DNS Privacy

Implementation and Deployment

DNS WG, RIPE 74, May 2017

Benno Overeinder
NLnet Labs

http://www.nlnetlabs.nl/

Why DNS Privacy?

- IAB published RFC 6473: “Privacy Considerations for Internet Protocols”, July 2013
- Snowden revelations, June 2013
- RFC 7258: “Pervasive Monitoring is an Attack”, May 2014
- RFC 7624: “Confidentiality in the Face of Pervasive Surveillance: A Threat model and Problem Statement”, August 2015

coincidental, but what a timing!

But Wait… DNS and Privacy?

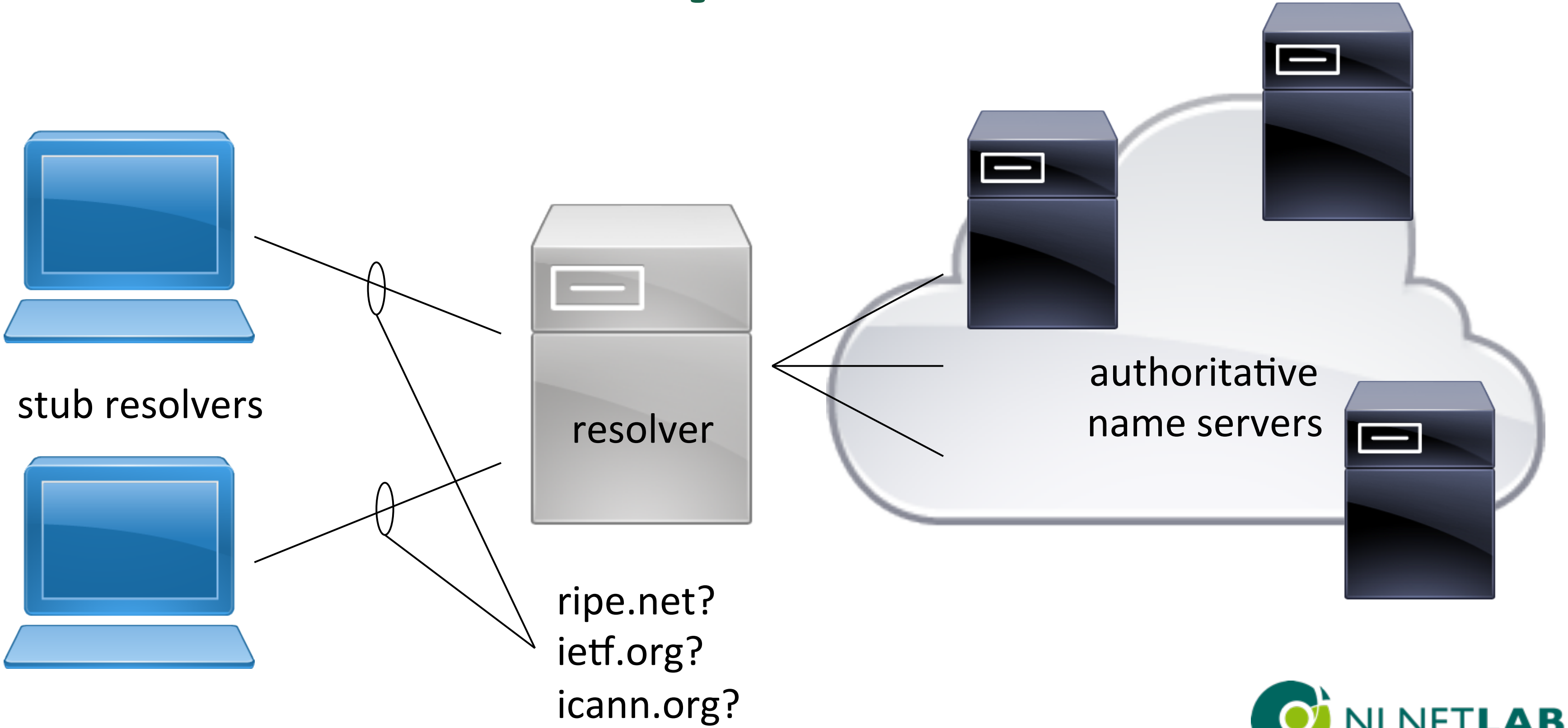
?

But Wait... DNS and Privacy?

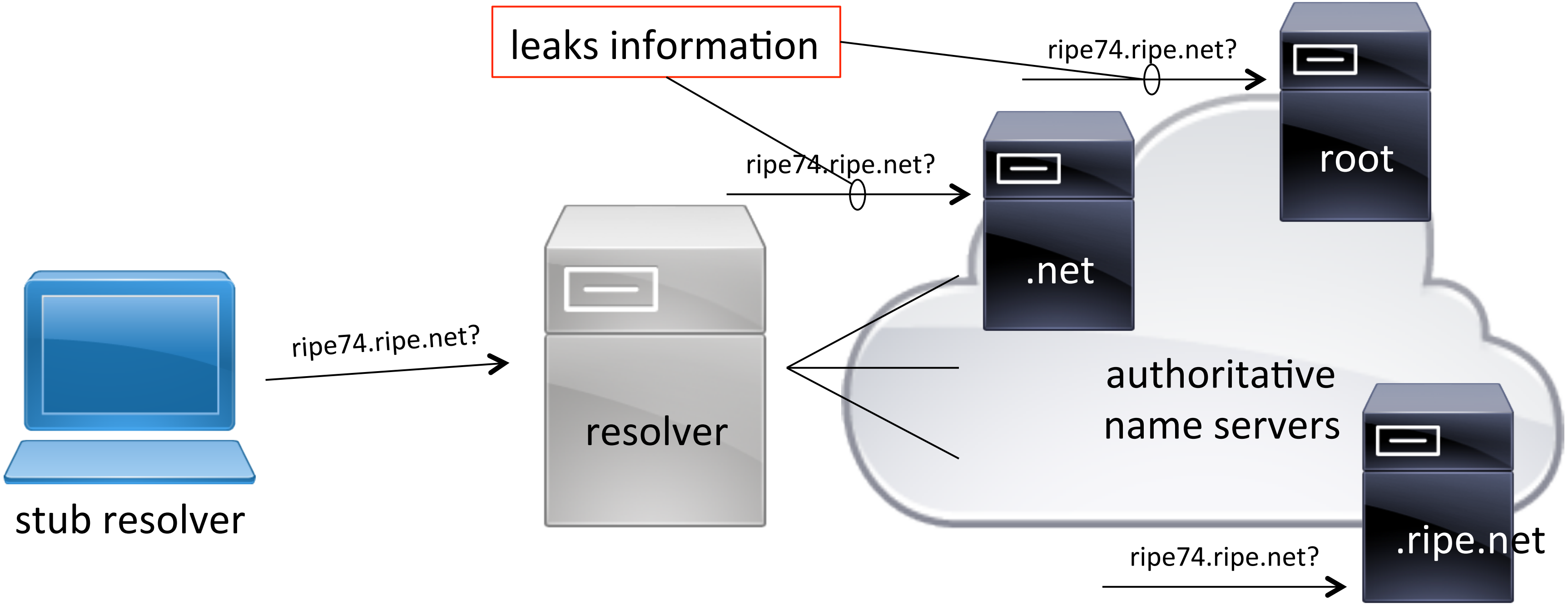
- RFC 7626: “DNS Privacy Considerations”, August 2015
- Debunk “the alleged public nature of DNS data”
- Data might be public, but a DNS transaction is not (or should not be)

ATTACKS

The First/Last Mile



DNS Information Leakage



Etc. and More Information

- Excellent IETF tutorial by Sara Dickinson (Sinodun)
  - Background information
  - Other attack or DNS disclosure scenarios
  - Recent IETF RFCs and IETF WG activities
  - https://www.ietf.org/meeting/97/tutorials/dns-privacy.html
- https://dnsprivacy.org/

IMPLEMENTATION

Protecting the First/Last Mile

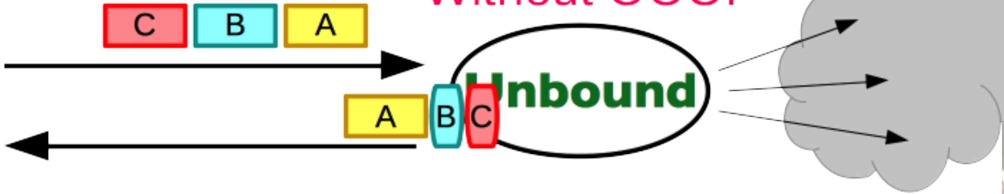
- Encrypt your DNS traffic
  - STARTTLS
  - TLS
  - DTLS
  - Confidential DNS draft
  - DNSCurve and DNSCrypt (not in IETF)

DNS over TLS

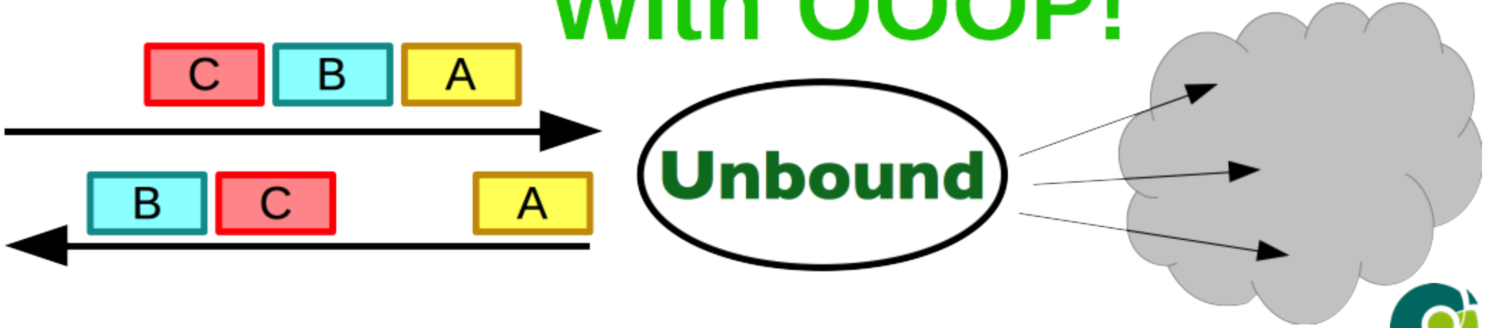
- DNS queries to resolver via (authenticated) TLS connections
- Requires "tuning" for DNS over TCP/TLS
  - optimise session setup & resumption
    - TCP Fast Open and TLS session resumption
  - pipelining & out-of-order processing
    - see next slide
  - robust TCP management of many connections
    - learn from HTTP servers & proxies

Out-of-Order Processing

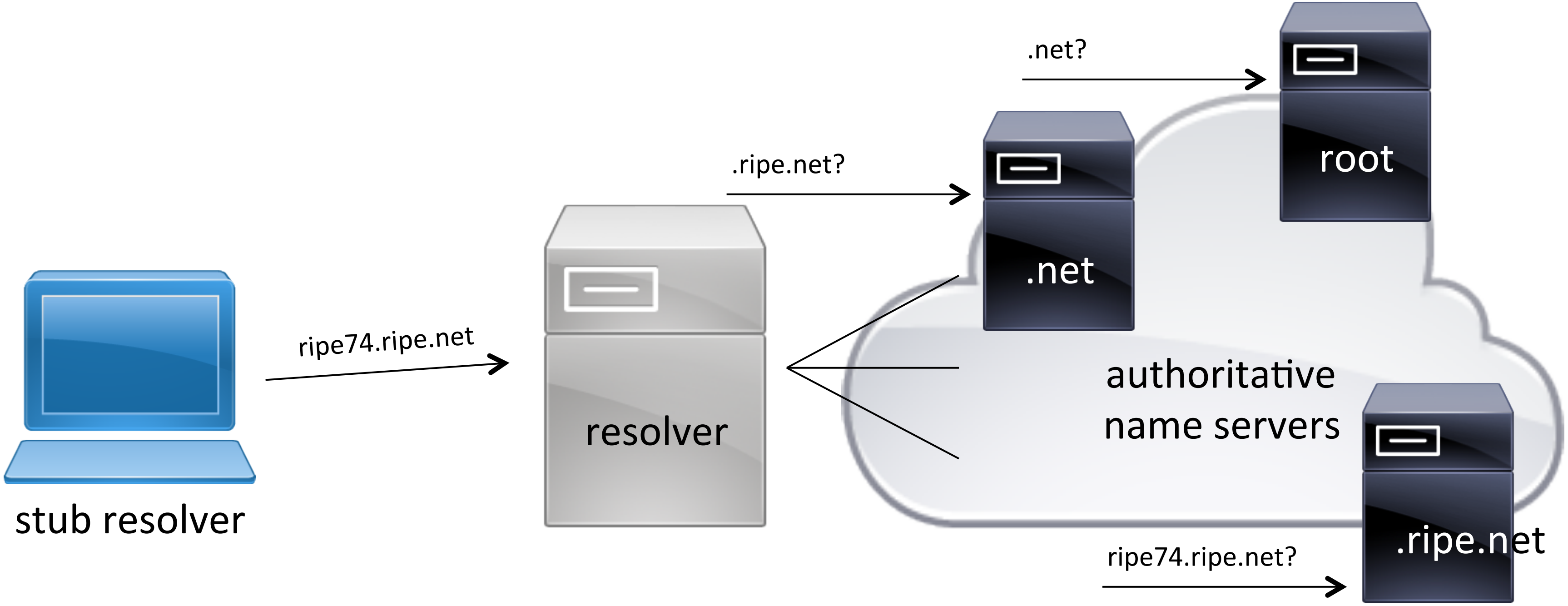
Without OOOP



With OOOP!

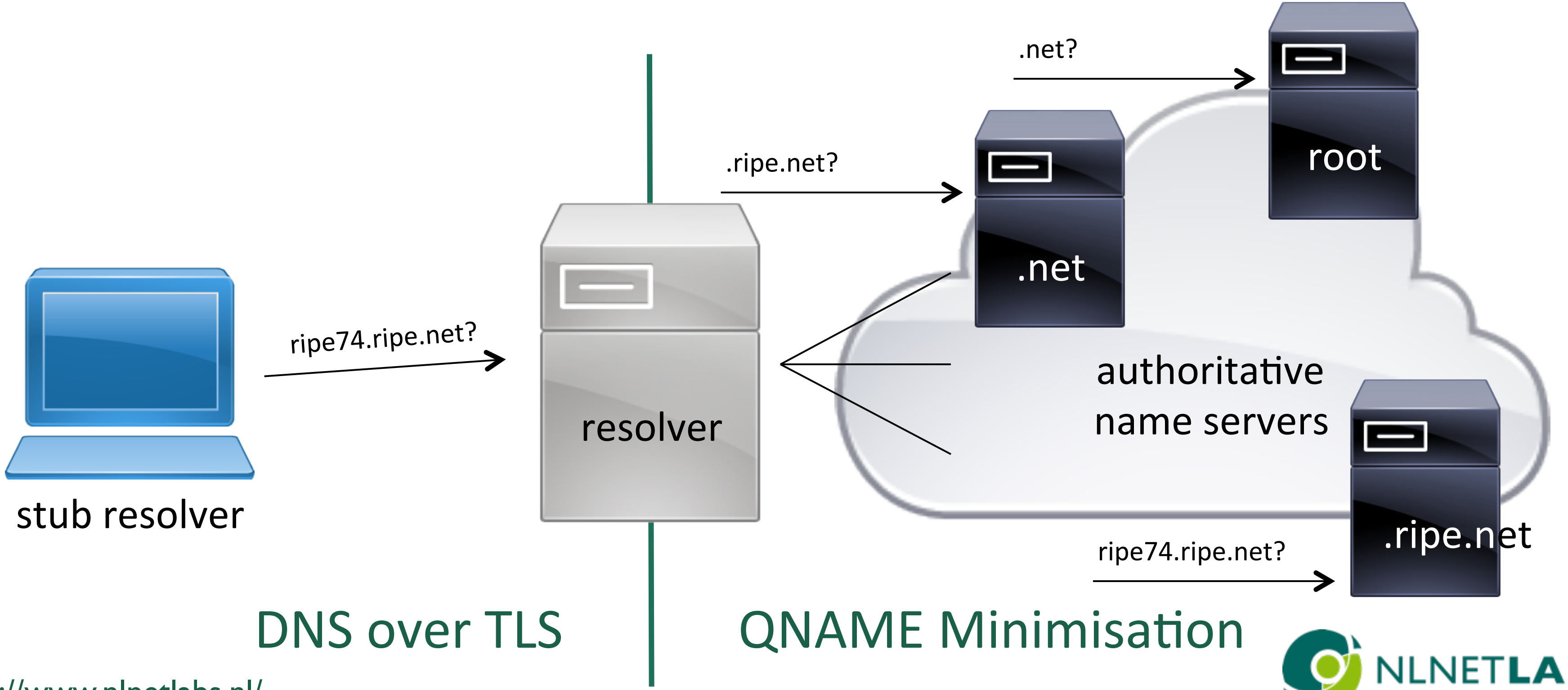


Reducing DNS Leakage: QNAME Minimisation



DEPLOYMENT

Deployment of DNS Privacy Enhanced DNS services



http://www.nlnetlabs.nl/

NLNETLABS

Deployment of DNS Over TLS

getdns
Unbound security

- getdns as stub
  - act as stub or full recursive
  - DNSSEC as a stub
    - even without validating upstreams
  - avoid DNSSEC roadblocks
    - works around upstreams that hamper DNSSEC
  - DNS64
    - signed IPv4 can be validated
  - DNS Privacy
    - DNS over TLS

- *Stubby* is getdns stub resolver with all privacy options enabled

DNS Privacy Enhanced Resolvers

- Available implementations
  - Unbound
  - Knot Resolver
  - Bind + TLS proxy (nginx or HAProxy)
- DNS-over-TLS test resolvers (see dnsprivacy.net)
  - NLnet Labs/OARC/Yeti: Unbound
  - SURFnet/Sinodun: Bind + HAProxy/nginx
  - dkg: Knot Resolver

QNAME Minimisation Enabled Resolvers

- Implemented
  - Unbound
  - Knot Resolver
- In future release
  - Bind

WRAPPING-UP

Resources

- IETF DPRIVE Tutorial by Sara Dickinson and Daniel Kahn Gillmor
  - https://www.ietf.org/meeting/97/tutorials/dns-privacy.html
- DNS Privacy websites
  - Community, non-technical: dnsprivacy.org
  - Enterprise/corporate users: dnsprivacy.net
- getdns project website
  - getdnsapi.net

Acknowledgements & Questions?

- Acknowledgements
  - Sara Dickinson
  - Allison Mankin
  - Willem Toorop
  - getdns team
  - IETF hackathon participants

http://www.nlnetlabs.nl/