Privacy analysis of DNS resolver solutions

J.H.C. van Heugten

University of Amsterdam
MSc System and Network Engineering

July 3, 2018

UNIVERSITY OF AMSTERDAM

Introduction

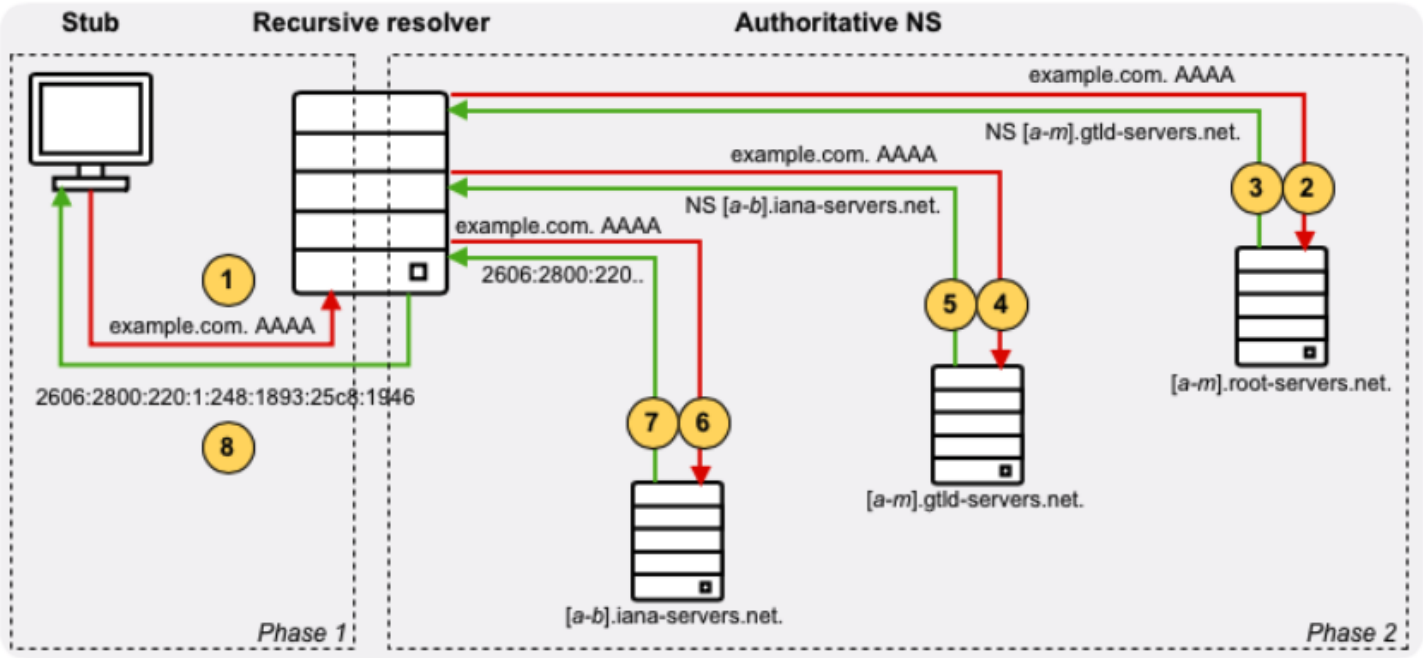
”We’ve updated our privacy policy”

Introduction

Research question:
How can modern techniques improve the privacy of DNS users?

- Regular DNS resolution
- The problem of DNS privacy
- Modern techniques to solve this
- Combine techniques for the best result

DNS resolution 1/2



DNS resolution 2/2

- DNS server types
  - Stub resolver
  - Recursive resolver
  - Forwarding resolver
  - Authoritative server
- Recursive/forwarder locations
  - Local
  - Remote
  - ISP
  - Public

The problem of DNS privacy

Eavesdropping & MITM

DNS data:

- QNAME
- QTYPE
- IP-addresses
- Responses
- Metadata (TTL, flags, etc.)

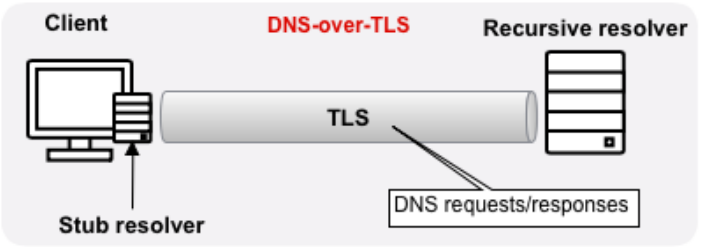
EDNS(0)

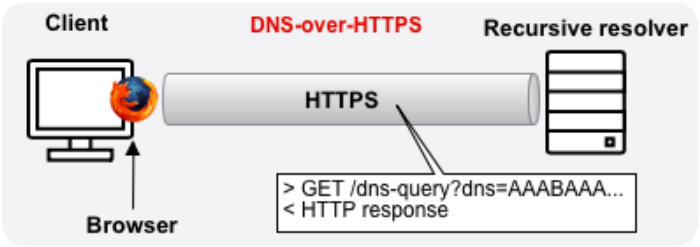
- Client subnet
- Client ID

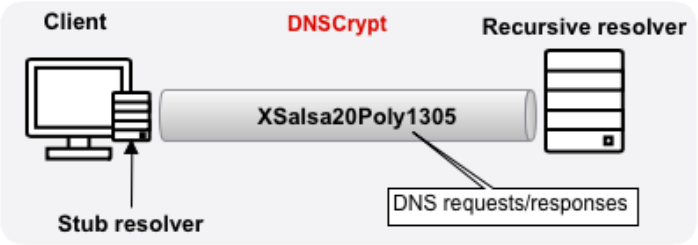
DNSSEC

Privacy techniques

- DNS-over-TLS
- DNS-over-HTTPS
- DNSCrypt
- Oblivious DNS
- DNSCurve
- QNAME minimisation

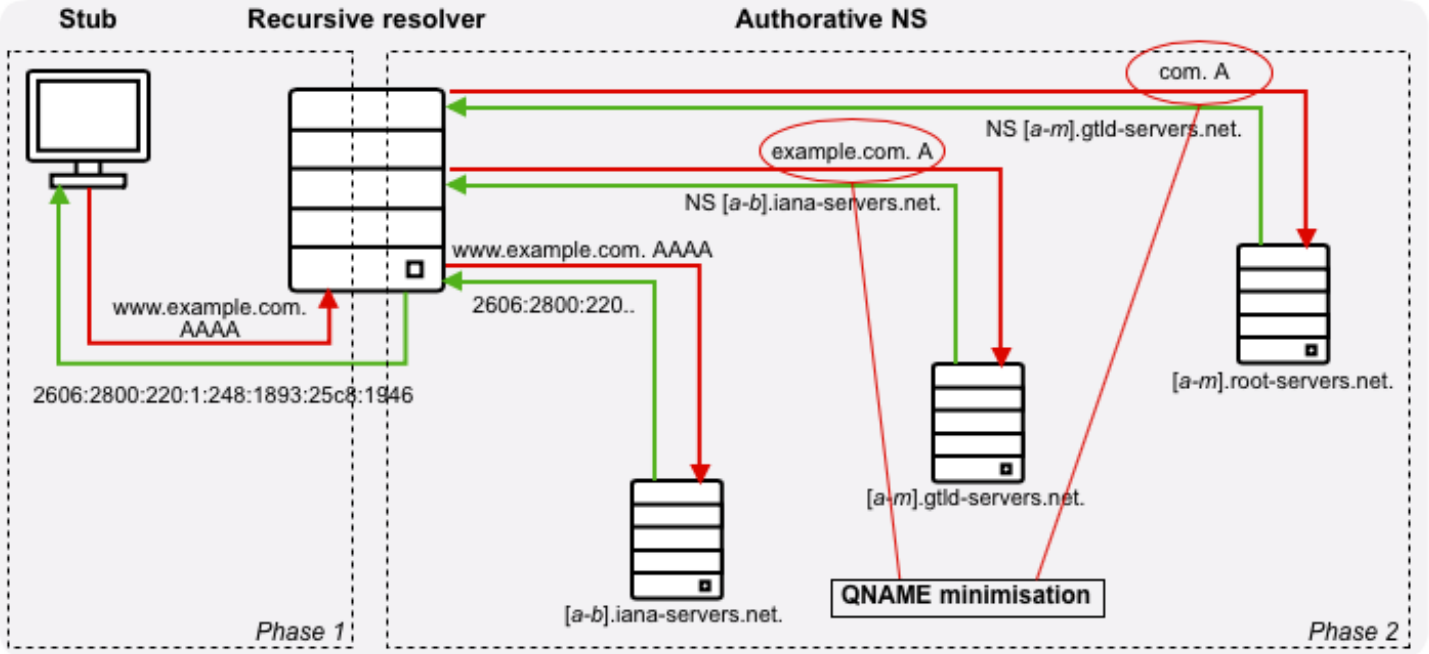






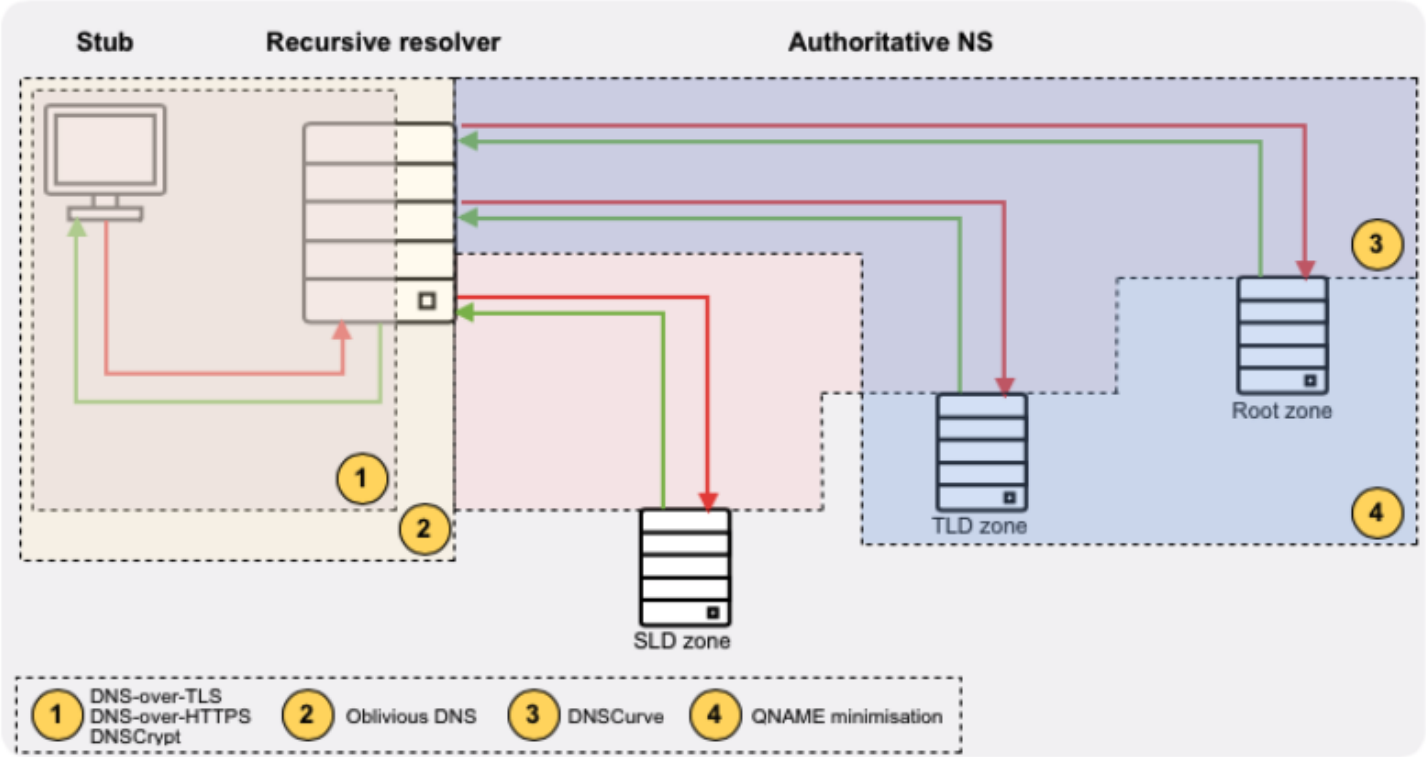
Privacy techniques

- Query Name (QNAME) minimisation



Privacy techniques

- Coverage of techniques



Combining techniques

Combining previous techniques and resolver types/locations together.

Techniques not available to the user:

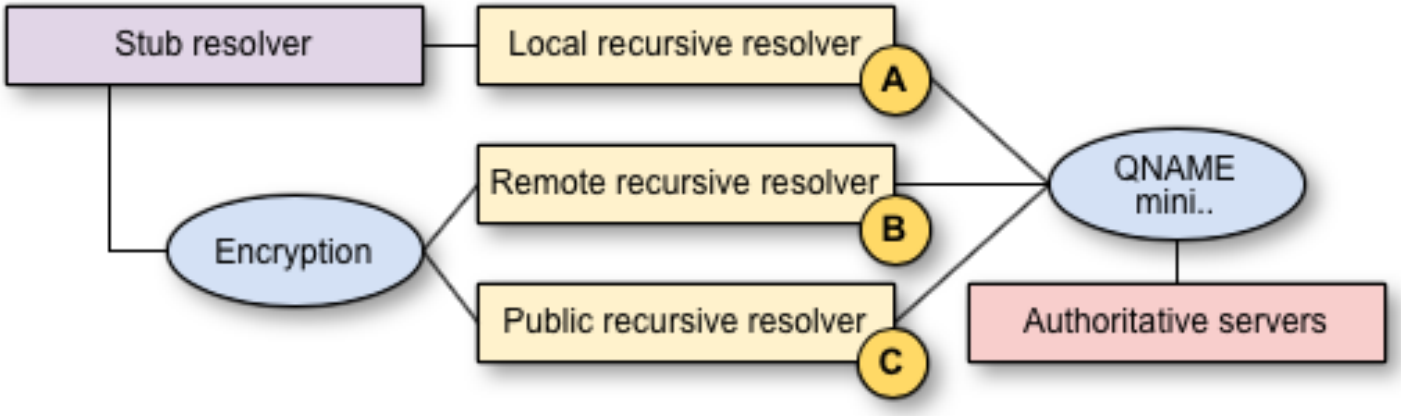
- Oblivious DNS
- DNSCurve

Do not use the ISP's resolver

- Regulation
- No support for techniques
- IP-address to user relation

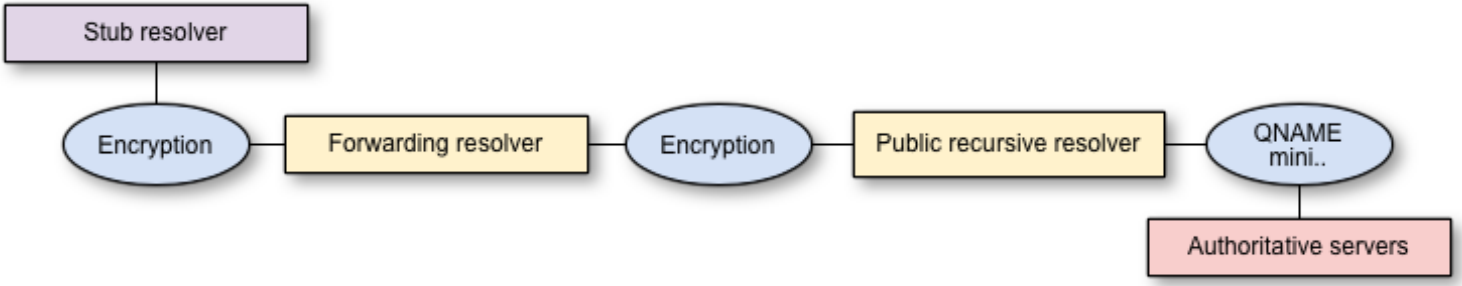
Combining techniques

Who do you trust with your data?



Combining techniques

Decouple data over different servers



And share the forwarding resolver with trusted friends...

Conclusion

Conclusion

- Work done
- Importance of caching
- Recursive resolver selection (ECS, logging)

Discussion & future work:

- TLS SNI
- DNS padding
- Overlay networks (Tor)
- Multiple public resolvers

Acknowledgements

Supervisors

Ralph Dolmans, NLnet Labs
Martin Hoffmann, NLnet Labs