Exploration of the deployment and use of the DNS HTTPS Resource Record

DNS OARC 44 Workshop
Feb 6th, 2025

Hongying Dong*, **Yizhe Zhang***, Hyeonmin Lee, Shumon Huque, Yixin Sun

*Both authors contributed equally

HTTPS Resource Records

DNS HTTPS resource records

- SVCB (service binding) record tailored to the HTTPS protocol, providing essential information for accessing HTTPS services
- Two modes: ServiceMode vs. AliasMode (`SvcPriority` parameter)

```
example.com. 300 IN HTTPS 0 anotherdomain.com
example.com. 300 IN HTTPS 1 .   alpn=h3   ech={version,...,public_name=public.com,…,Keyconfig,…}
```

DNS HTTPS record benefits

- Compared to ***CNAME***:
  - Can coexist with other record types at an owner name. So allows name redirection at any location within the zone, including zone apexes.
- Compared to ***SRV***:
  - Is tailored to the HTTP protocol, and crucially has been adopted by the web community (which has in the past been opposed to any proposed use of SRV for name redirection).
  - Supports a more flexible record name format that allows deployment of wildcards.
- Supports an extensible parameter framework that provides indication of other capabilities:
  - Supported protocols (ALPN etc)
  - IP address hints
  - Cryptographic parameters to enable use of TLS Encrypted Client Hello

Overview

- Server-side HTTPS records deployment among Tranco 1M domains
  - HTTPS records adoption rate
  - Name servers support of HTTPS records
  - ECH deployment
    - Key rotation
  - DNSSEC deployment
  - IP inconsistency in HTTPS records
    - Potential connection issues
  - Inconsistent use of HTTPS records

- Client-side HTTPS records support
  - Major browsers support
  - ECH share-mode support
  - ECH split-mode support
    - Potential error configuration

Datasets

- Target domains: Tranco 1M list*
  - Apex: *example.com.*
  - www: *www.example.com.*
- Public resolvers:
  - `8.8.8.8.`
  - `1.1.1.1.`
- Scan frequency:
  - Daily
- DNS records type:
  - HTTPS, A, AAAA
  - SOA, NS
- Enrichment data:
  - WHOIS

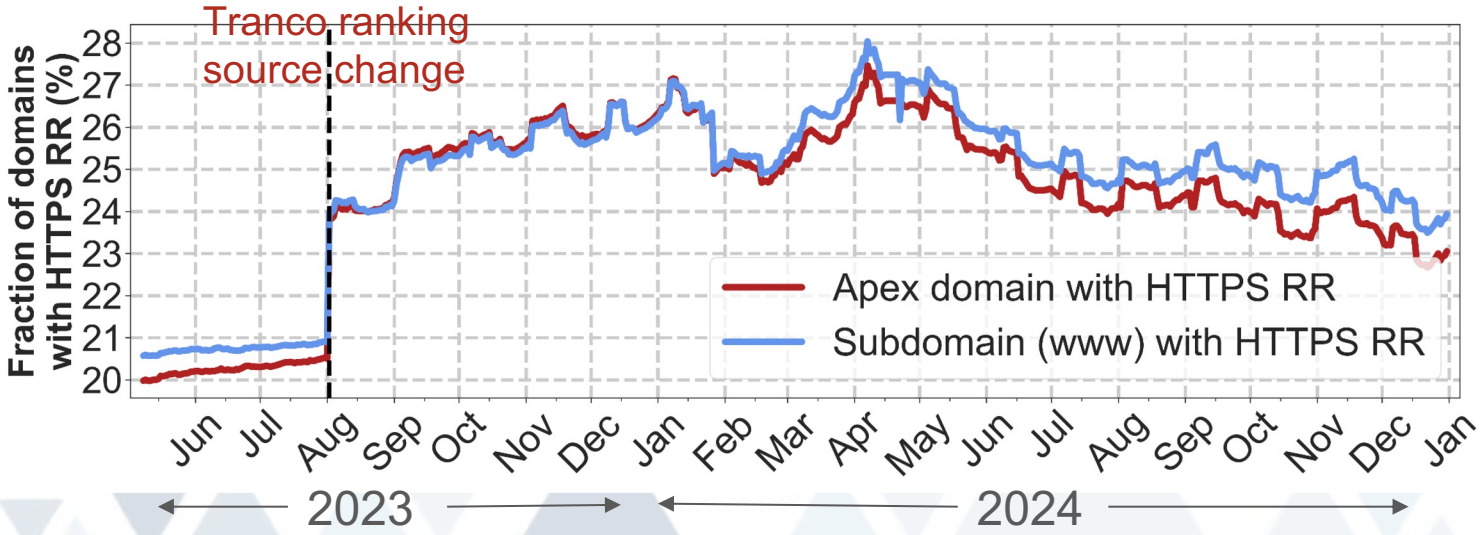
*A ranking of the top one million websites based on their popularity and usage (https://tranco-list.eu/).

Data Type		Collection Period
Domain (Apex, www)	HTTPS, A, AAAA	2023-05-08 – now
	SOA, NS	2023-08-16 – now

Available dataset at:
https://keyinfra.cs.virginia.edu

HTTPS RR Adoption Rate & Name Server Support

- Adoption rate: >20% among Tranco 1 million domains
- Name Servers:
  - Cloudflare related: 99.85%
  - Others: 0.15%
    - Entities:Google, Facebook, etc.
    - Providers: GoDaddy, NS1, Akamai, AWS, Domeneshop, deSEC, etc.



Encrypted ClientHello (ECH)

- Allow clients to encrypt its initial ClientHello message in a TLS session.
- ECH public key is delivered through DNS HTTPS records.

```
example.com. 300 IN HTTPS 1 . alpn=h3
ech={version,...,public_name=public.com,...,Keyconfig,...}
```

- Important for ECH clients to make DNS queries over an encrypted transport like DoT (DNS over TLS) and DoH (DNS over HTTPS), etc.

ClientHello without ECH

ClientHello
Sensitive Info
(SNI: example.com, ALPN, key share…)

ClientHello with ECH

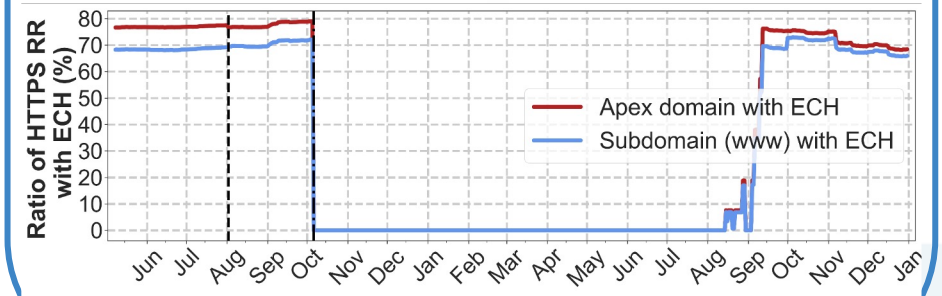
Outer ClientHello
Non-sensitive Info
(Outer SNI: public.com, ALPN, key share…)

(Encrypted) Inner ClientHello
Sensitive Info
(Inter SNI: example.com, ALPN, key share…)

ECH Deployment and Key Rotation

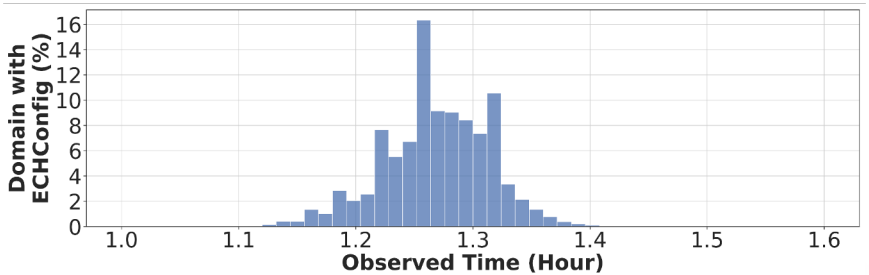
ECH Deployment

- Major player: Cloudflare
- Cloudflare **disabled** ECH in early Oct, 2023 (https://community.cloudflare.com/t/early-hints-and-encrypted-client-hello-ech-are-currently-disabled-globally/567730) and **re-enabled** since mid Aug, 2024.



ECH Key Rotation

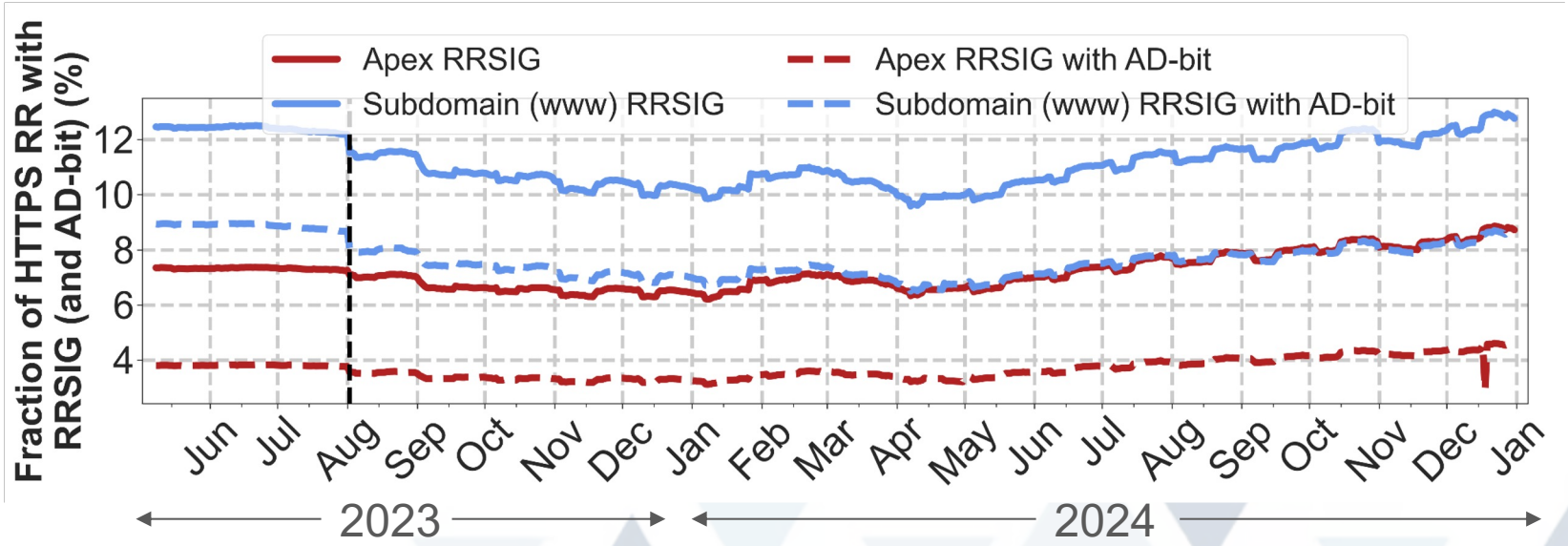
- Frequent ECH configuration rotation, with intervals ranging from 1.1 to 1.4 hours.
- Necessity of the **ECH retry mechanism** on the client-facing server.



Measurement conducted from July 21 to July 27, 2023.

HTTPS RR and DNSSEC Deployment

- DNSSEC ensures the integrity and authenticity of DNS records.
- **<10 %** apex domain are signed protected by DNSSEC.
- Deploying DNSSEC for HTTPS records is important to prevent them from being dropped or spoofed and in the case of ECH, downgrading the privacy of the SNI name.



HTTPS with RRSIG and AD-bit

IP Inconsistency in HTTPS RR and A/AAAA records

From July, 2024 to December, 2024

- Observed 974 unique domains has IP inconsistency (inconsistency in either HTTPS and A records or HTTPS and AAAA records).
  - 3,275 unique *{domain, date} tuples*
  - Average 18.89 days in duration

- Potential connectivity issue (only test on IPv4)
  - 570 *{domain, date} tuples* have both ipv4hints and A records
    - 79 (<14%) reachable via both **ipv4hints** and **A** records
    - 438 accessible only via **ipv4hints** in HTTPS records
    - 43 accessible only via **A** records
    - 10 cannot be accessed

```
example.com. 300 IN HTTPS 1 . alpn=h3 ipv4hint=IPv4A  ipv6hint=IPv6A

example.com. 300 IN A                                  IPv4B
example.com. 300 IN AAAA                               IPv6B
```

The IPv4hint/IPv6hint **differs from** the IP addresses specified in the A/AAAA records

Inconsistent Use of HTTPS Records

Employment of different name servers

- Domains utilize a mixture of Cloudflare and other name servers when HTTPS records are observed to be deactivated.

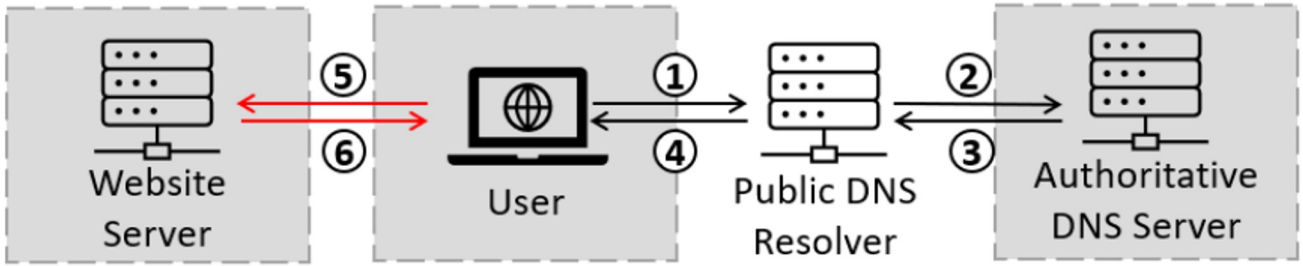
Change of name servers

- Domains lose their HTTPS records when switching name servers from Cloudflare to non-Cloudflare name servers.

Change in configurations

- Cloudflare automatically generate an HTTPS record for domains when they have the "proxied" option turned on.

Client Experiment Setups



- Website Server: Nginx
- Browsers: **Chrome, Safari, Edge, Firefox**
- DNS authoritative server: Bind9
- Public DNS Resolver: `8.8.8.8.`

Browsers' Support of HTTPS RR

		Chrome		Safari	Edge		Firefox	
OS		macOS	Windows	macOS	macOS	Windows	macOS	Windows
Browser Version		120.0.6099		17.2.1	120.0.2210		122.0.1	
HTTPS RR Utilization	{apex}	●	●	◐	●	●	●	●
	http://{apex}	●	●	◐	●	●	●	●
	https://{apex}	●	●	●	●	●	●	●

- All four browsers send **HTTPS** queries, together with **A** and **AAAA** query
- Safari send traffic to port 80 when directed to visit `{apex}` and `http://{apex}`

- Solid-filled circle - the record or parameter is utilized
- Half solid-filled circle - the record or parameter is utilized, yet some essential function associated is lacked
- Unfilled circle - no support

Browsers' Support of HTTPS RR

		Chrome		Safari	Edge		Firefox	
OS		macOS	Windows	macOS	macOS	Windows	macOS	Windows
Browser Version		120.0.6099		17.2.1	120.0.2210		122.0.1	
AliasMode	TargetName	○	○	●	○	○	○	○
ServiceMode	TargetName	○	○	●	○	○	●	●
	port	○	○	●	○	○	●	●
	alpn	●	●	●	●	●	●	●
	IP Hints	○	○	●	○	○	●	●

- Support:
  - Parameter: **alpn**
- Limited support:
  - **AliasMode** and other parameters
- **Inconsistent handling:**
  - Firefox* and Safari connect to the IPs in ***IP Hints*** parameter.
  - Chrome and Edge connect to the IPs in ***A/AAAA*** records.

*Firefox now visit IPs in A/AAAA records.

RFC Standards: ipv4hint/ipv6hint in HTTPS RR

https://datatracker.ietf.org/doc/rfc9460/

The "ipv4hint" and "ipv6hint" keys convey IP addresses that clients MAY use to reach the service. If A and AAAA records for TargetName are locally available, the client SHOULD ignore these hints. Otherwise, clients SHOULD perform A and/or AAAA queries for TargetName per Section 3, and clients SHOULD use the IP address in those responses for future connections. Clients MAY opt to terminate any connections using the addresses in hints and instead switch to the addresses in response to the TargetName query. Failure to use A and/or AAAA response addresses could negatively impact load balancing or other geo-aware features and thereby degrade client performance.

Browsers' Support of HTTPS RR

		Chrome		Safari	Edge		Firefox	
OS		macOS	Windows	macOS	macOS	Windows	macOS	Windows
Browser Version		120.0.6099		17.2.1	120.0.2210		122.0.1	
AliasMode	TargetName	○	○	●	○	○	○	○
ServiceMode	TargetName	○	○	●	○	○	●	●
	port	○	○	●	○	○	●	●
	alpn	●	●	●	●	●	●	●
	IP Hints	○	○	●	○	○	●	●

- Support:
  - Parameter: **alpn**
- Limited support:
  - **AliasMode** and other parameters
- **Inconsistent handling:**
  - Firefox* and Safari connect to the IPs in ***IP Hints*** parameter.
  - Chrome and Edge connect to the IPs in ***A/AAAA*** records.

*Firefox now visit IPs in A/AAAA records.

Take away:
1. Be aware of varying support levels for the HTTPS RR parameter
2. Ensure IP consistency and connectivity across A/AAAA and IP hints.

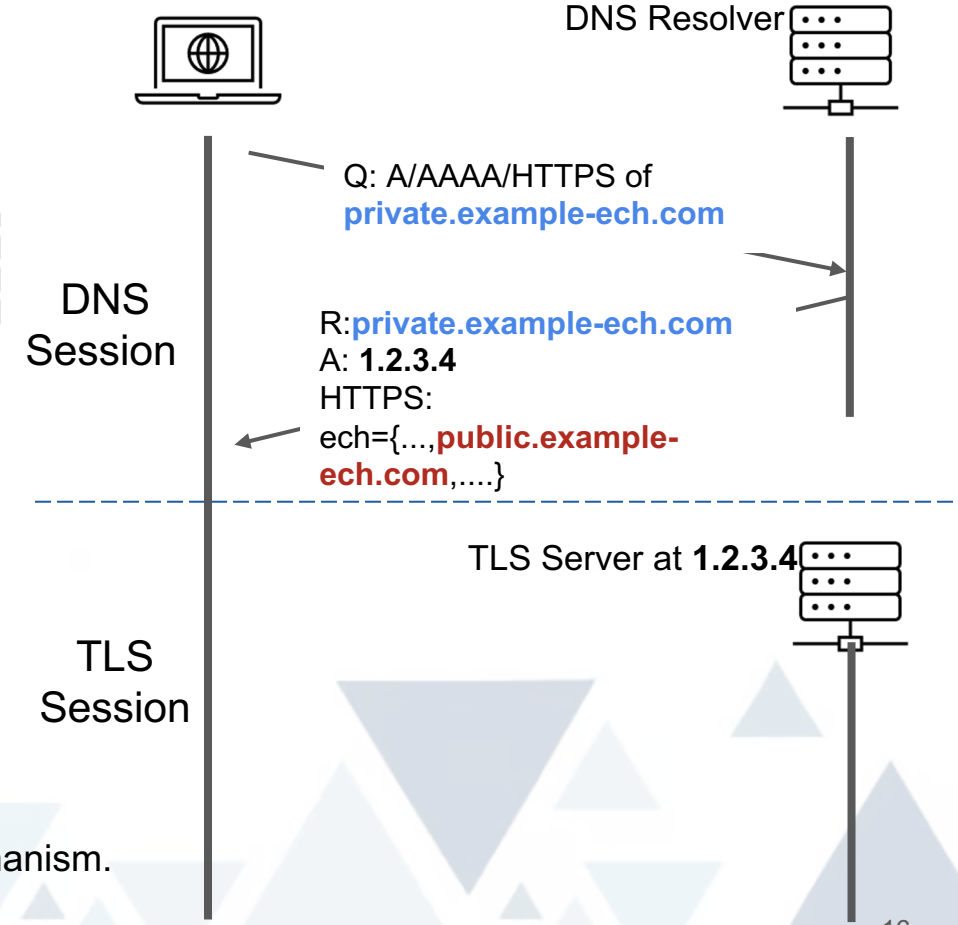
Shared Mode ECH

Client-Facing and Backend Combined.

	Chrome	Edge	Firefox
Shared Mode Support	●	●	●
(1) Unilateral ECH	●	●	●
(2) Malformed ECH	○	○	●
(3) Mismatched key	●	●	●

Safari does not support ECH mode yet.
Solid-fill circle: successful connection.

- Falls back to regular TLS connection.
- Successful ECH connection with retry mechanism.



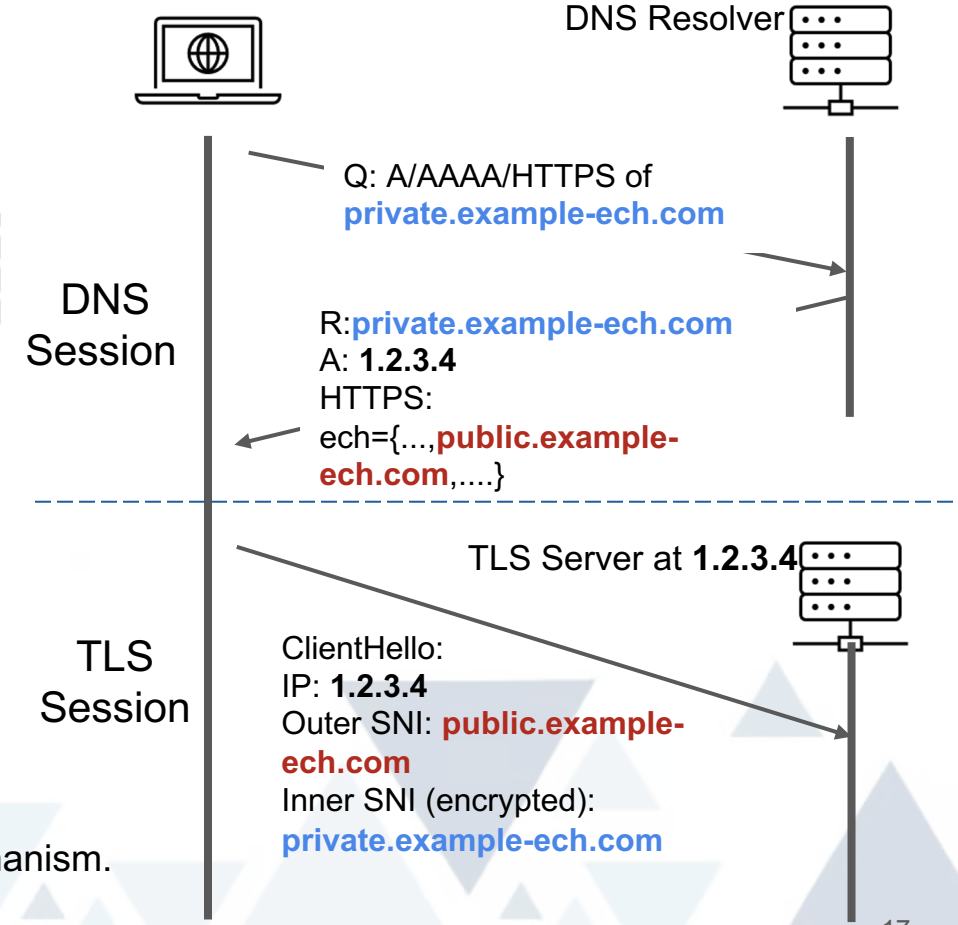
Shared Mode ECH

Client-Facing and Backend Combined.

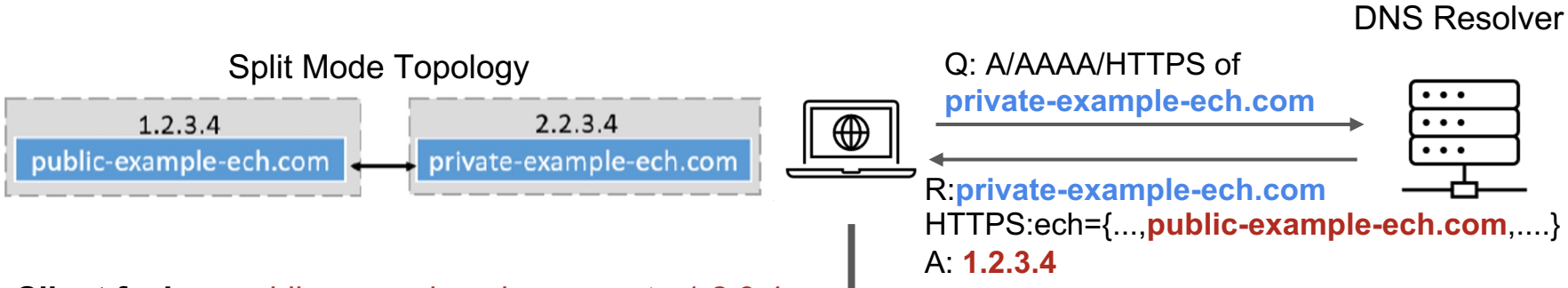
	Chrome	Edge	Firefox
Shared Mode Support	●	●	●
(1) Unilateral ECH	●	●	●
(2) Malformed ECH	○	○	●
(3) Mismatched key	●	●	●

Safari does not support ECH mode yet.
Solid-fill circle: successful connection.

- Falls back to regular TLS connection.
- Successful ECH connection with retry mechanism.



Split Mode ECH

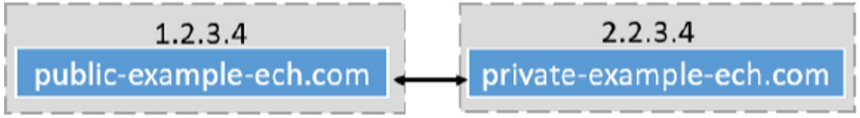


Client facing: public-example-ech.com at 1.2.3.4
Back end: private-example-ech.com at 2.2.3.4

Zone Config for private-example-ech.com:
HTTPS: …. ech={...,**public-example-ech.com**,....}
A: **1.2.3.4** **< Point to client-facing server.**

Split Mode ECH

Split Mode Topology

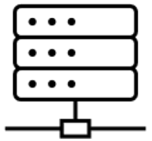


Client facing: public-example-ech.com at 1.2.3.4
Back end: private-example-ech.com at 2.2.3.4

Zone Config for private-example-ech.com:
HTTPS: …. ech={...,**public-example-ech.com**,....}
A: **1.2.3.4**

< Point to client-facing server.

DNS Resolver

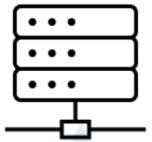


Q: A/AAAA/HTTPS of **private-example-ech.com**

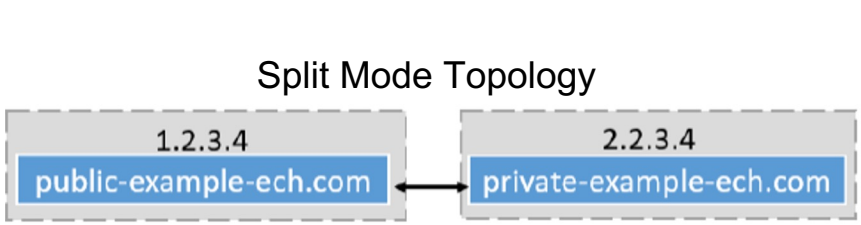
R:**private-example-ech.com**
HTTPS:ech={...,**public-example-ech.com**,....}
A: **1.2.3.4**

ClientHello:
IP: **1.2.3.4**
Outer SNI: **public-example-ech.com**
Inner SNI (encrypted): **private-example-ech.com**

Server at **1.2.3.4**



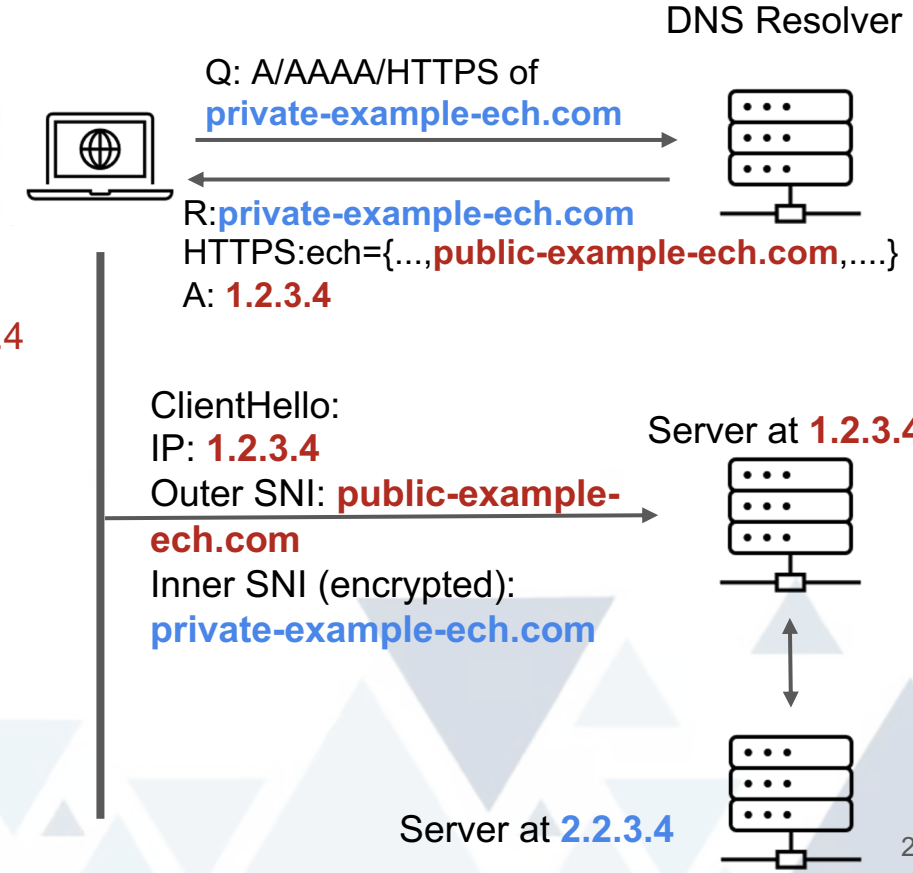
Split Mode ECH



Client facing: public-example-ech.com at 1.2.3.4
Back end: private-example-ech.com at 2.2.3.4

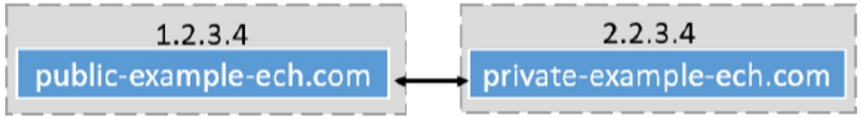
Zone Config for private-example-ech.com:
HTTPS: …. ech={...,**public-example-ech.com**,....}
A: **1.2.3.4**

< Point to client-facing server.



Split Mode ECH: Misconfiguration

Split Mode Topology

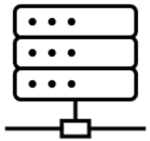


Client facing: public-example-ech.com at 1.2.3.4
Back end: private-example-ech.com at 2.2.3.4

Zone Config for private-example-ech.com:
HTTPS: …. ech={...,**public-example-ech.com**,....}
A: **2.2.3.4**

DNS Resolver

Q: A/AAAA/HTTPS of **private-example-ech.com**



R:**private-example-ech.com**
HTTPS:ech={...,**public-example-ech.com**,....}
A: **2.2.3.4**

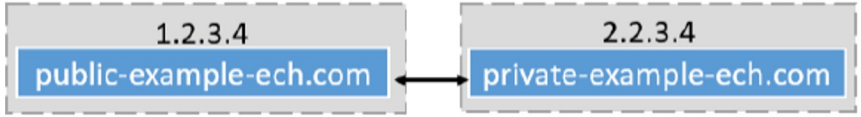
ClientHello:
IP: **2.2.3.4**
Outer SNI: **public-example-ech.com**
Inner SNI (encrypted): **private-example-ech.com**

Server at **2.2.3.4**

Reject:
Since public-example-ech.com ***not*** hosted on 2.2.3.4

Split Mode ECH: Misconfiguration

Split Mode Topology



Client facing: public-example-ech.com at 1.2.3.4
Back end: private-example-ech.com at 2.2.3.4

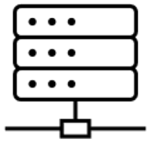
Zone Config for private-example-ech.com:
HTTPS: …. ech={...,**public-example-ech.com**,....}
A: **2.2.3.4**

Chrome and Edge will hardfail the connection
Firefox now falls back to non-ECH connection

Impacting Cloudflare's customers:
https://community.cloudflare.com/t/ech-with-split-dns/711539
https://www.vindit.dk/err_ech_fallback_certificate_invalid/

DNS Resolver

Q: A/AAAA/HTTPS of **private-example-ech.com**



R:**private-example-ech.com**
HTTPS:ech={...,**public-example-ech.com**,....}
A: **2.2.3.4**

ClientHello:
IP: **2.2.3.4**
Outer SNI: **public-example-ech.com**
Inner SNI (encrypted): **private-example-ech.com**

Server at **2.2.3.4**

Reject:
Since public-example-ech.com ***not*** hosted on 2.2.3.4

Public Release - DNS Datasets

- Parsed data (in CSV format):
  - Daily DNS HTTPS scans of top 1M sites
  - One tarball per month, starting May 2023, and ongoing (*updated monthly*)
  - https://keyinfra.cs.virginia.edu/dns_http/artifact/#dataset

- Raw data:
  - Contact us
- Paper with more details:
  - IMC'24-Exploring the Ecosystem of DNS HTTPS Resource Records: An End-to-End Perspective
  - https://dl.acm.org/doi/abs/10.1145/3646547.3688410

Summary and Discussion

DNS HTTPS records support

- Over 20% of domains in the Tranco list support HTTPS records, with Cloudflare playing a crucial role in this adoption
- A noticeable increase in support from other major DNS providers
- Four major web browsers support HTTPS record lookups

Challenges and issues

- The lack of DNSSEC protection for many HTTPS records, particularly those using ECH
- The complexities of managing HTTPS records, including issues related to IP consistency and ECH configurations
- Browsers' handling of HTTPS records can lead to connection failures

Recommendations

- Operators should take to correct configure HTTPS records.
- Cloud providers and domain administrators should take major browsers' support into account when integrating HTTPS records

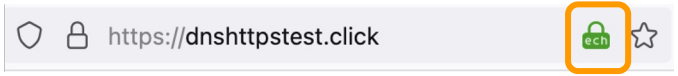
Thank you!

We appreciate any questions.

Active Updates in the Community

Client Side

- Firefox updates on DNS HTTPS records and ECH.[1]
  - New ECH fallback mechanisms.
  - New DNS HTTPS resolving mechanisms.
- Browser addon to track ECH status.[2]



Server Side

- Cloudflare switch on ECH deployment for many websites.
  - See if the cloudflare hosted website is encrypted *"{domain}/cdn-cgi/trace"*

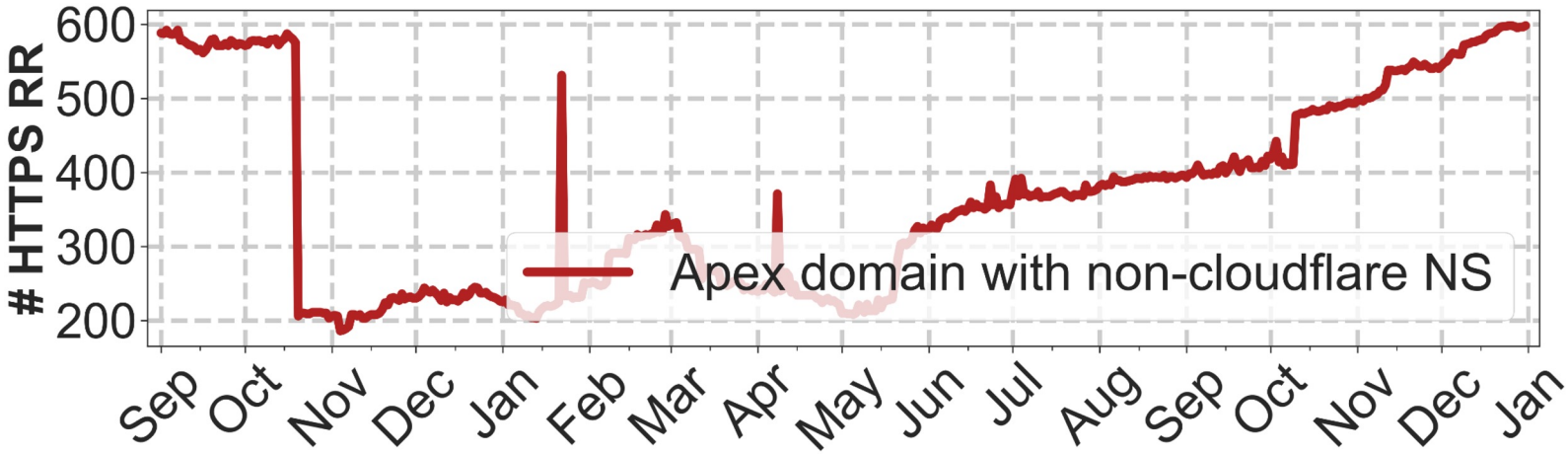
```
http=http/2
loc=US
tls=TLSv1.3
sni=encrypted
warp=off
```

1. https://www.mozilla.org/en-US/firefox/129.0/releasenotes/
2. https://github.com/27justin/ohmyech

Name Servers Support of HTTPS RR

Average ratio:
Cloudflare related: 99.85%
Others: 0.15%

- Other observed non-Cloudflare DNS providers/entities that support HTTPS RR:
  - Entities:Google, Facebook, etc.
  - Providers: GoDaddy, NS1, Akamai, AWS, Domeneshop, deSEC, etc.



Non-Cloudflare DNS providers supporting HTTPS records

HTTPS RR Parameters

- Cloudflare HTTPS RR practices:

```
a.com. 300 IN HTTPS 1 . alpn=h2,h3
ipv4hint=a.b.c.d ipv6hint=e:f::g
```

- Other DNS providers' HTTPS RR practices:

	Google NS	*GoDaddy* NS
SvcPriority	1 (98.95%)	0 (99.19%)
TargetName	. (98.95%)	An alternative endpoint (99.19%)
alpn	- (95.11%)	- (99.19%)
ipv4hint	- (97.76%)	- (99.19%)
ipv6hint	- (98.90%)	- (99.19%)

Browser Support

		Chrome		Safari	Edge		Firefox	
OS		macOS	Windows	macOS	macOS	Windows	macOS	Windows
Browser Version		120.0.6099		17.2.1	120.0.2210		122.0.1	
HTTPS RR Utilization	{apex}	●	●	◐	●	●	●	●
	http://{apex}	●	●	◐	●	●	●	●
	https://{apex}	●	●	●	●	●	●	●

- All four browsers send **HTTPS** queries, together with **A** and **AAAA** query
- Safari send traffic to port 80 when directed to visit `{apex}` and `http://{apex}`

- Solid-filled circle - the record or parameter is utilized
- Half solid-filled circle - the record or parameter is utilized, yet some essential function associated is lacked
- Unfilled circle - no support

Browsers' Support of HTTPS RR

- Support:
  - All browsers send **HTTPS** queries, together with **A** and **AAAA** query
  - Parameter: **alpn**
- Limited support:
  - **AliasMode** and other parameters
- Inconsistent handling**:**
  - Firefox* and Safari connect to the IPs in ***IP Hints*** parameter.
  - Chrome and Edge connect to the IPs in ***A/AAAA*** records.

		Chrome		Safari	Edge		Firefox	
OS		macOS	Windows	macOS	macOS	Windows	macOS	Windows
Browser Version		120.0.6099		17.2.1	120.0.2210		122.0.1	
HTTPS RR Utilization	{apex}	●	●	◐	●	●	●	●
	http://{apex}	●	●	◐	●	●	●	●
	https://{apex}	●	●	●	●	●	●	●
AliasMode	TargetName	○	○	●	○	○	○	○
ServiceMode	TargetName	○	○	●	○	○	●	●
	port	○	○	●	○	○	●	●
	alpn	●	●	●	●	●	●	●
	IP Hints	○	○	●	○	○	●	●

*Firefox now visit IPs in A/AAAA records.

Background

DNS HTTPS resource records

- SVCB (service binding) record tailored to the HTTPS protocol
- Provide essential information for accessing HTTPS services
- Two modes: ServiceMode vs. AliasMode (`SvcPriority` parameter)

```
example.com. 300 IN HTTPS 0 anotherdomain.com
example.com. 300 IN HTTPS 1 . alpn=h3 ipv4hint=1.2.3.4.
```

Encrypted ClientHello (ECH)

- Allow client to encrypt its initial ClientHello message in a TLS session
- ECH public key is delivered through DNS HTTPS records

```
example.com. 300 IN HTTPS 1 . alpn=h3
ech={version,...,public_name=public.com,...,Keyconfig,...}
```

Domain Name System Security Extensions (DNSSEC)

- Secure DNS by authenticating responses to domain name lookups
- Protect DNS against threats like cache poisoning

ClientHello without ECH

ClientHello
Sensitive Info
(SNI: example.com, ALPN, key share…)

ClientHello with ECH

Outer ClientHello
Non-sensitive Info
(Outer SNI: public.com, ALPN, key share…)

(Encrypted) Inner ClientHello
Sensitive Info
(Inter SNI: example.com, ALPN, key share…)