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

**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

Recursive Resolver

Root
Auth Nameserver

.ch
Auth Nameserver

ethz.ch
Auth Nameserver

Client

- 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
DNS security today — Secure channel
DNS security today — Secure channel limitation

Channel security $\not\Rightarrow$ E2E data authenticity
DNS security today — Secure channel limitation

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 …

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

Not end users!
DNS security today — DNSSEC limitations

No E2E guarantee *in practice*

No validation at stub resolvers...

“Because Fedora is not prepared to handle an influx of DNSSEC-related bug reports, we will disable this feature altogether.”
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
- [1461399790] 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

- [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 <viagrokopen.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)
- .tt — 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–qxa — Greek IDN (November 2022)
- .mx — Mexico (April 2023)
- .internetociety.org, isoc.org (June 2015)
- .af.mil (June 2015)
- .nasa.gov (August 2015)
- .NICMX (August 2015)
- .abuse.ch (February 2017)
- .internetocity.org (February 2017)
- .danyork.com (February 2017)
- .Godaddy (domaincontrol.com) DNS (Marc
- .nst.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

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*

RHINE security

hard to analyse!

Client -> Distribution Infrastructure -> Zone

Zone -> Parent

Zone -> CA

CA -> DT Logger

CA -> DT Logger

trusted
RHINE security

Formally verified using the Tamarin prover

Main property: E2E data authenticity for delegated zones

Untrusted Network (Dolev-Yao model)
### RHINE deployability

<table>
<thead>
<tr>
<th>Entity</th>
<th>End User</th>
<th>Recursive Resolver</th>
<th>Auth NS</th>
<th>Zone Owner</th>
</tr>
</thead>
</table>
| 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

<table>
<thead>
<tr>
<th>Entity</th>
<th>End User</th>
<th>Recursive Resolver</th>
<th>Auth NS</th>
<th>Zone Owner</th>
<th>CA</th>
<th>Logger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Truststore</td>
<td>• Serve security records</td>
<td>• Request and update cert (and dtg status)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cert &amp; data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>verification</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Query, validation, and caching of security records</td>
<td></td>
<td>• Data signing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Key rollover</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• No key sync</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comparison</td>
<td>DoT/DoH</td>
<td>DNSSEC</td>
<td>DNSSEC</td>
<td>DNSSEC</td>
<td>ACME Client</td>
<td>ACME Server</td>
</tr>
<tr>
<td>Infrastructure Compatibility</td>
<td>DNS (RHINE can co-exist with DoT/DoH)</td>
<td>DNSSEC</td>
<td>DNSSEC</td>
<td>DNSSEC</td>
<td>ACME Client</td>
<td>ACME Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- simpler
- comparable /reusable
- extra effort

**Comparison**

- DoT/DoH
- 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)
RHINE prototype evaluation

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

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