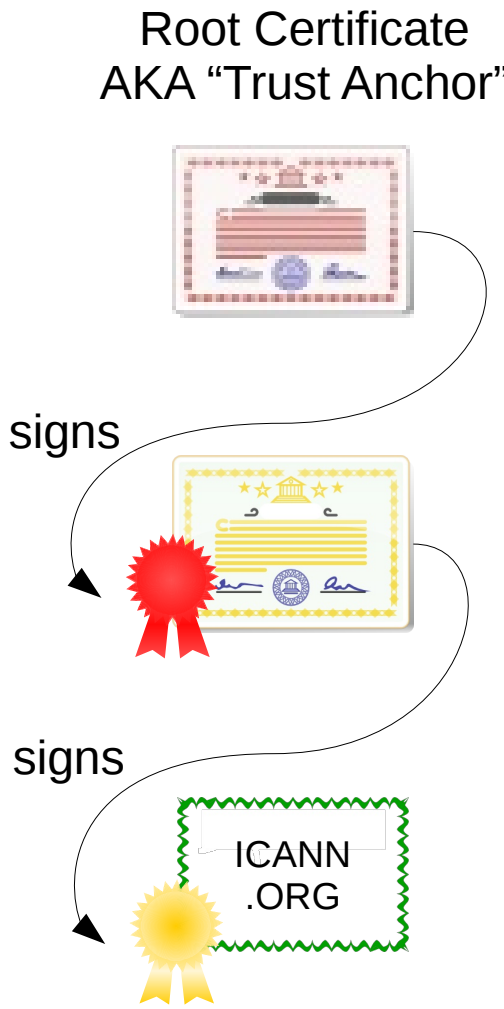
- DNS Spoofing by cache poisoning
  - attacker flood a DNS resolver with phony information with bogus DNS results
  - by the law of large numbers, these attacks get a match and plant a bogus result into the cache

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



PKIX/X.509 Certificate Tree

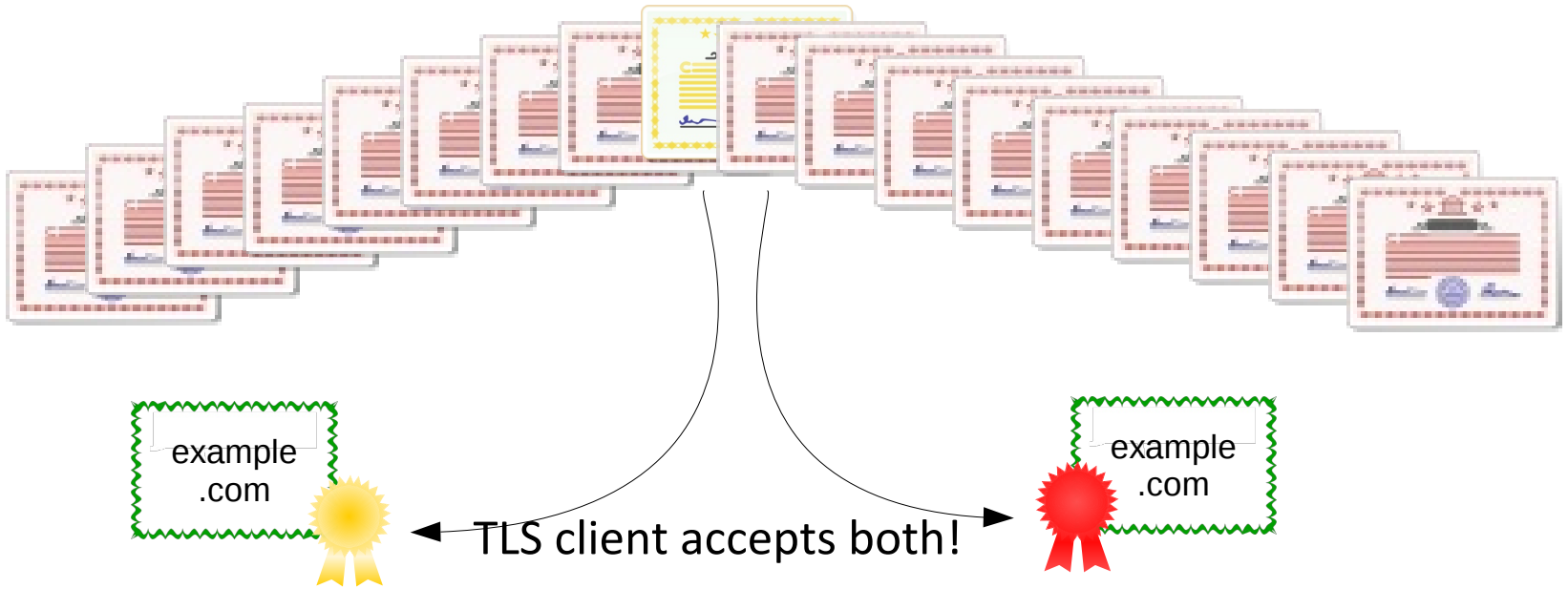
- Certification authorities (CAs)
  - sign child certificates
  - should verify child identity
  - can be trust anchors (TAs)
- TLS clients
  - trust their trust anchors
- All is good? CAs are trustworthy?



credits wes.hardaker@parsons.com

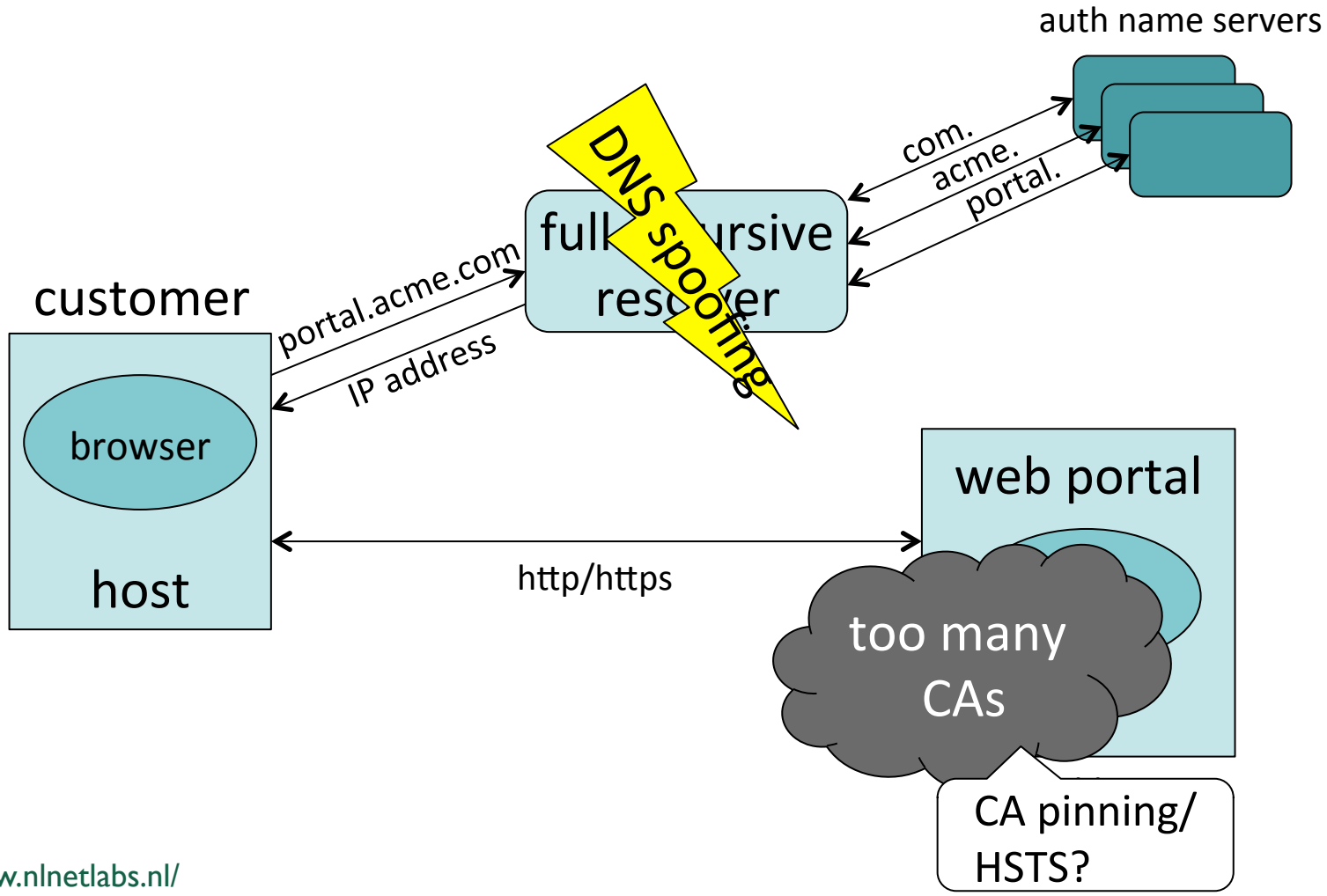
The “Too Many CAs” Problem

- 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 Revisited



DNS SECURITY EXTENSIONS & DNS-BASED AUTHENTICATION OF NAMED ENTITIES

DNSSEC and DANE to the Rescue

- DNSSEC
  - validates the authenticity of the DNS data using digital signatures

- DANE
  - allows one to securely specify which TLS/SSL certificate an application or service should use

What is DNSSEC?

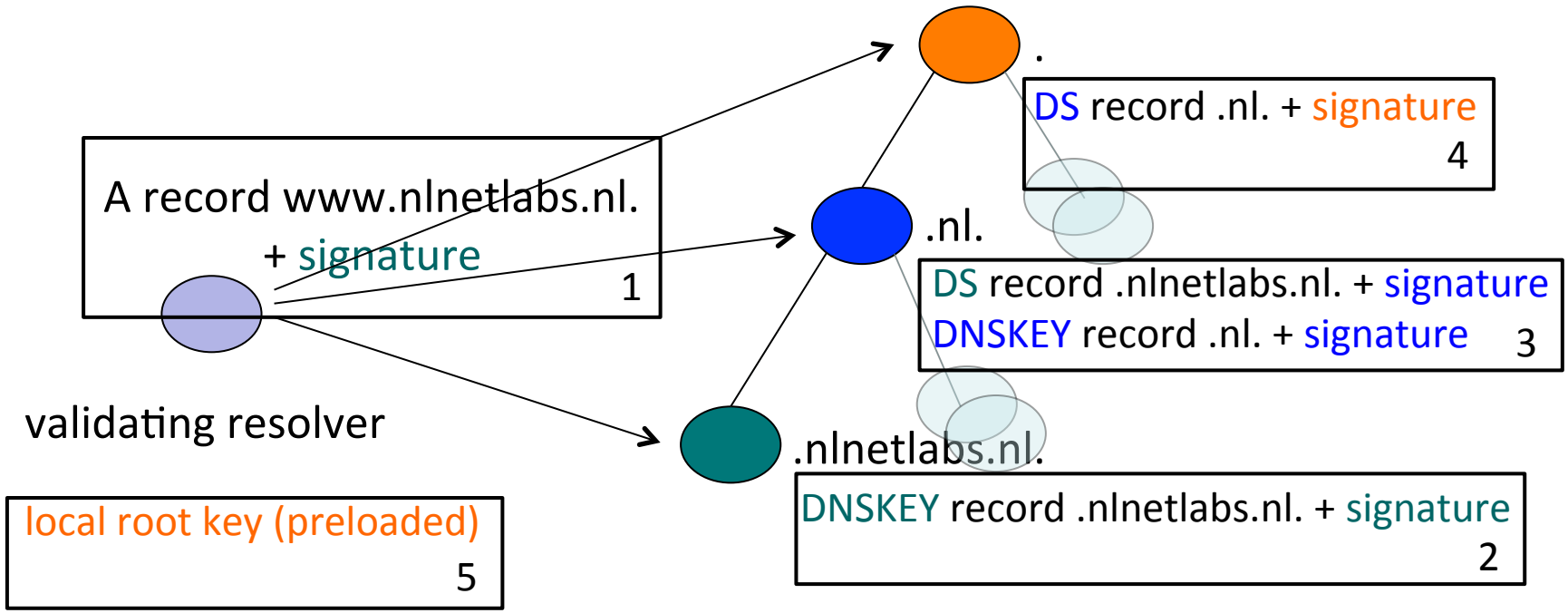
the one slide version

- Digital signatures are added to responses by authoritative servers for a zone
- Validating resolver can use signature to verify that response is not tampered with
- Trust anchor is the key used to sign the DNS root
- Signature validation creates a chain of overlapping signatures from trust anchor to signature of response

credits Geoff Huston

DNSSEC and Validation

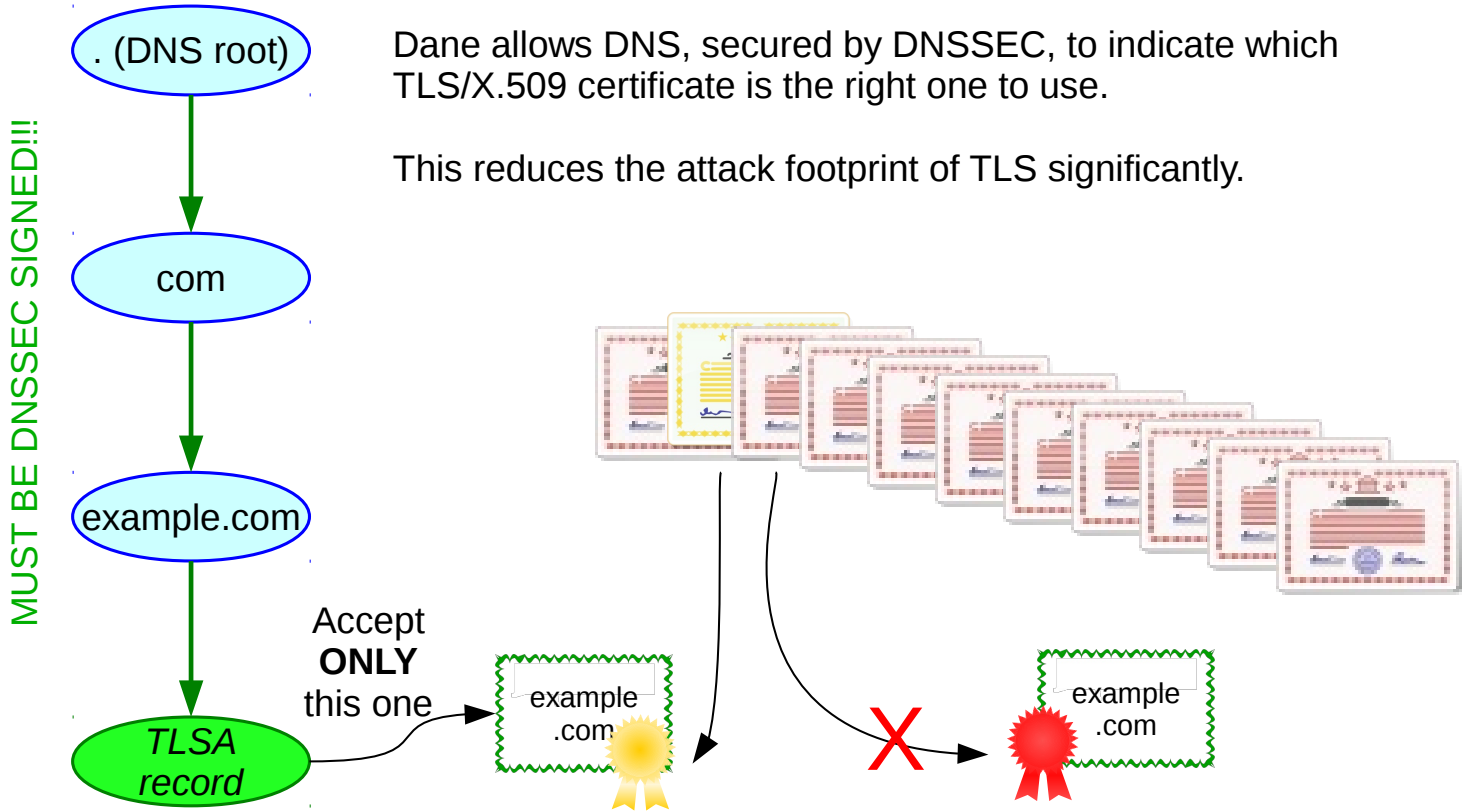
in a single picture



DANE: DNS-based Authentication of Named Entities

- Securely specify which certificate an application or service should use
  - works perfectly fine with existing CA cerficates
- DANE defines TLSA resource record and usage field
  - 0 – CA specification
  - 1 – specific TLS certificate
  - 2 – trust anchor assertion
  - 3 – domain issued certificate

DNSSEC, DANE and X.509

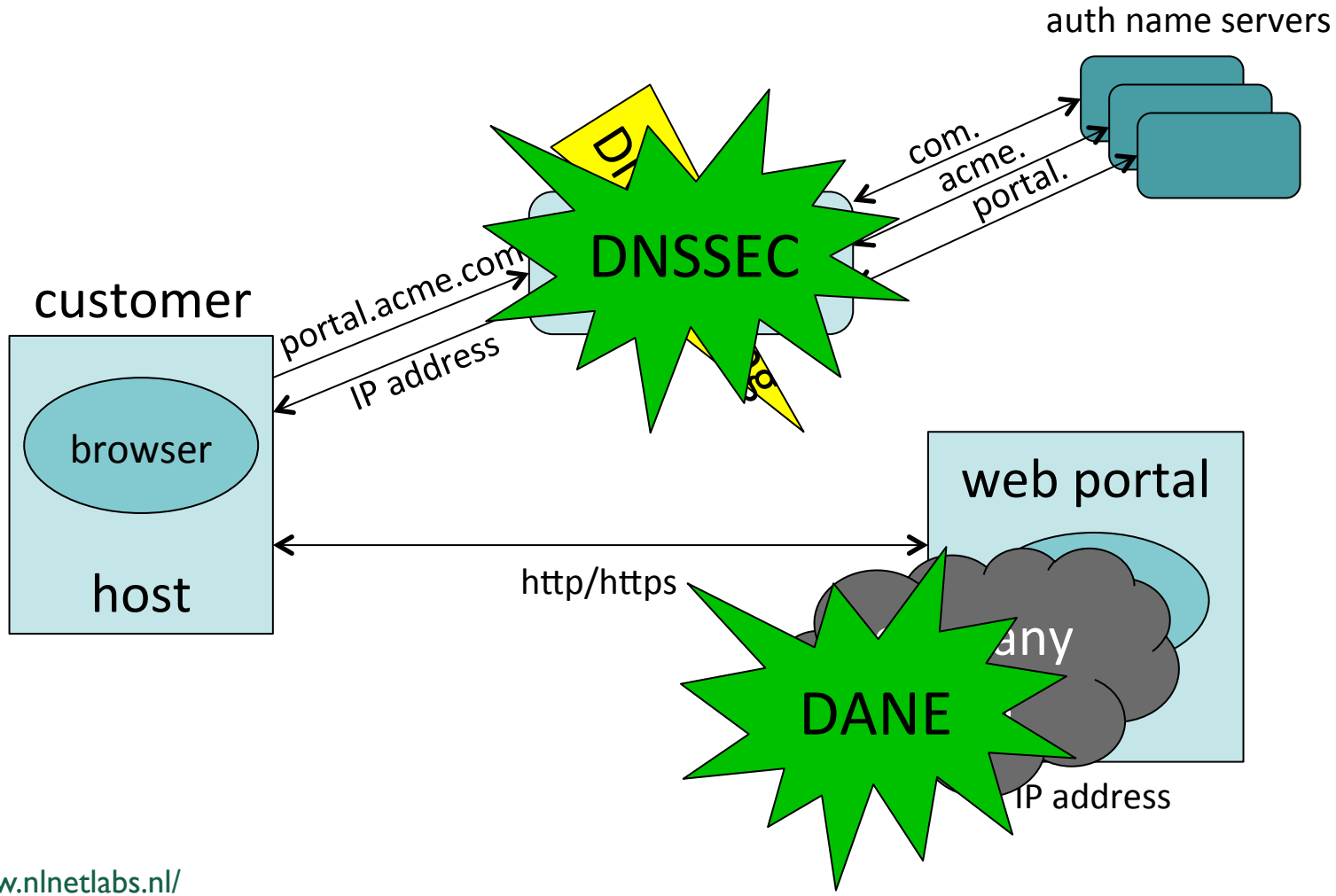


Dane allows DNS, secured by DNSSEC, to indicate which TLS/X.509 certificate is the right one to use.

This reduces the attack footprint of TLS significantly.

credits wes.hardaker@parsons.com

DNS-based Secure Customer–Web Portal Interaction



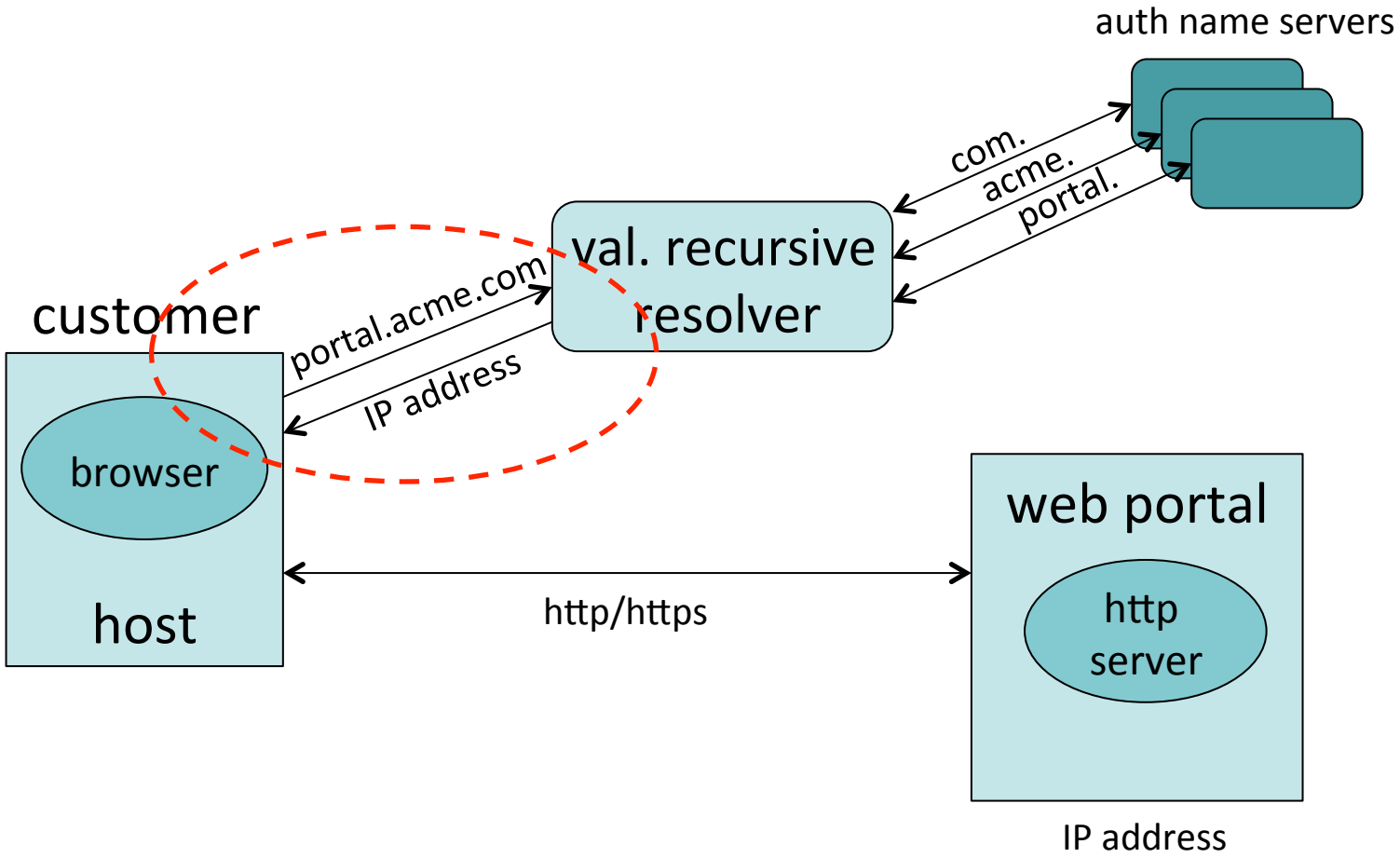
Closing the gap

SECURING THE FIRST MILE

The First Mile: From Host to Resolver

- Host/application DNS reliance on validating full resolver
  - resolver in trust realm?
  - resolver in local network, ISP, or open validating recursor (Google Public DNS, OpenDNS, OpenNIC DNS, Level 3, Verisign, …)
- Privacy and authentication of resolver
  - DNS queries considered privacy sensitive information

The First Mile: From Host to Resolver



DPRIVE: DNS over TLS

- Host stub resolver or application queries recursive resolver over encrypted TLS
  - TLSA records for stub/app to full recursor
- Privacy
  - DNS queries to resolver are encrypted on the wire
- In-band authentication of recursive resolver
  - TLSA chain extension (draft-ietf-tls-dnssec-chain-extension)
  - not solved yet: resolver IP configured on host or with DHCP

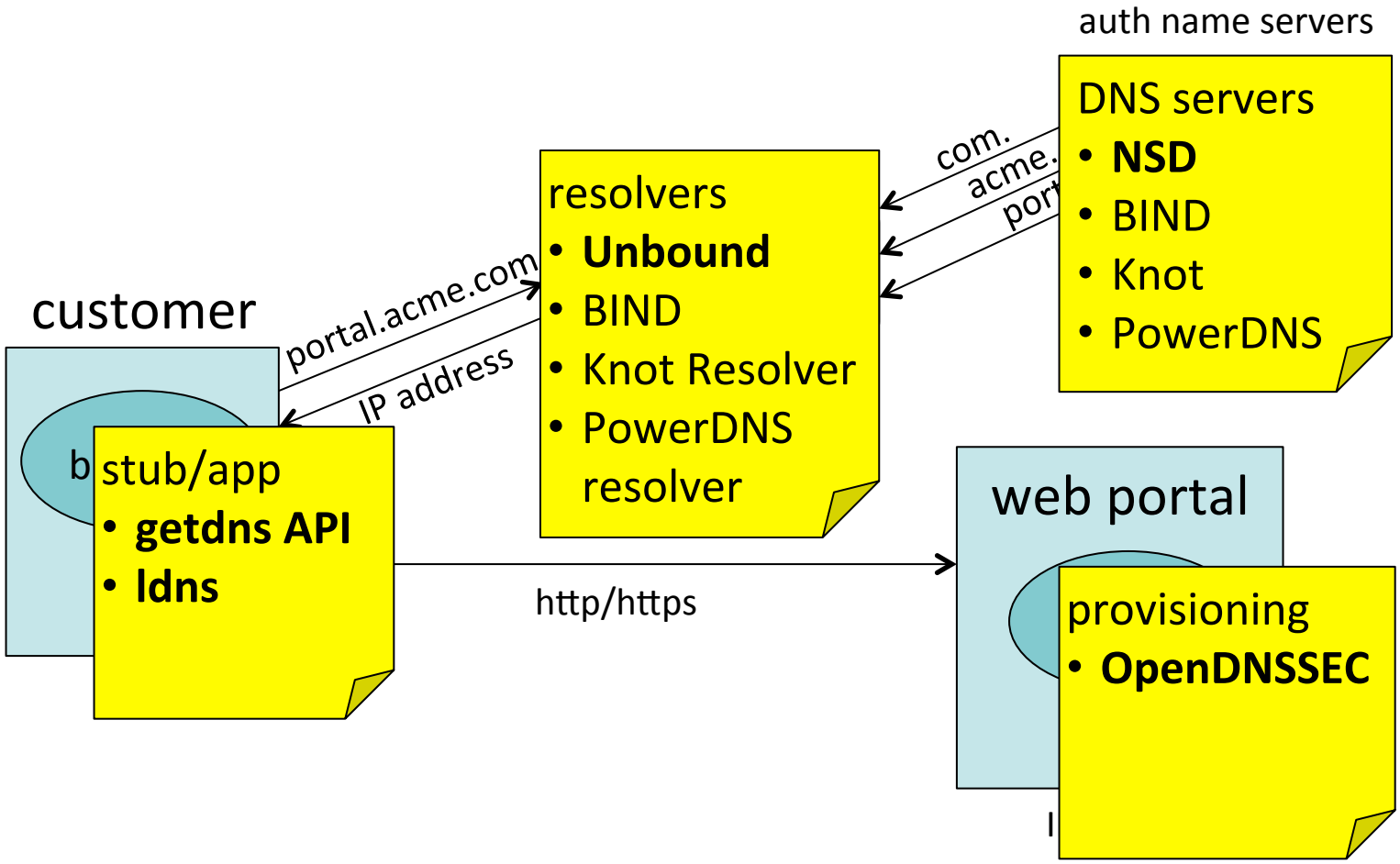
OTHER SHOWCASES OF DNSSEC, DANE AND DPRIVE

Email and SMTP

XMPP/CHAT

WRAPPING UP

Open Source Software for Security from the Ground Up



Summary

- DNSSEC, DANE and new DPRIVE bring security to next level
- Deploy DNSSEC!
  - not trivial, but open source deploy and provisioning tools are available
  - DANE and DPRIVE for “free” with DNSSEC
- Encrypt all in face of privacy and confidentiality (RFC 7624)