Domain Name System without Root Servers

Matthäus Wander,
Christopher Boelmann, Torben Weis

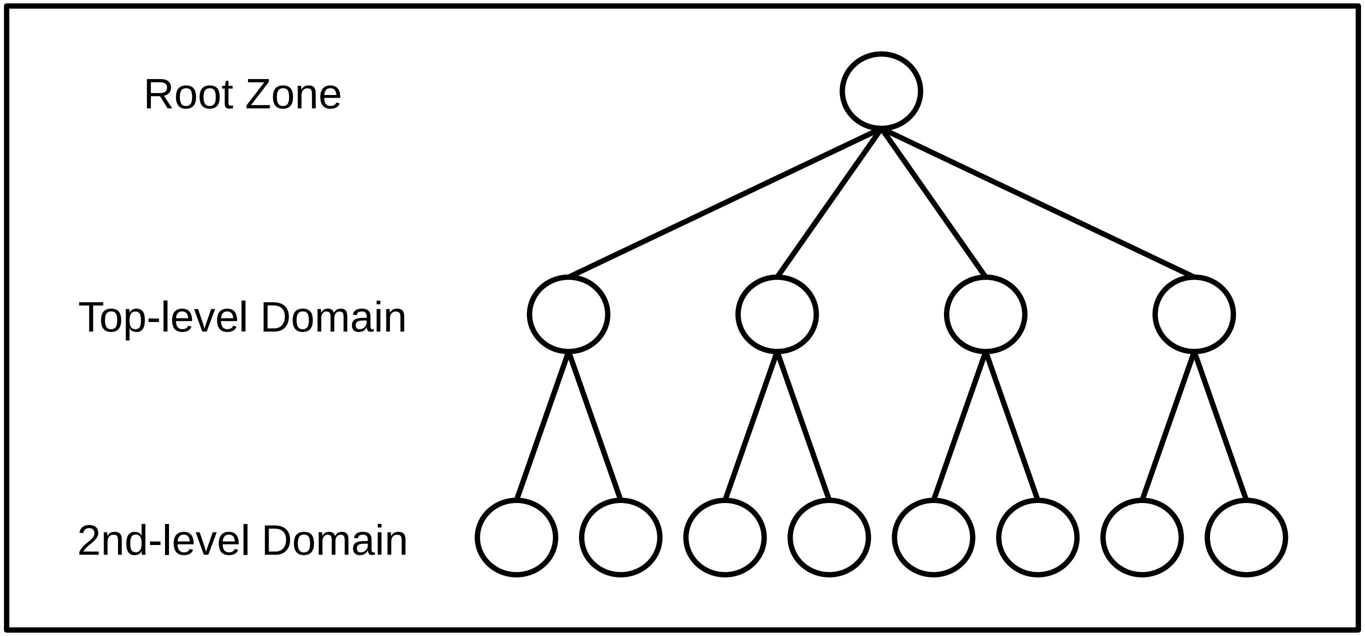
<matthaeus.wander@uni-due.de>

CRiSIS 2017

Dinard, France, September 21, 2017

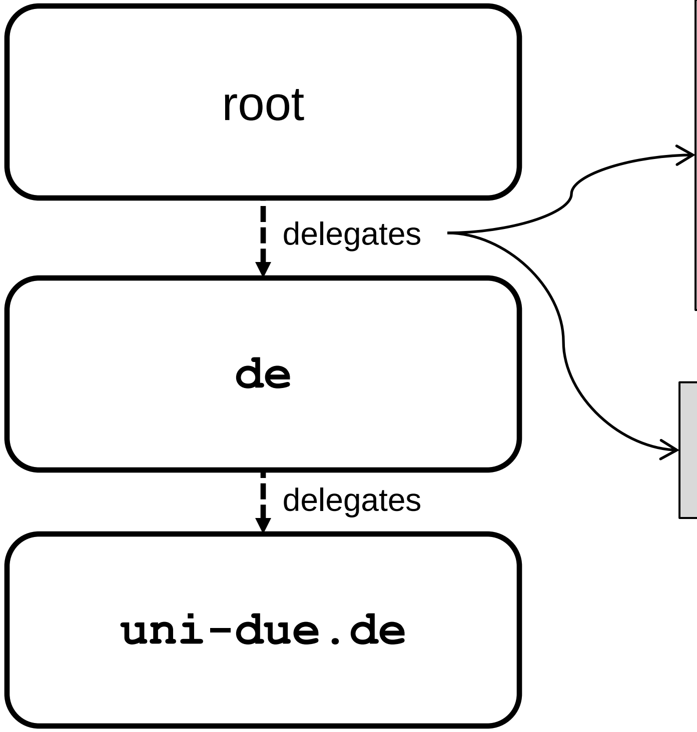
Domain Name System

- DNS is a critical infrastructure in the Internet
  - Authenticity secured with DNSSEC signatures
  - Hierarchical trust model



Chain of Trust

Parent delegates trust
for subnamespace



IP addresses for `de.`

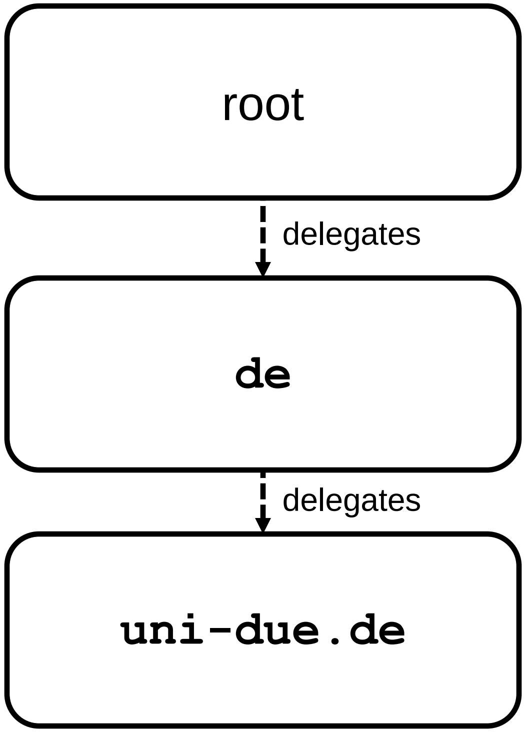
```
de.  IN NS a.nic.de.
de.  IN NS f.nic.de.

a.nic.de.  IN A  194.0.0.53
f.nic.de.  IN A 81.91.164.5
```

```
de.  IN DS   AAB73083B9EF7...
de.  IN RRSIG S7IOGXtvRtx...
```

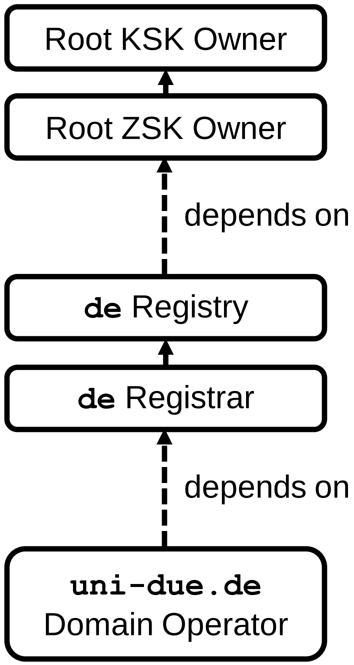
Secure fingerprint of
public key for **`de`**

Chain of Trust

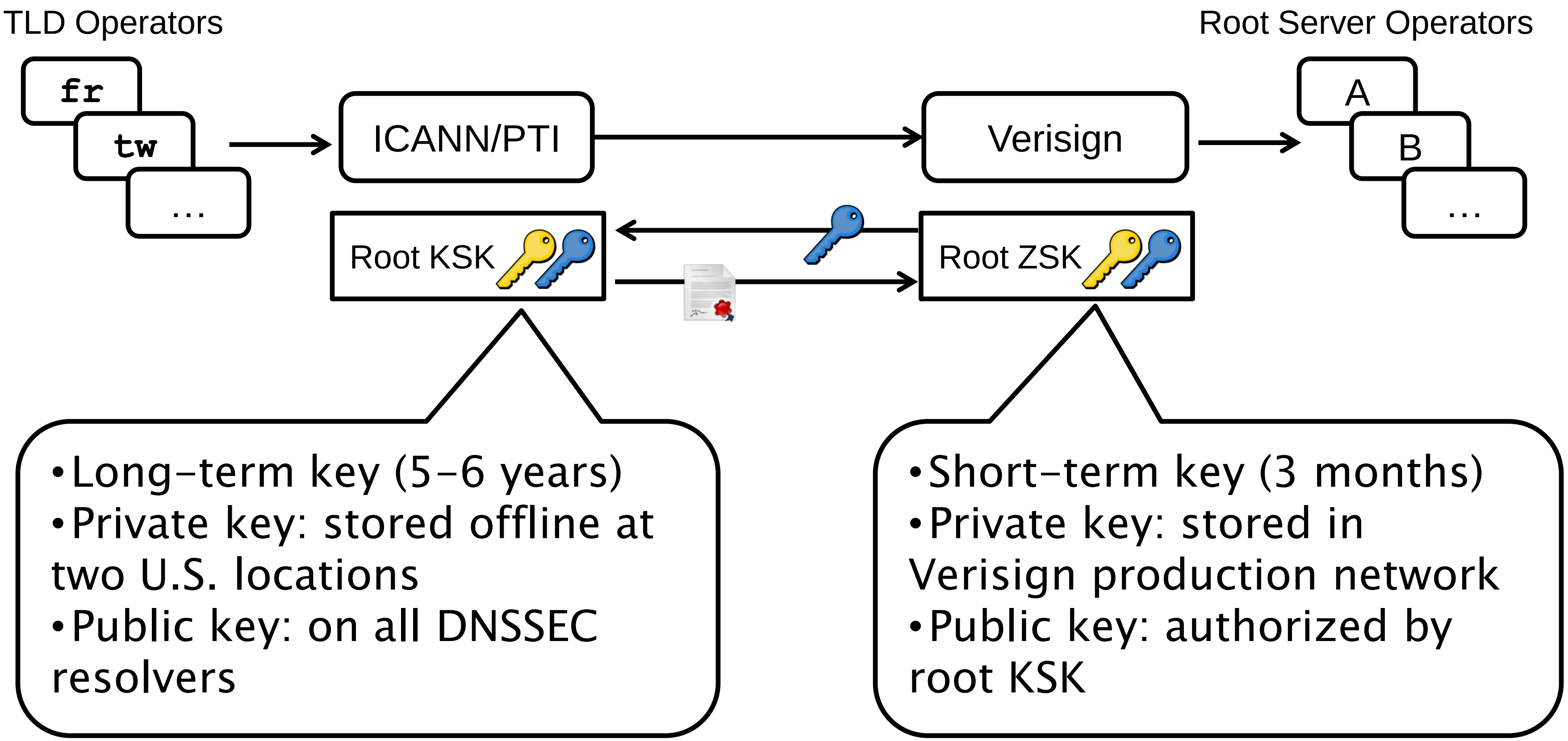
Parent delegates trust for subnamespace



Domain owner depends on all parents



Root Zone Management



TLD Operators

fr

tw

…

ICANN/PTI

Verisign

Root Server Operators

A

B

…

Root KSK

Root ZSK

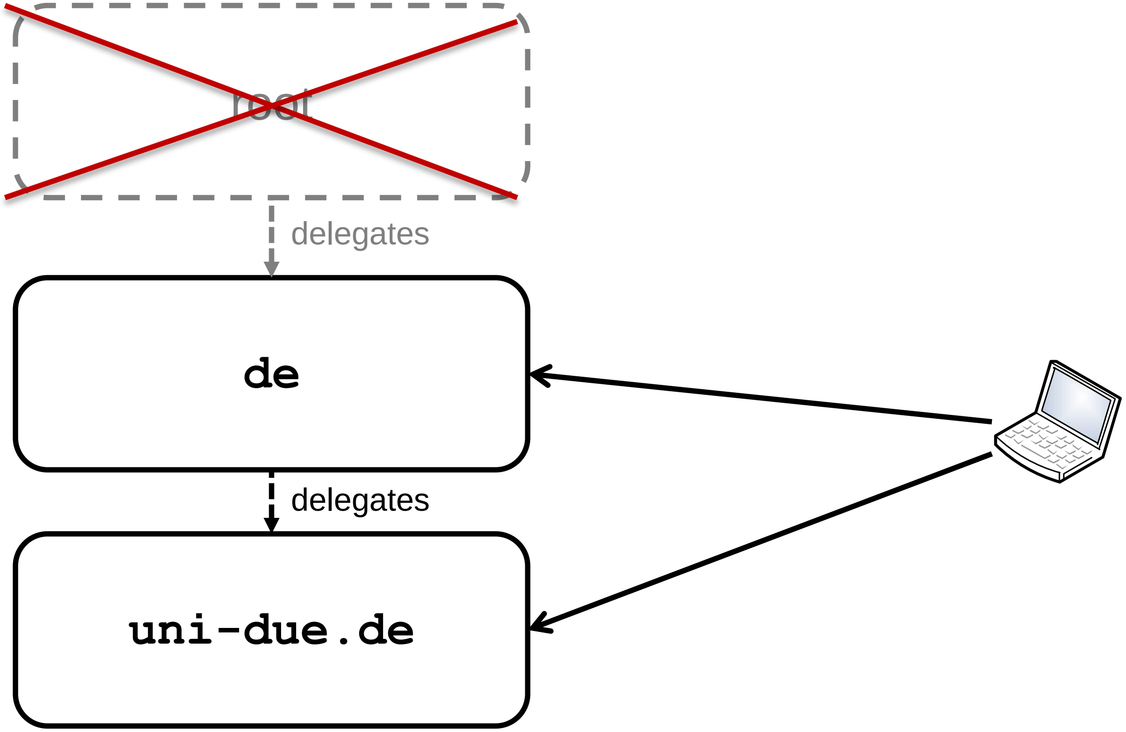
- Long-term key (5-6 years)
- Private key: stored offline at two U.S. locations
- Public key: on all DNSSEC resolvers

- Short-term key (3 months)
- Private key: stored in Verisign production network
- Public key: authorized by root KSK

PROPOSAL

DNSSEC without Root

- Skip root and start resolution on top level?
  - Root zone is rather small (2 MByte)

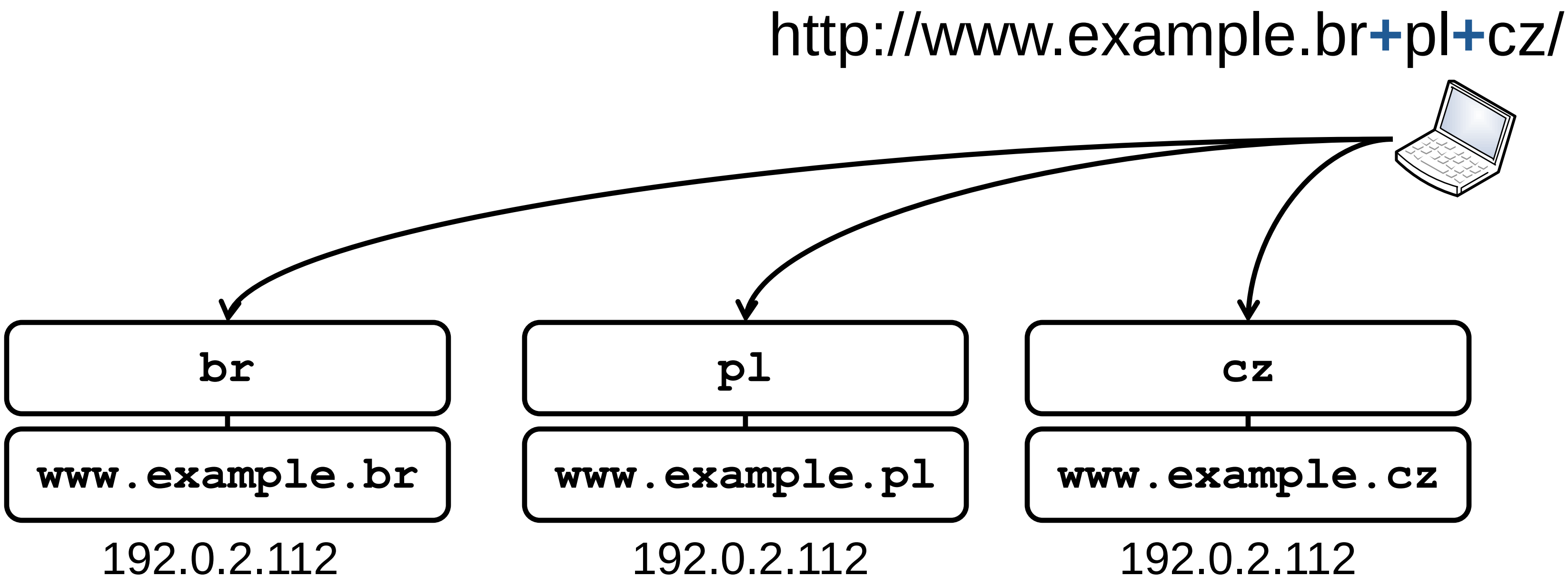


Motivation

- Trust
  - Avoid centralization in single point of trust
  - Root can tamper with any top-level domain
  - Root keys are held within U.S. jurisdiction
- Reliability
  - No dependency on root operations
- Client Privacy
  - One less level for leaking query names

Use Case

- Redundant domain names in URL
  - Resolve multiple names, majority voting over result
  - No organization can tamper with all three names

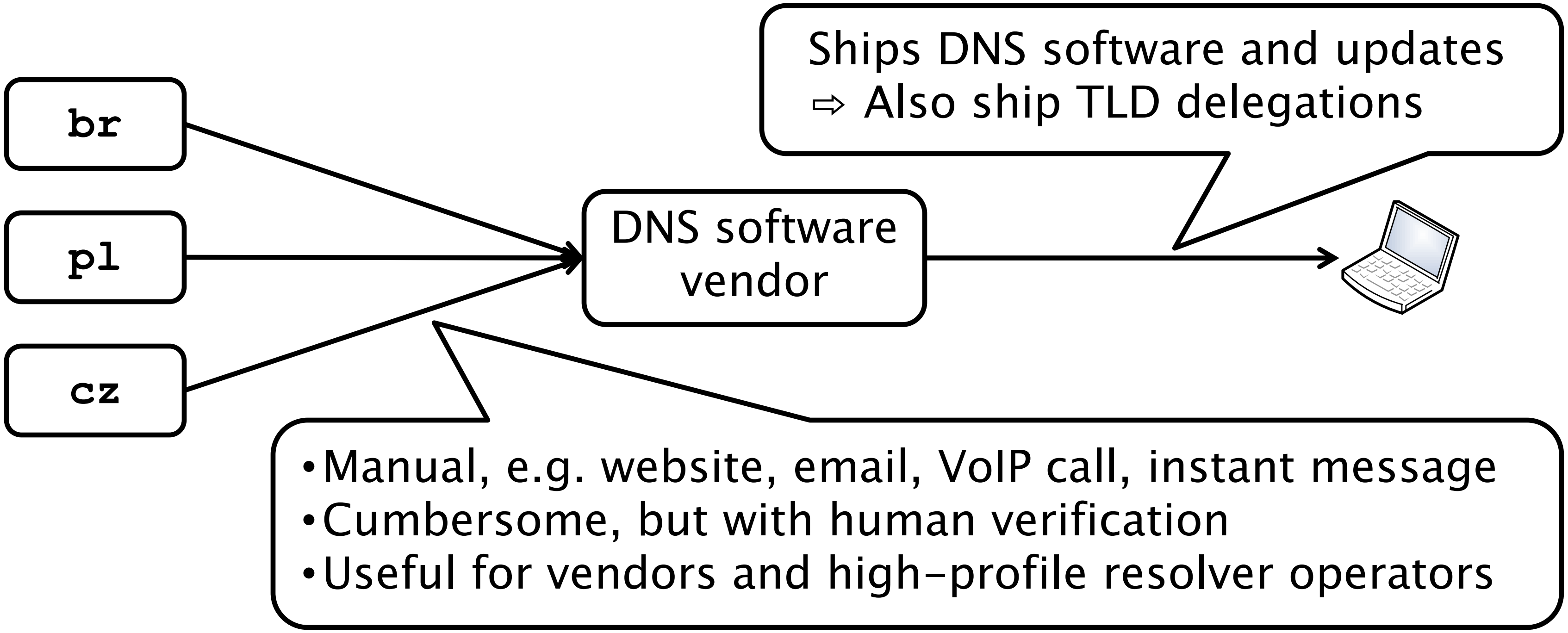


Challenges

- Resolver needs the root zone contents
- **Challenge**: How to retrieve the TLD delegations?
  - ⇨ Bootstrapping
- TLD delegations change occassionally
- **Challenge**: How to update the TLD delegations?
  - ⇨ Priming: update server IP addresses
  - ⇨ Trust anchor update: update public keys
- Solutions exist on root level
  - ⇨ Use similar mechanisms for top-level domains

Bootstrapping

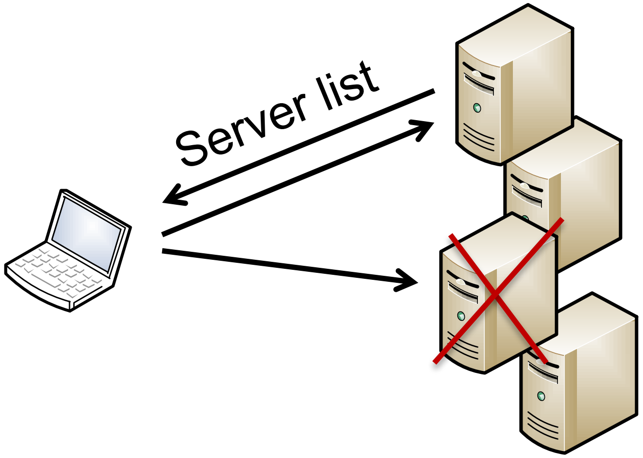
- Objective: retrieve IP addresses and keys of TLD
- Automatically over existing trusted path
- Manually from TLD operators



Ships DNS software and updates
⇨ Also ship TLD delegations

- Manual, e.g. website, email, VoIP call, instant message
- Cumbersome, but with human verification
- Useful for vendors and high-profile resolver operators

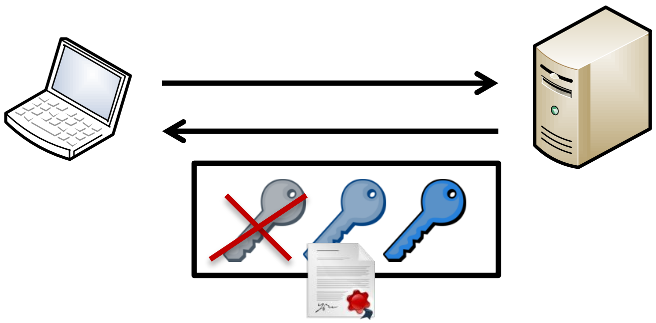
Priming: Update Server Addresses



[RFC 8109]

- Query TLD for set of server IP addresses
  - Timeout? ⇨ query another known server
  - Succeeds if at least one known server responds
- Check all TLDs regularly for new IP addresses

Update Trust Anchors



[RFC 5011]

- Query TLD for set of public keys
- Key rollover
  - Introduce new key (signed by well-known key)
  - Later revoke and remove old key
- Check all TLDs regularly for new public keys

Commitment and Update Periods

- TLDs must keep one server address and one public key for commitment period Δt
  - e.g. $\Delta t = 1$ year
- Resolvers must update every $\Delta u < \Delta t$
  - If update has been missed: bootstrapping required
- Opt-in: let operators choose
  - TLD: signalize rootless support during bootstrapping
  - Rootless and traditional approach can coexist in the same system

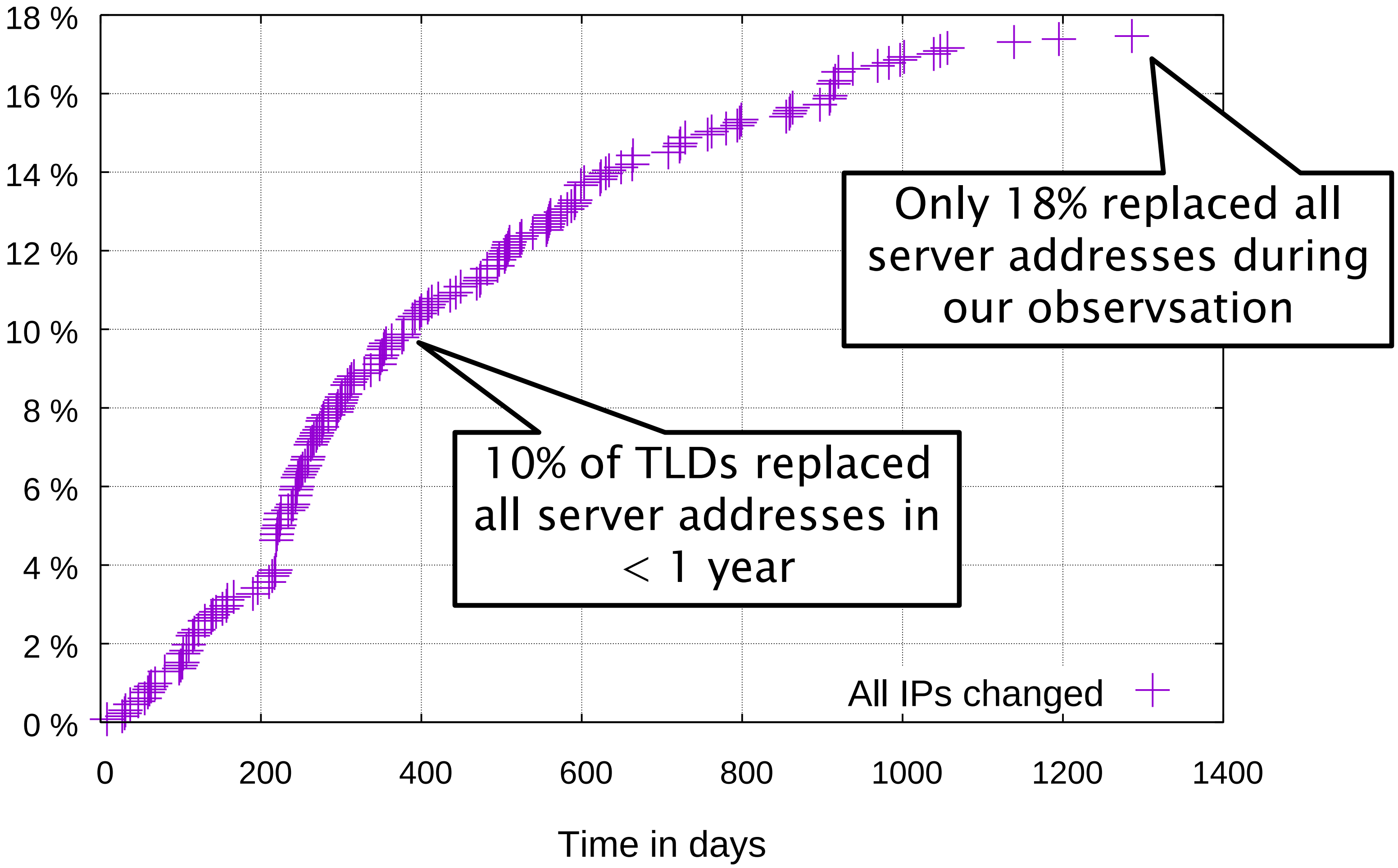
Feasibility Study

Will It Blend?

Feasibility Study

- Research questions:
  - How long until a TLD replaces all server addresses?
  - What is the availability with different update Δu?
  - How often do TLDs replace their DNSSEC keys?
- 4-year measurement, every day
  - Download root zone to get TLD server addresses
  - Query TLD server for their public keys
- Data cleaning
  - We consider 1317 TLDs that existed for >1 year

IP Address Replacement

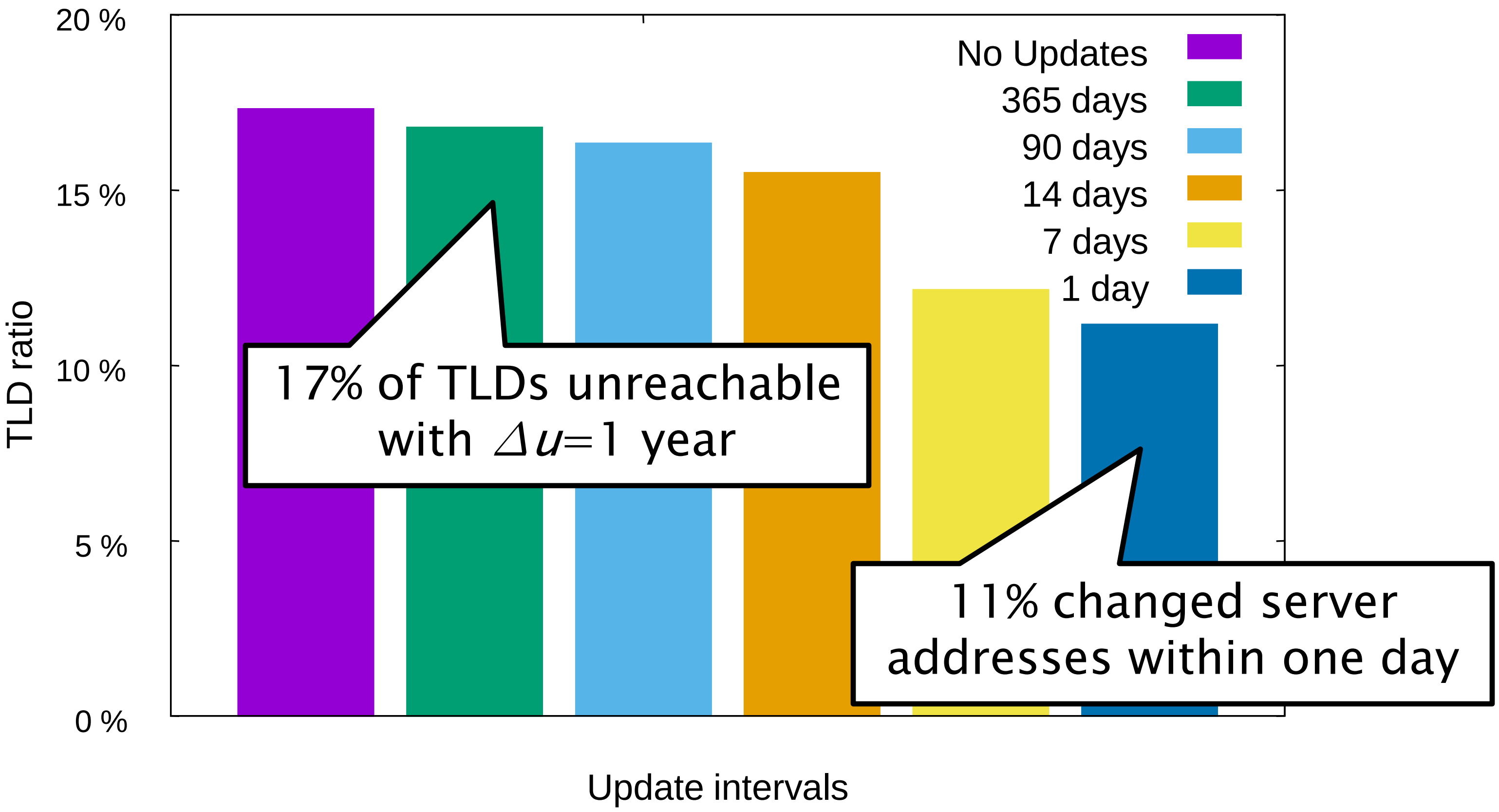


Only 18% replaced all server addresses during our observsation

10% of TLDs replaced all server addresses in < 1 year

How many TLDs would become unreachable?

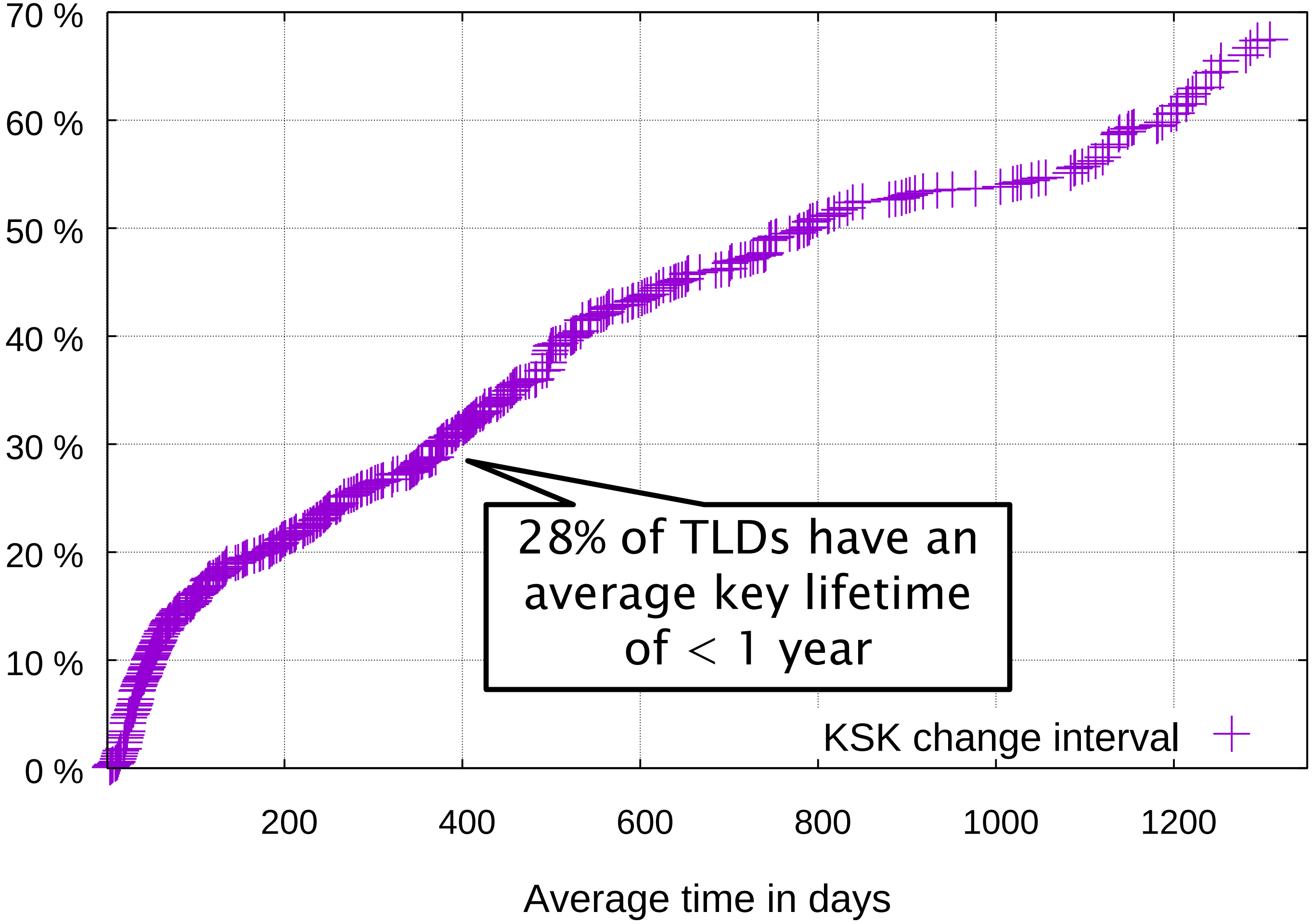
- Simulation with different update periods Δu



17% of TLDs unreachable with Δu=1 year

11% changed server addresses within one day

Average Key Rollover Interval



28% of TLDs have an average key lifetime of < 1 year

Conclusions

- Without root, there is one less authority to trust
  - We still need to trust the TLD operator that we choose
  - Drawback: cannot rely on root for emergency updates
- Approach requires long key rollover intervals
  - 4-year study shows suitability for 72% of TLDs
- Opt-in: operator chooses whether to go rootless
- Approach integrates within existing DNS
  - Shares characteristics of today‘s DNS ecosystem
  - Does not require a fundamentally new architecture