ETH zürich

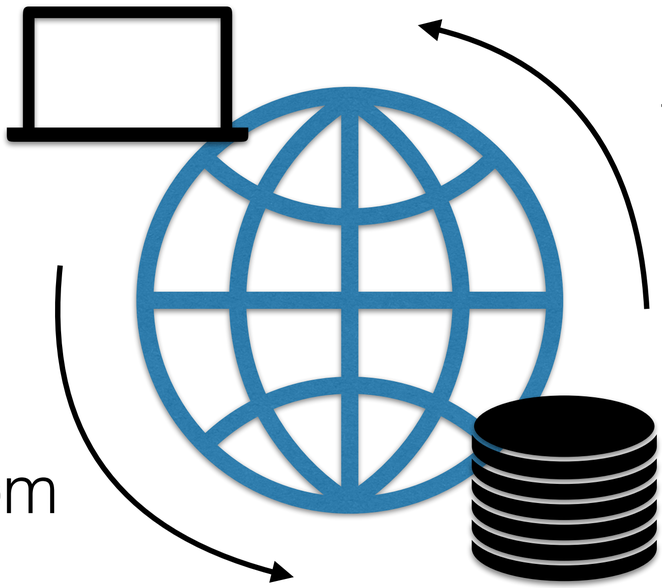
Network Security Group
Department of Computer Science

RHINE: Robust and High-performance Internet Naming with E2E Authenticity

Huayi Duan, Rubén Fischer, Jie Lou, Si Liu,
David Basin, and Adrian Perrig

NSDI 2023, Boston

Domain Name System (DNS) — Internet's phonebook and beyond



domain.com

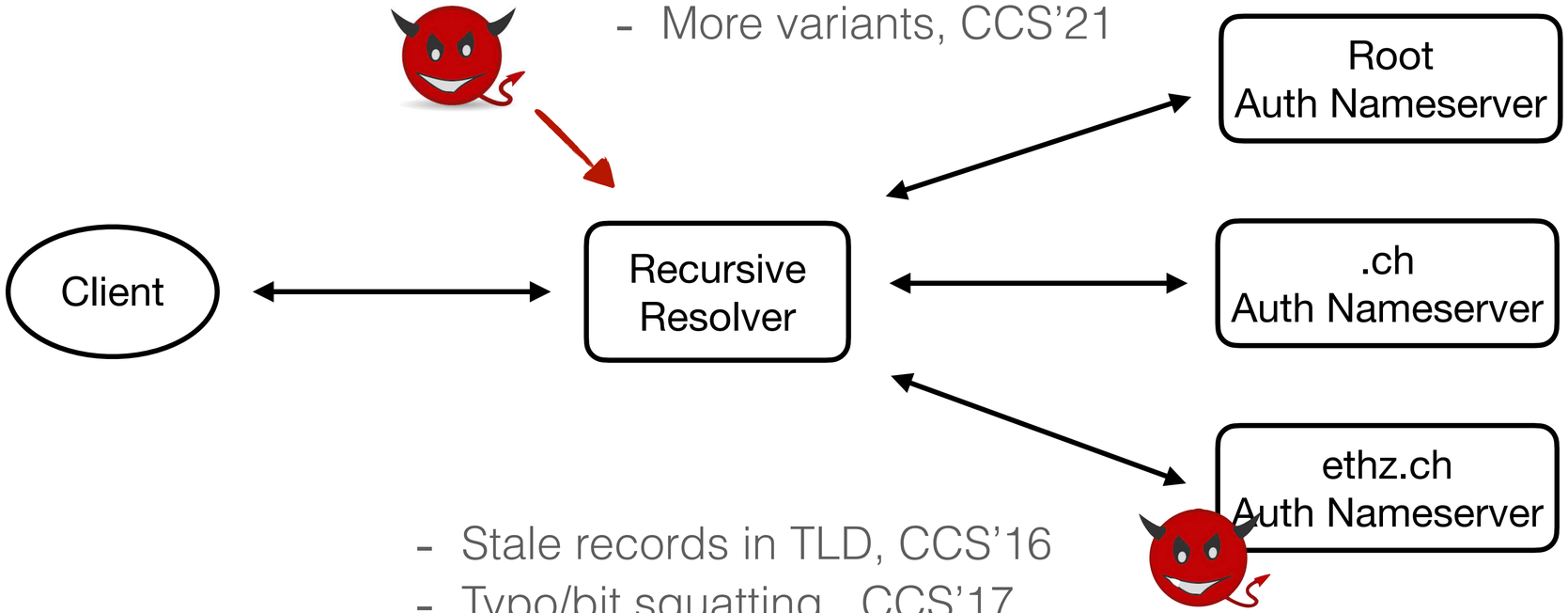
18.221.195.49

Versatile system supports
- load balancing
- content delivery
- email exchange (MX)
- service discovery (SRV)
- customised apps (TXT)
- …

DNS in a fast-moving threat landscape

Cache Poisoning
(Kaminsky, 2008)

- Fragmentation-based, CNS'13
- Poisoning forwarders, SEC'20
- SAD DNS, CCS'20
- More variants, CCS'21

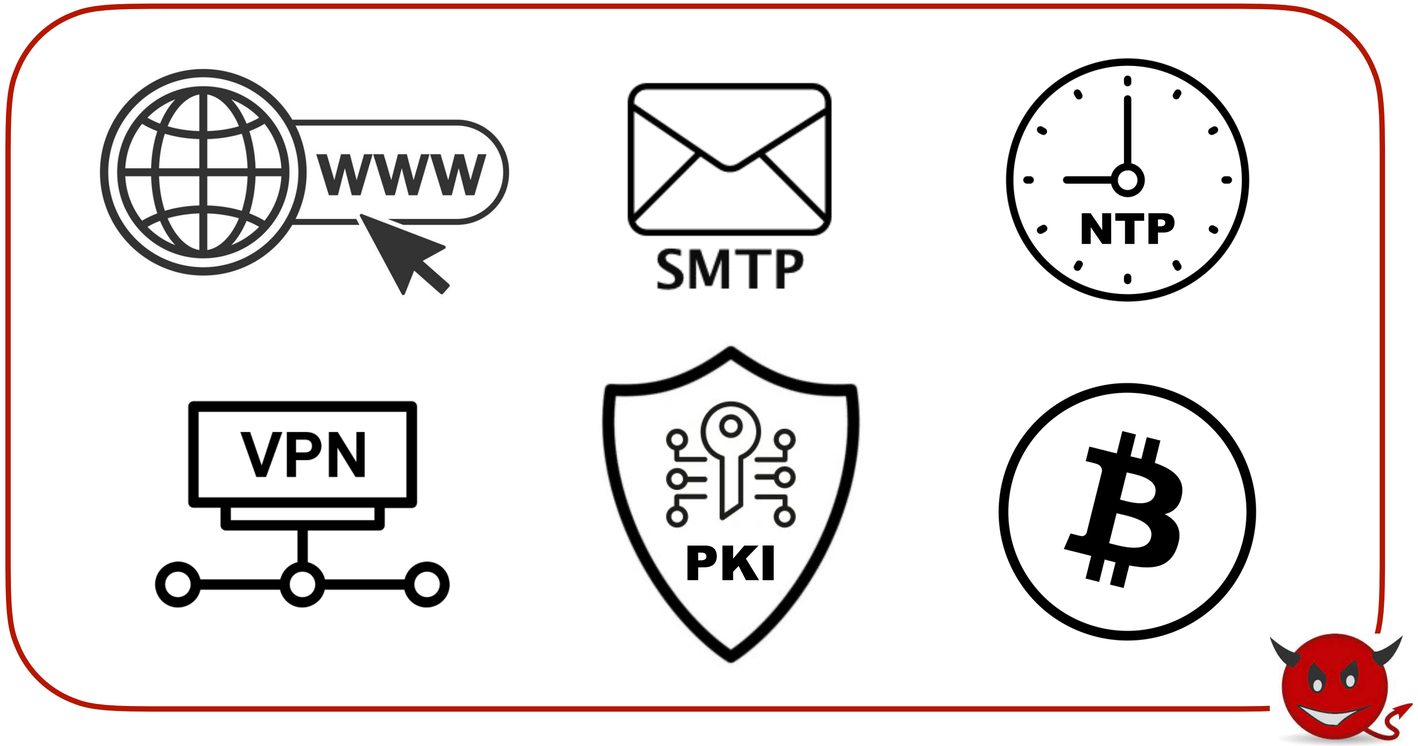


- Stale records in TLD, CCS'16
- Typo/bit squatting , CCS'17
- Stale records in 2LD, CCS'20
- Subdomain takeover, SEC'21

Domain Hijacking

DNS in a fast-moving threat landscape

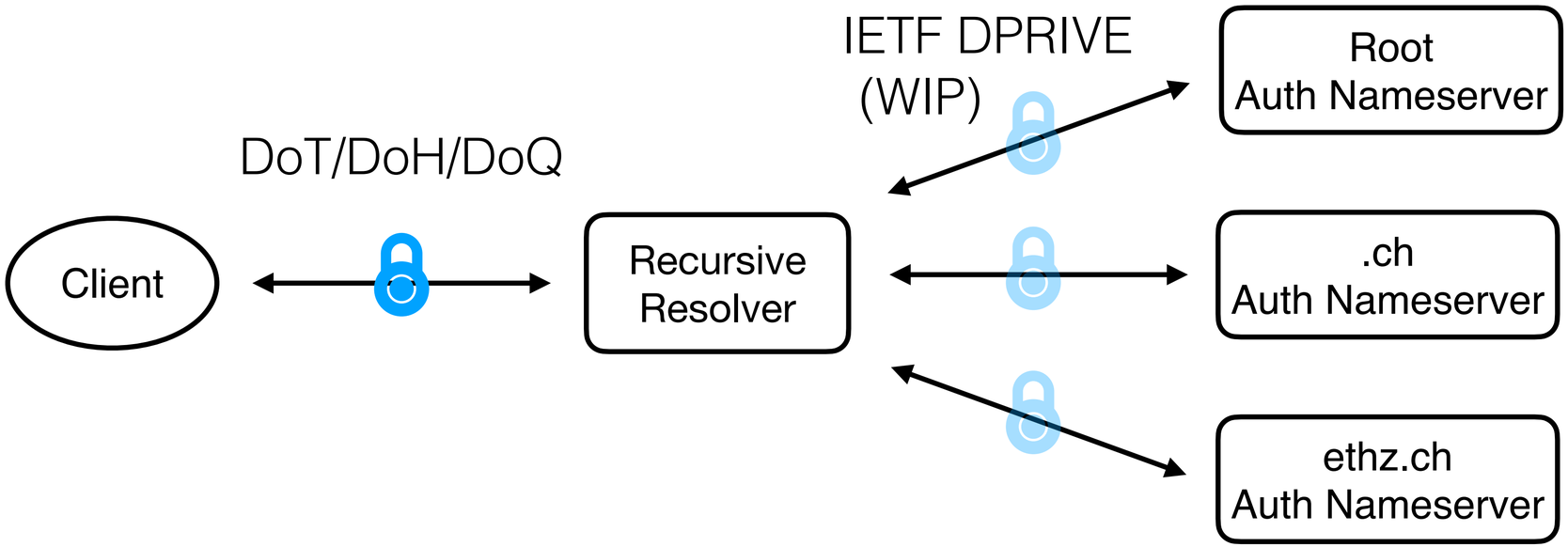
DNS attacks affect the entire Internet



Dai et al. *From IP to Transport and Beyond: Cross-Layer Attacks Against Applications*. SIGCOMM'21

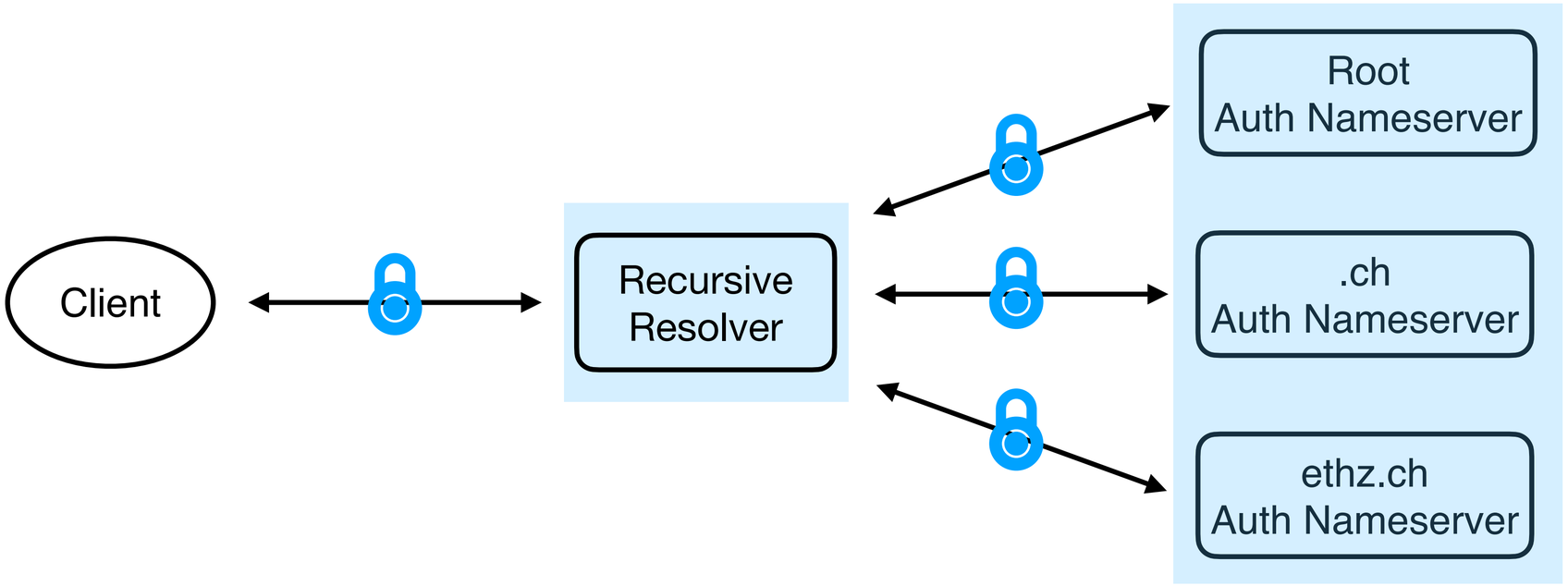
Dai et al. *The Hijackers Guide To The Galaxy: Off-Path Taking Over Internet Resources*. SEC'21

DNS security today — Secure channel



DNS security today — Secure channel limitation

Channel security $\not\Rightarrow$ E2E data authenticity

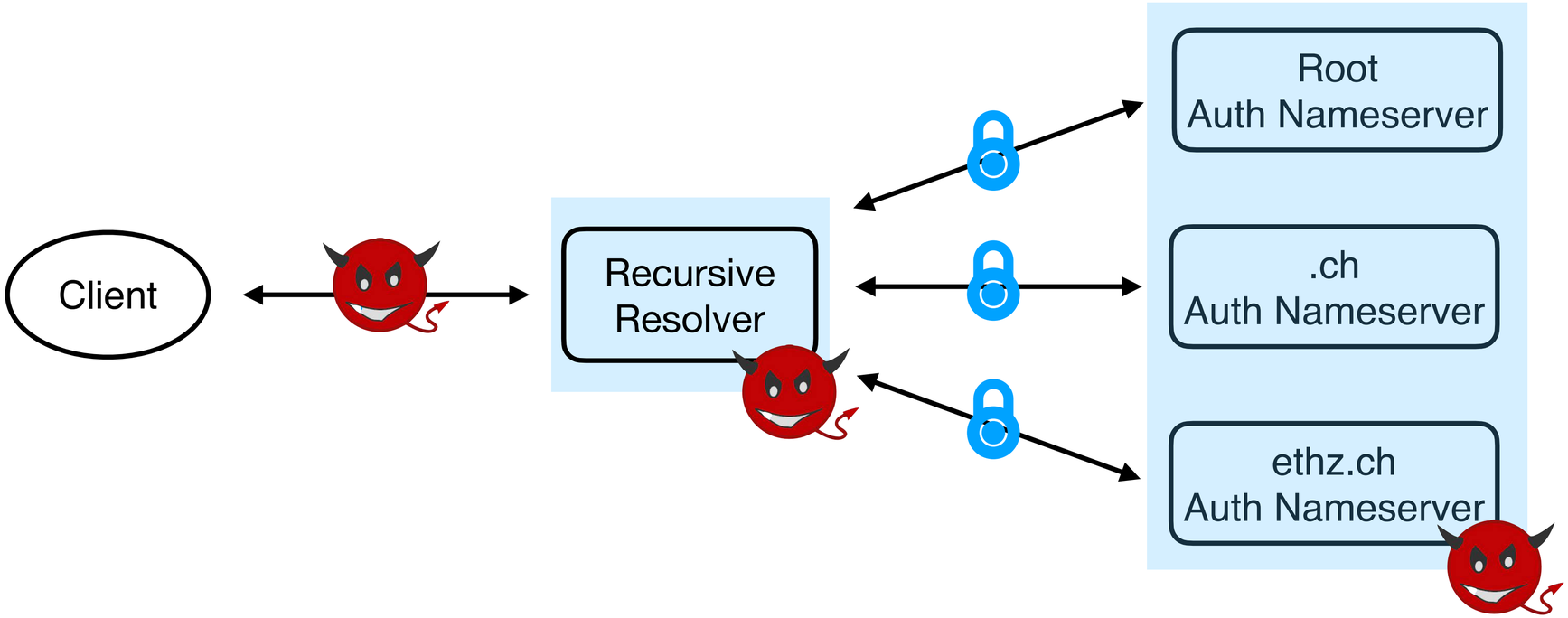


DNS security today — Secure channel limitation

Trusted

On-path data manipulation exists

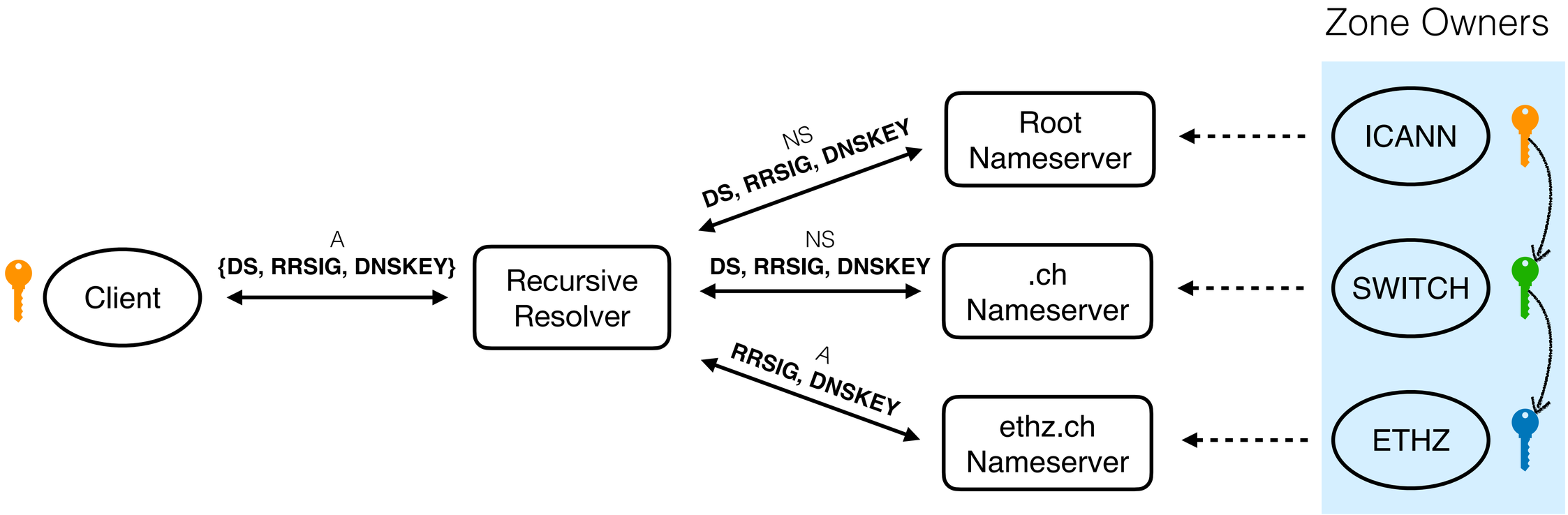
- ISPs [Randall et al.; IMC'21]
- Open resolvers [Jeman et al.; DSN'19]
- TLS-intercepting middleboxes [Durumeric et al.; NDSS'17]



DNS security today — DNSSEC

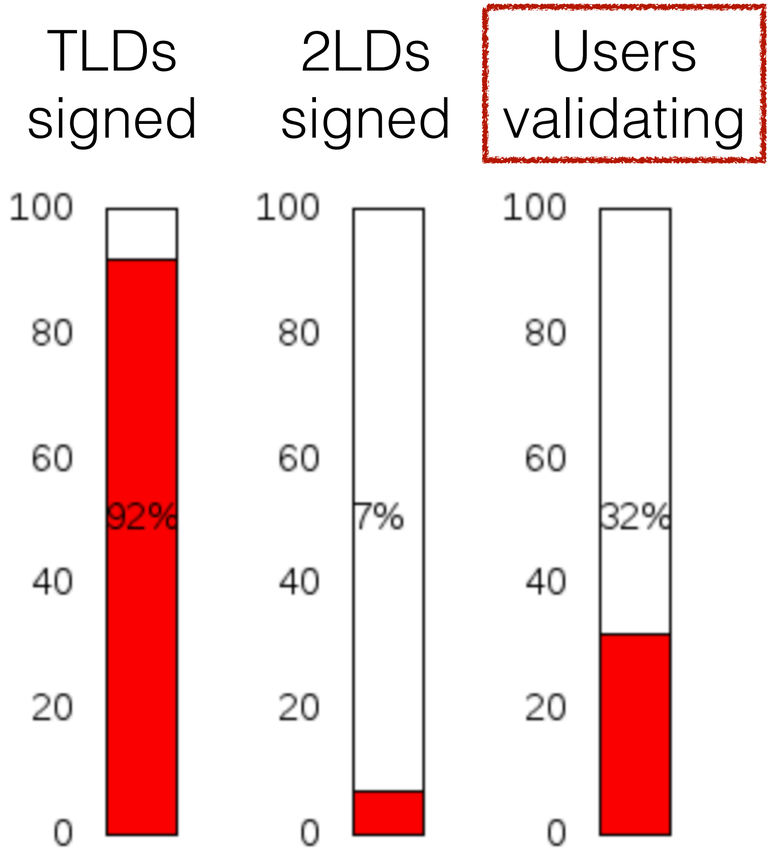
Offline data signing

Data authentication with chain of trust



DNS security today — DNSSEC

Slow adoption …

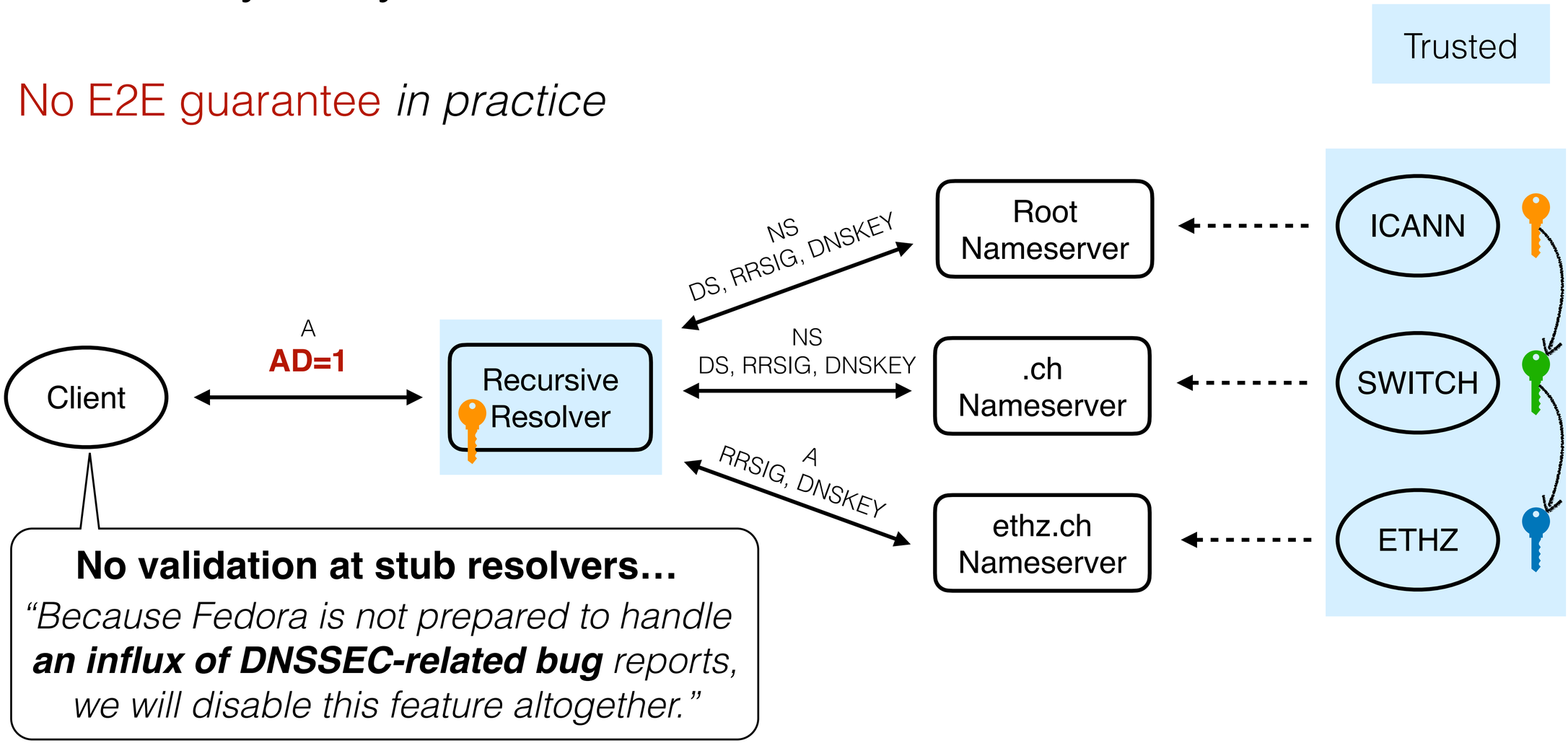


Not end users!

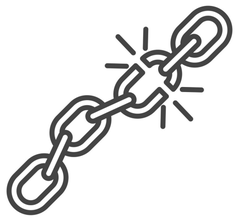
* http://rick.eng.br/dnssecstat/, retrieved on April 12, 2023

DNS security today — DNSSEC limitations

No E2E guarantee *in practice*



DNS security today — DNSSEC limitations



Complex and fragile

*__DNSSEC Outages and Validation Failures__, https://ianix.com/pub/dnssec-outages.html

- [1455504478] unbound[10562:0] info: validation failure <geekpac.com. A IN> **no keys have a DS with algorithm DSA** from 216.218.132.2 for key geekpac.com. while building chain of trust
- [1461807469] unbound[9788:0] info: validation failure <slim-shirt.com. A IN>: **no keys have a DS with algorithm DSA-NSEC3-SHA1** from 149.210.161.148 for key slim-shirt.com. while building chain of trust
- [1416399790] unbound[6665:0] info: validation failure <www.root-dnssec.org. A IN>: **no keys have a DS with algorithm RSASHA1** from 199.43.133.53 for key

- [1532015786] unbound[52909:0] info: validation failure <www.bsws.de. A IN>: **signer name mismatches key name** from 80.86.183.57 for DS www.bsws.de.

- [1390966241] unbound[6793:0] info: validation failure <uofk.edu. NS IN>: **DS hash mismatches key** from 41.67.20.4 for key uofk.edu. while building chain of

- [1405129714] unbound[32474:0] info: validation failure <viagrakopen.net. NS IN>: **DNSKEY RRset did not match DS RRset by name** from 93.180.70.53 and

⋮

- .hr — Croatia (October 2015)
- .xn--y9a3aq — Armenia (November 2015)
- .zm — Zambia (December 2015)
- .mil — US Military (December 2015)

- .ntt — Japanese gTLD (September 2017)
- .bw — Botswana (October 2017)
- .lidl — new gTLD (December 2017)
- .schwarz — new gTLD (December 2017)

- .tm — Turkmenistan (September 2022)
- .na — Namibia (October 2022)
- .xn--qxam — Greek IDN (November 2022)
- .mx — Mexico (April 2023)

⋮

- internetsociety.org, isoc.org (June 2015)
- af.mil (June 2015)
- nasa.gov (August 2015)
- NICMX (August 2015)

- abuse.ch (February 2017)
- internetsociety.org (February 2017)
- danyork.com (February 2017)
- Godaddy (domaincontrol.com) DNS (Marc

- nist.gov (June 2021)
- lequipe.fr (June 2021)
- slack.com (September 2021)
- europa.eu (December 2021)

⋮

Rethinking authentication in hierarchical naming system

Desiderata:

E2E data authentication

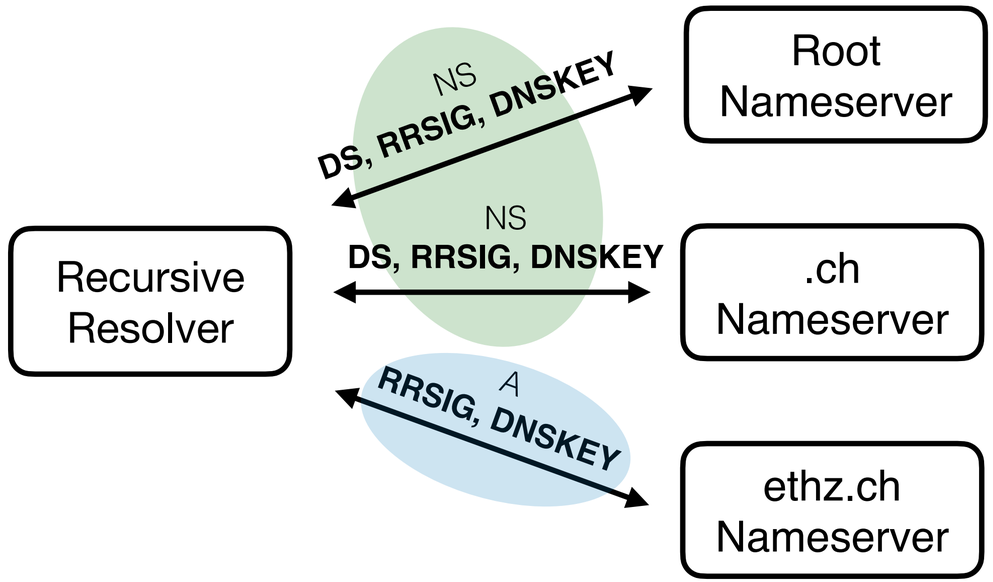
Simple and robust

Backward compatible

Rethinking authentication in hierarchical naming system

Observation:

Authentication of **zone delegation** vs. **zone data**

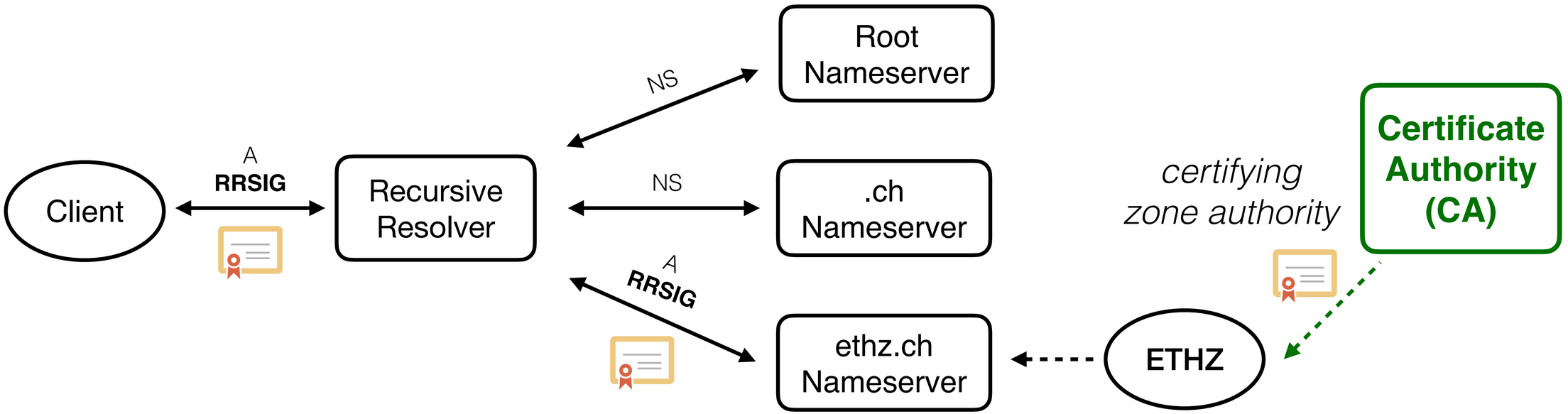


New architecture with opportunities

Simpler data authentication

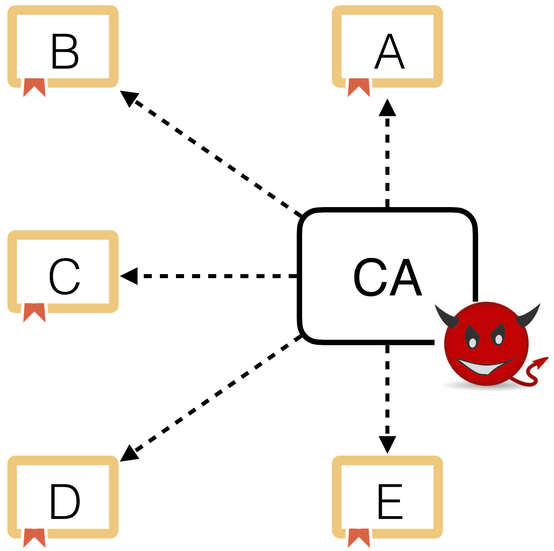
Easier client adoption

No child-parent sync



But also problems — better or worse security?

Malicious/compromised CA

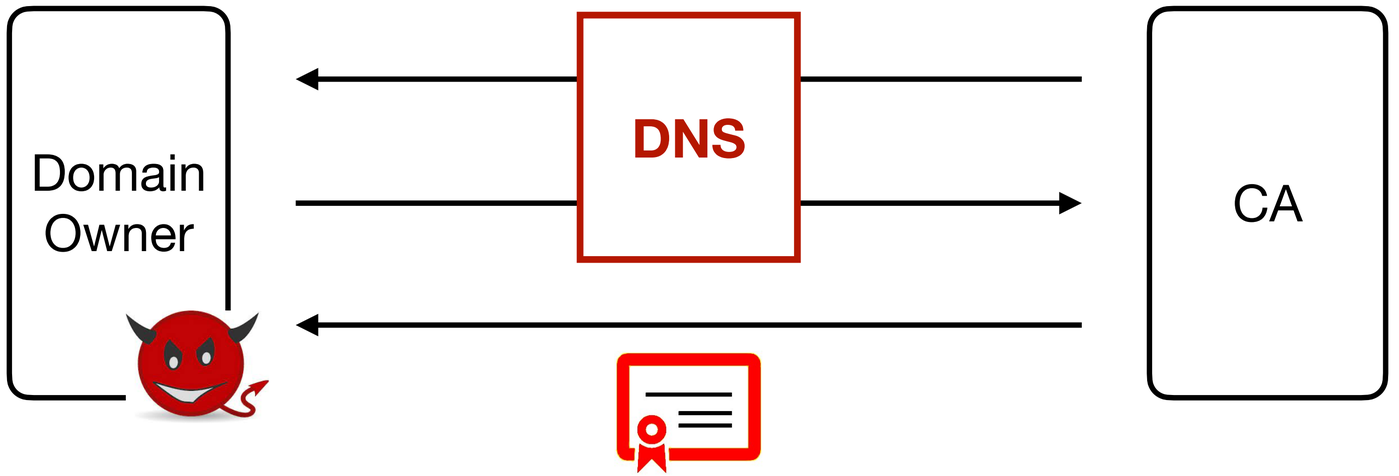


But also problems — how to bootstrap?

Certificate issuance requires zone/domain ownership validation

But also problems — how to bootstrap?

Certificate issuance requires zone/domain ownership validation



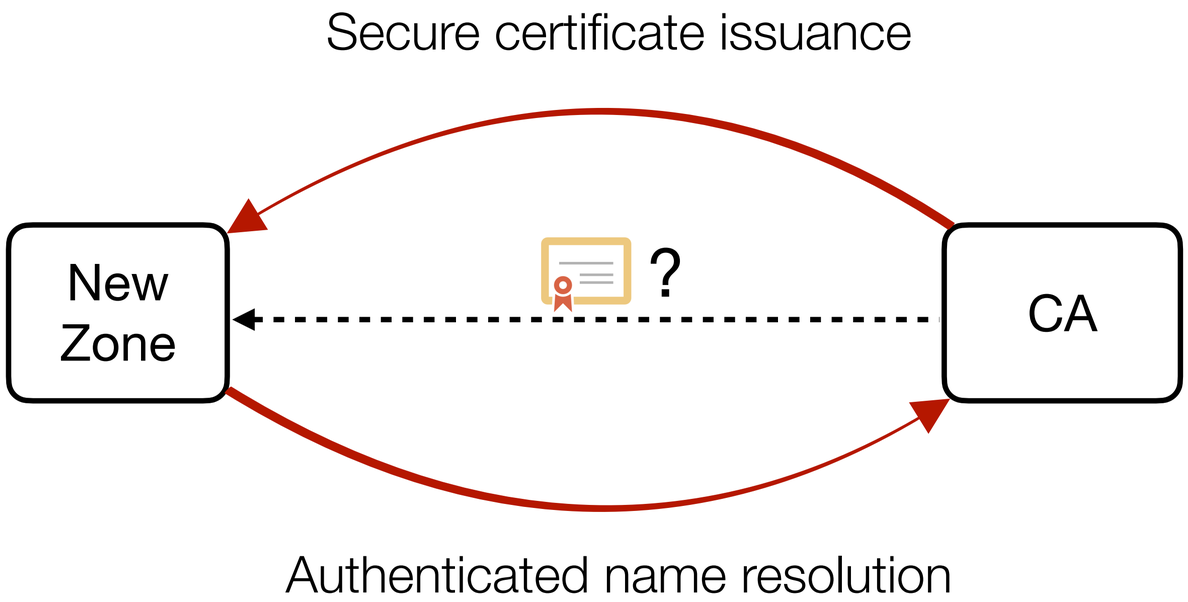
Dai et al. *Let's Downgrade Let's Encrypt*. CCS'21

Schwittmann et al. *Domain Impersonation is Feasible: A Study of CA Domain Validation Vulnerabilities*. EuroSP'19

Borgolte et al. *Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates*. NDSS'18

But also problems — how to bootstrap?

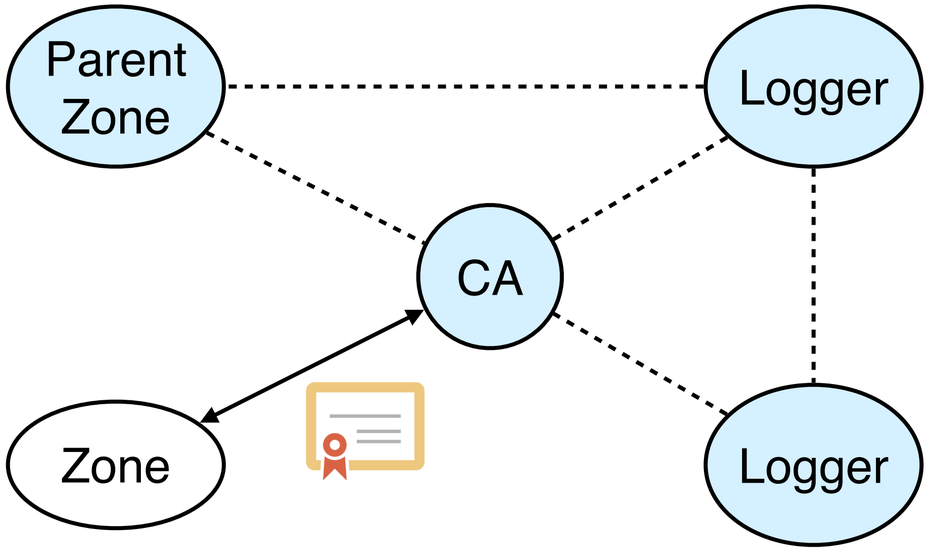
Circular dependency!



RHINE overview

Trusted

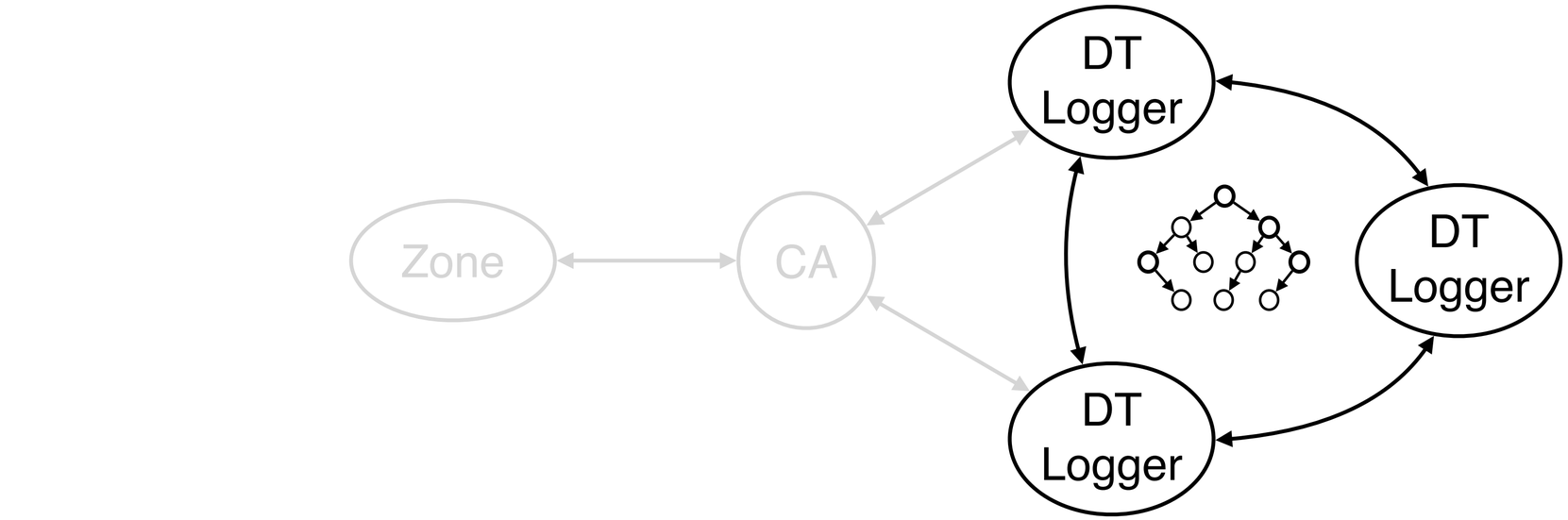
Robust trust model with ***checks and balances***



RHINE overview

Robust trust model with ***checks and balances***

Delegation Transparency (DT) to track global ***delegation status***

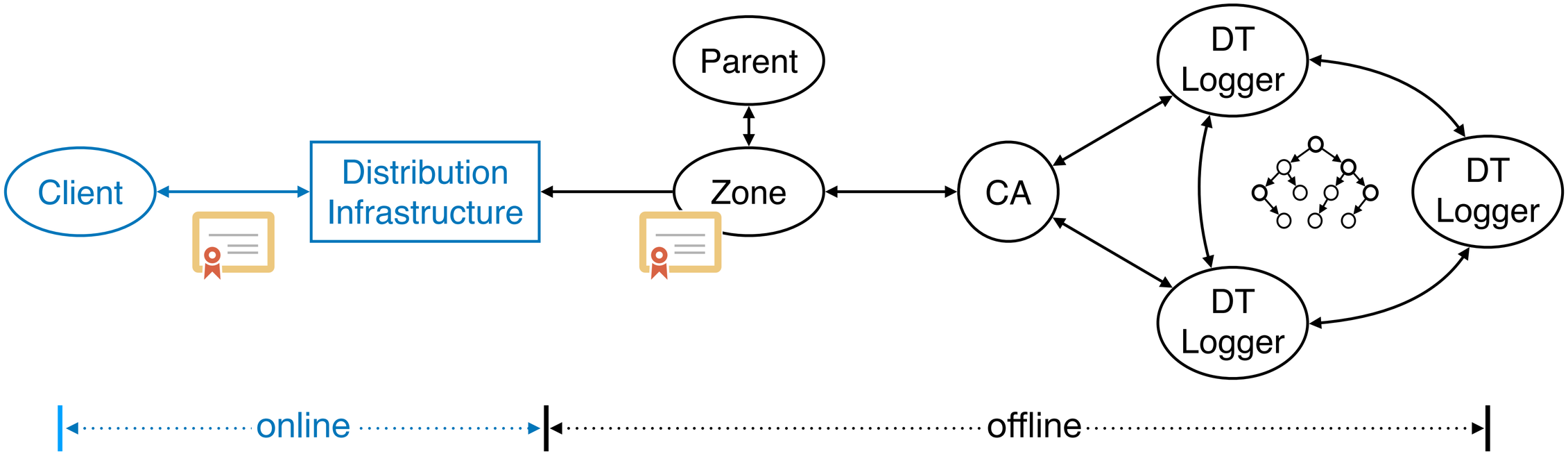


RHINE overview

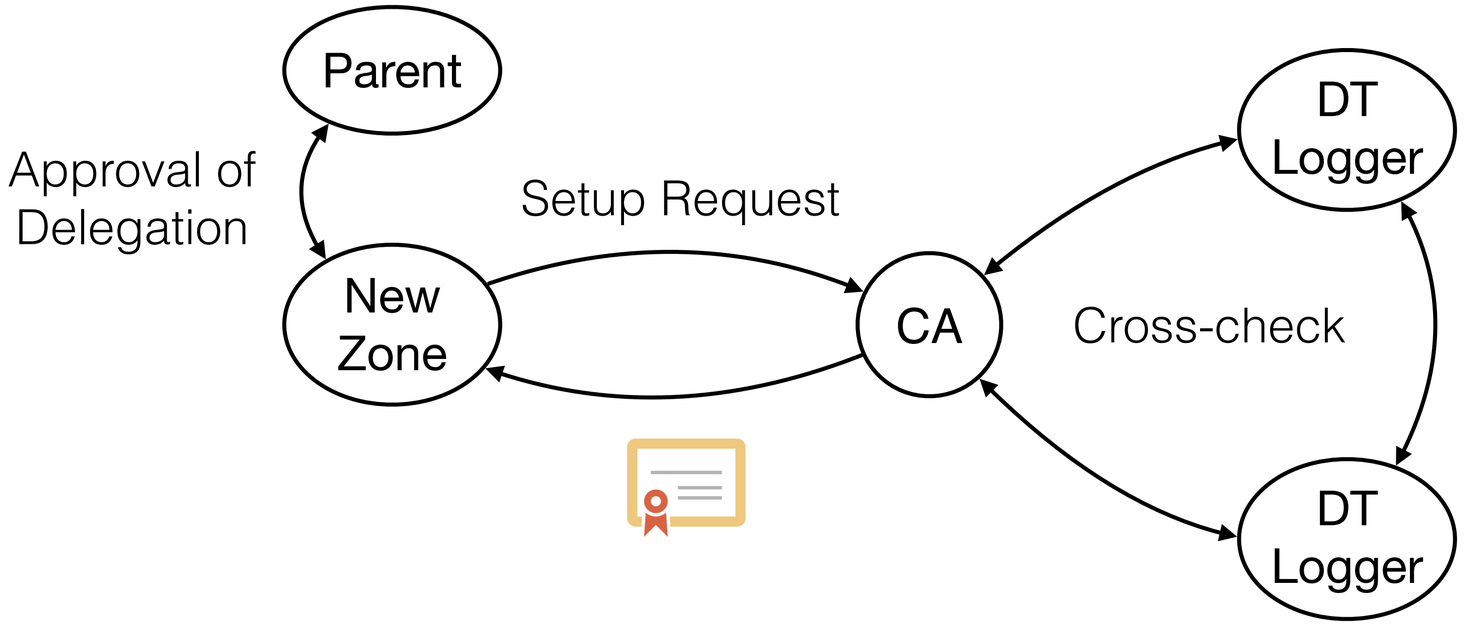
Robust trust model with ***checks and balances***

Delegation Transparency (DT) to track global ***delegation status***

Complexity shifted to ***offline***

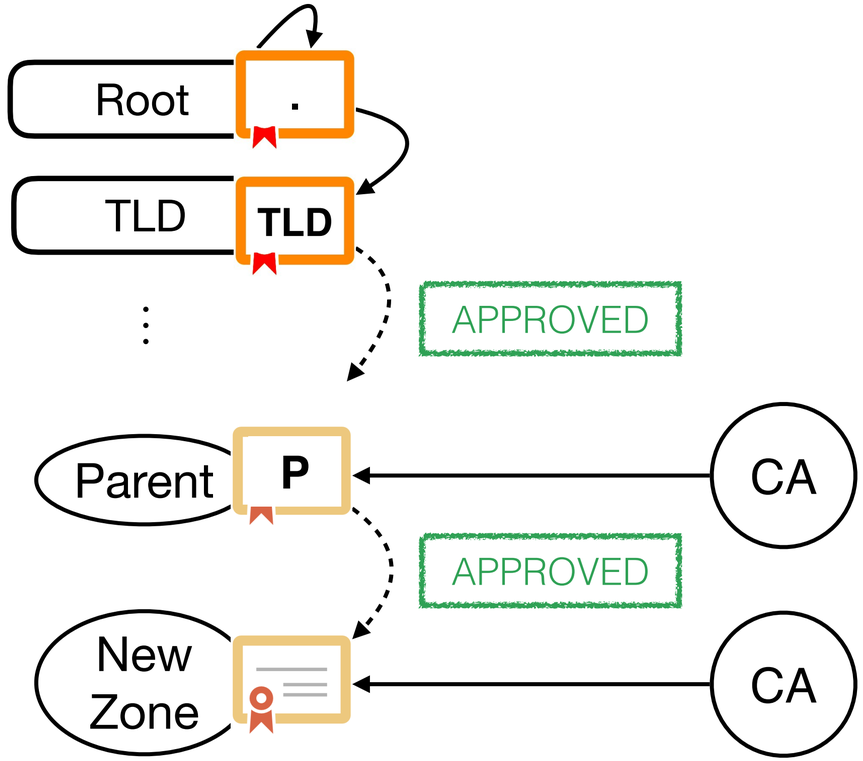


RHINE protocols — Secure delegation setup



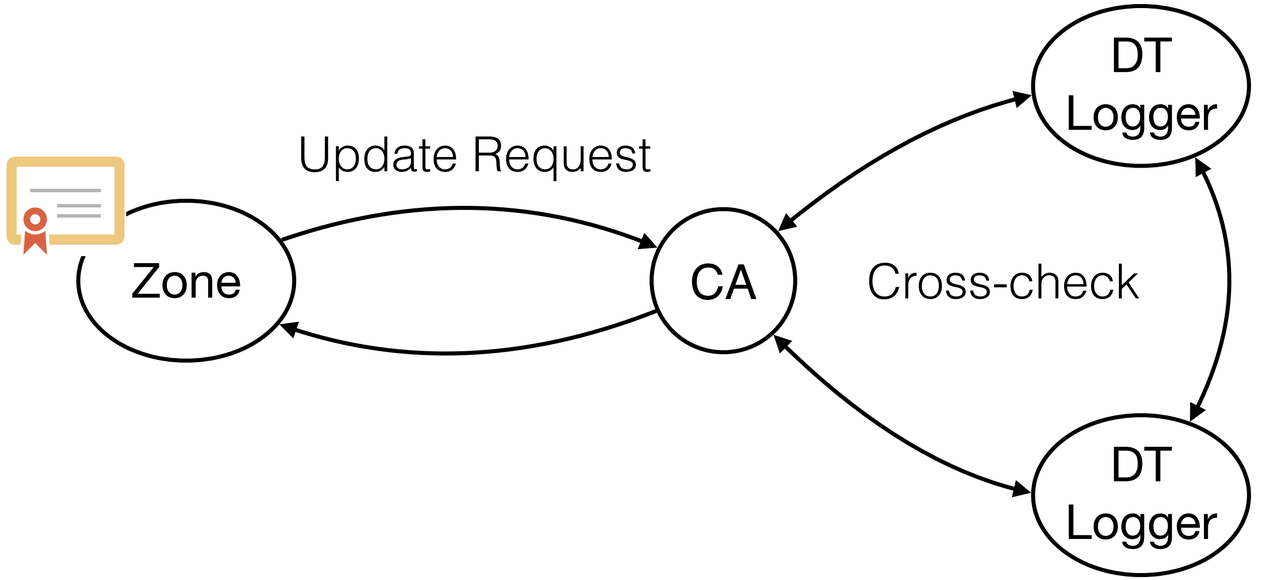
Circular dependency broken by parent engagement

RHINE protocols — Secure delegation setup



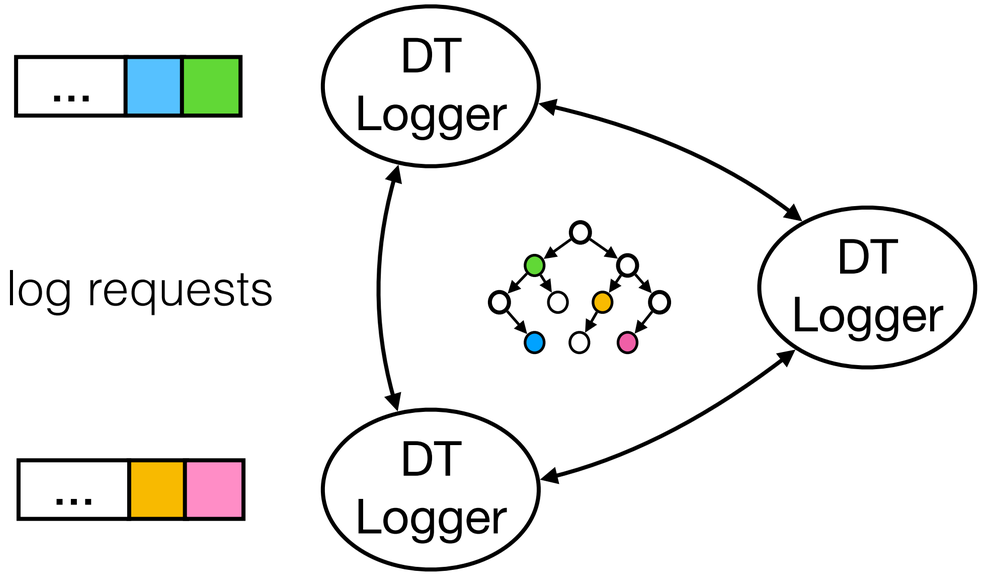
Circular dependency broken by parent engagement

RHINE protocols — Secure delegation update



Independent security management without parent sync (in most cases)

RHINE protocols — DT aggregation



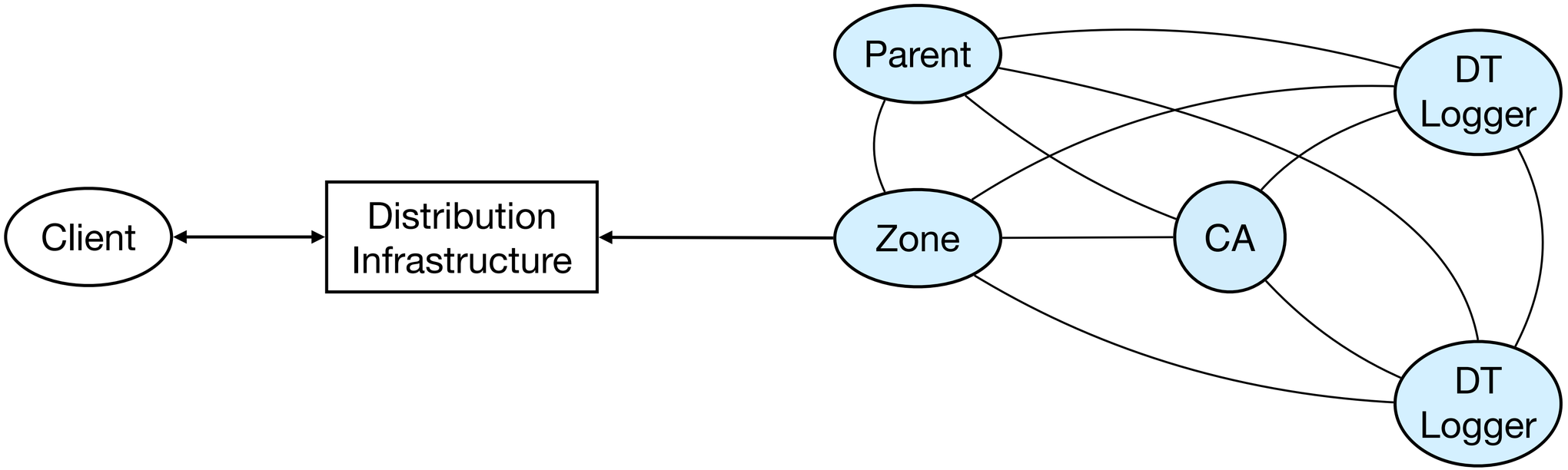
*Secure consensus based on Logres**

*Joel et al. *A Formally Verified Protocol for Log Replication with Byzantine Fault Tolerance*. SRDS'20

RHINE security

Trusted

hard to analyse!

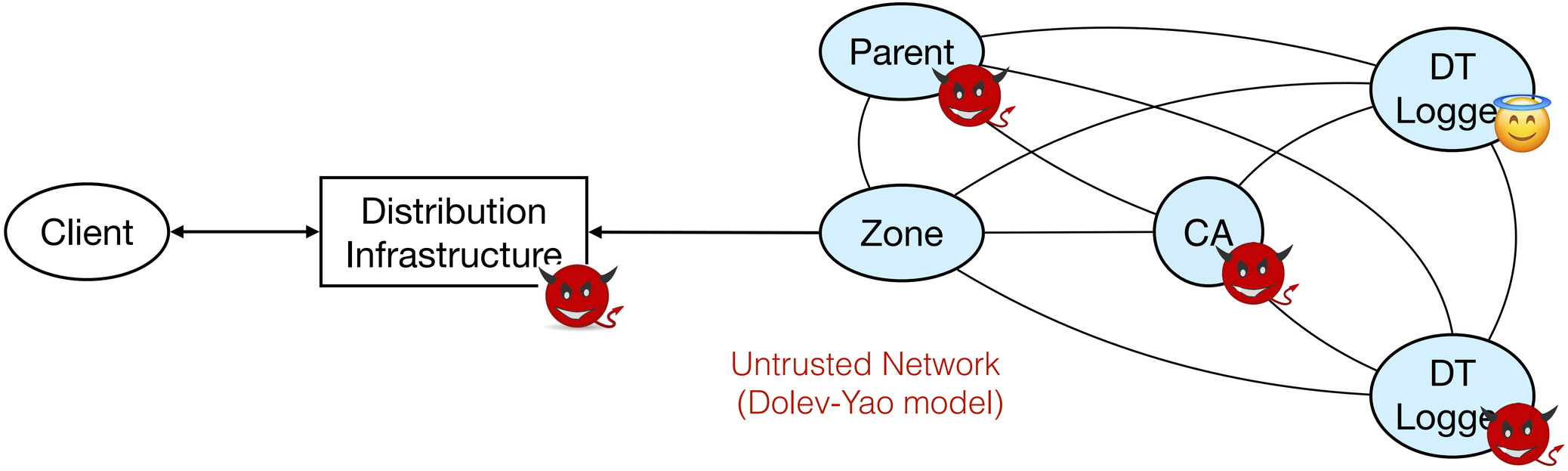


RHINE security

Trusted

Formally verified using the Tamarin prover

Main property: E2E data authenticity for delegated zones



RHINE deployability

Entity	End User	Recursive Resolver	Auth NS	Zone Owner
Operations	• Truststore maintenance • Cert & data verification	• Query, validation, and caching of security records	• Serve security records	• Data signing • Key rollover • **No key sync**
Comparison	DoT/DoH	DNSSEC	DNSSEC	DNSSEC
Infrastructure Compatibility	DNS (RHINE can co-exist with DoT/DoH)			

simpler

comparable /reusable

RHINE deployability

Entity	End User	Recursive Resolver	Auth NS	Zone Owner		CA	Logger
Operations	• Truststore maintenance • Cert & data verification	• Query, validation, and caching of security records	• Serve security records	• Data signing • Key rollover • **No key sync**	• Request and update cert (and dlgt status)	• Cert issuance • Update attestation	DT
Comparison	DoT/DoH	DNSSEC	DNSSEC	DNSSEC	ACME Client	ACME Server	CT
Infrastructure Compatibility	DNS (RHINE can co-exist with DoT/DoH)				Web PKI (DT loggers as a subset of CT loggers)		

simpler

comparable /reusable

extra effort

RHINE prototype evaluation

SDNS

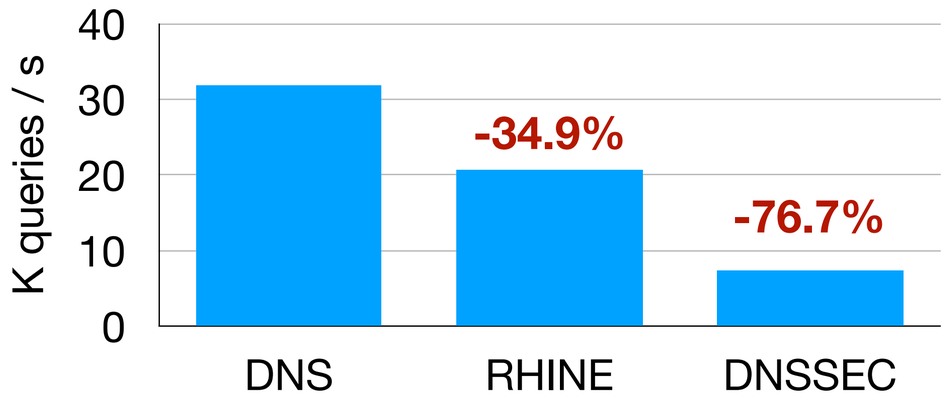
CoreDNS

Setup

- Servers: 8-core CPU (2.6GHz), 16GB RAM
- Network: 1Gbps, RTT=100 ms

Resolver throughput:

- Cache hit ratio: 80%
- Zones: 120K 2LDs/3LDs
- Query generator: dnsperf



RHINE prototype evaluation

SDNS

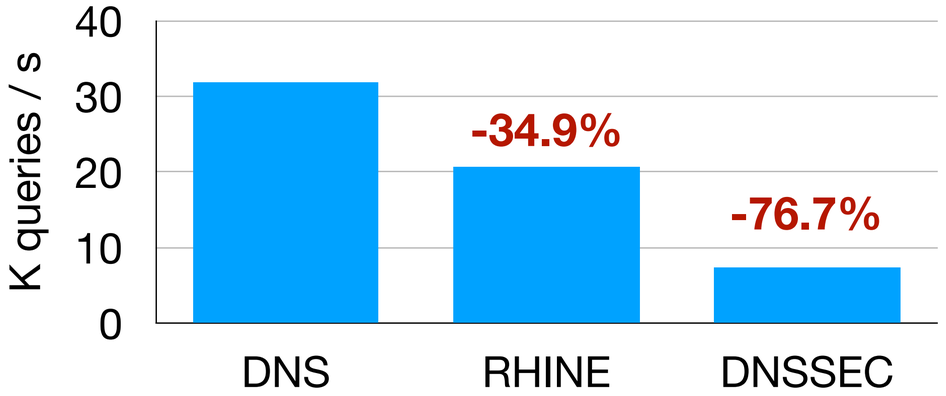
CoreDNS

Setup

- Servers: 8-core CPU (2.6GHz), 16GB RAM
- Network: 1Gbps, RTT=100 ms

Resolver throughput:

- Cache hit ratio: 80%
- Zones: 120K 2LDs/3LDs
- Query generator: dnsperf



Certificate issuance rate: **~20M** RHINE certs / day > **~6M** TLS certs / day

- Capped by DT consensus

*Merkle Town: https://ct.cloudflare.com/

Summary and outlook

Secure Internet needs **E2E-secure** name resolution

RHINE offers **robust** E2E authenticity, **formally verified**

RHINE is **deployable** today

Summary and outlook

Secure Internet needs **E2E-secure** name resolution

RHINE offers **robust** E2E authenticity, **formally verified**

RHINE is **deployable** today

Next steps: Experimental deployment

High-availability with **SCION**

Summary and outlook

Secure Internet needs **E2E-secure** name resolution

RHINE offers **robust** E2E authenticity, **formally verified**

RHINE is **deployable** today

Next steps: Experimental deployment

High-availability with **SCION**

Thank you!

Questions?

Contact: huayi.duan@inf.ethz.ch