Hasso Plattner Institut
Digital Engineering · Universität Potsdam

# The Fragile Privacy of Encrypted Client Hello:
## Quantifying Systemic Gaps in a Centralized Ecosystem

***Jannis Hajda***, Bengin Oezdil, John Bauer,
Felix Hoffmann, Vaibhav Bajpai

{jannis.hajda, bengin.oezdil, john.bauer, felix.hoffmann}@student.hpi.de

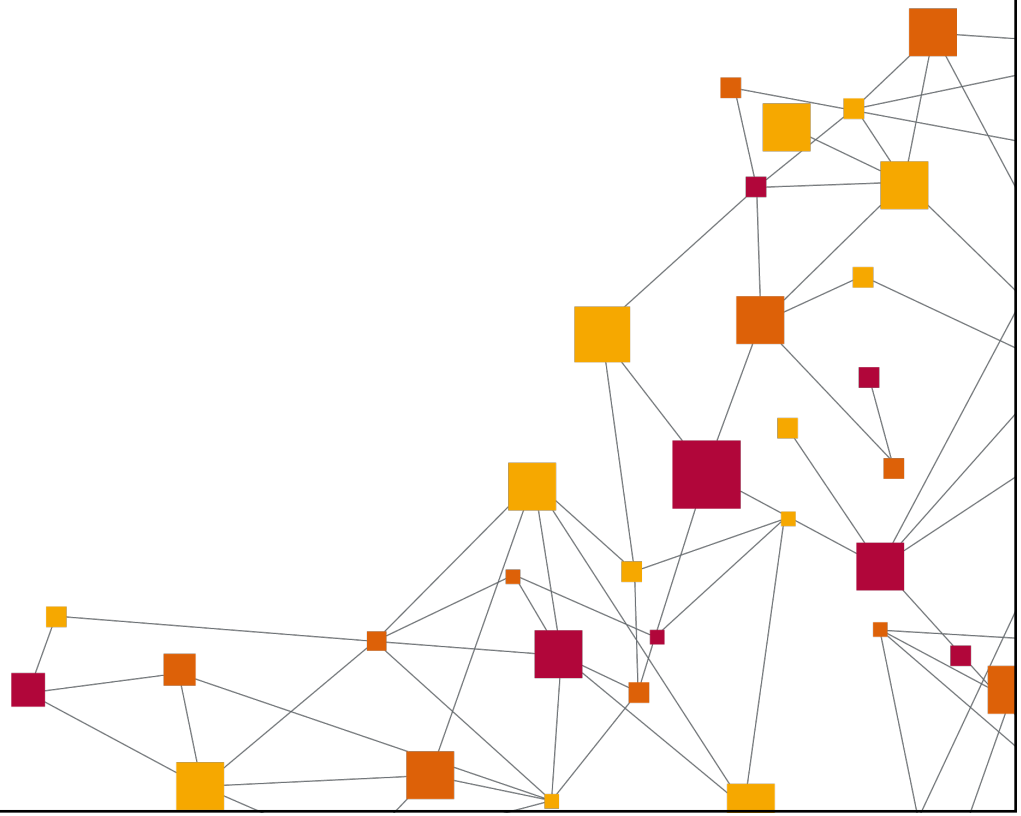
vaibhav.bajpai@hpi.de

**Design IT.**
**Create Knowledge.**

www.hpi.de

HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

# Preliminaries



**Design IT.**
**Create Knowledge.**

www.hpi.de

# Preliminaries

TLS 1.3 encrypts sessions between client and server

→ BUT: SNI field leaks target hostname in clear

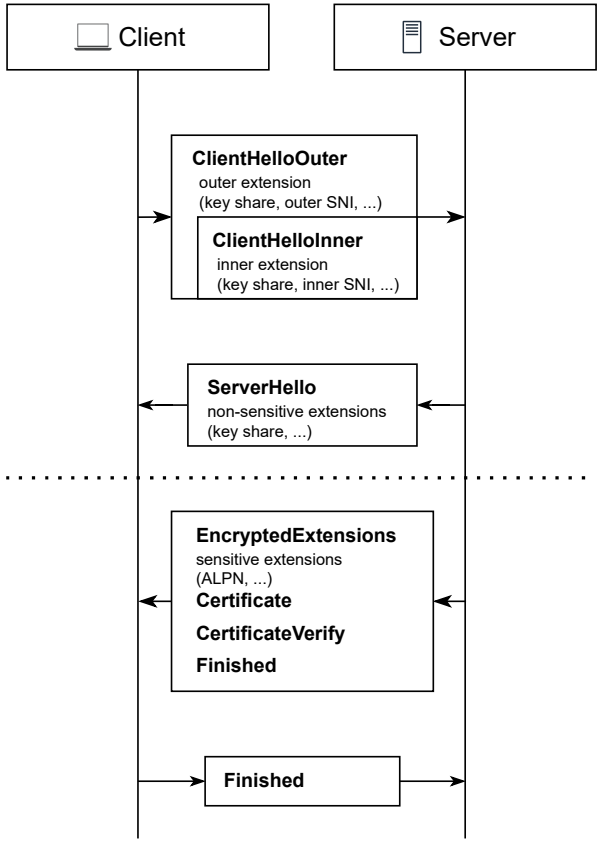
→ on-path observers can determine/block accessed service

**The ECH Solution (RFC 9849; March 2026)**

- Encapsulation: Hide sensitive ClientHelloInner inside benign ClientHelloOuter
- Key Distribution: Relies on public keys distributed via DNS (SVCB/HTTPS)

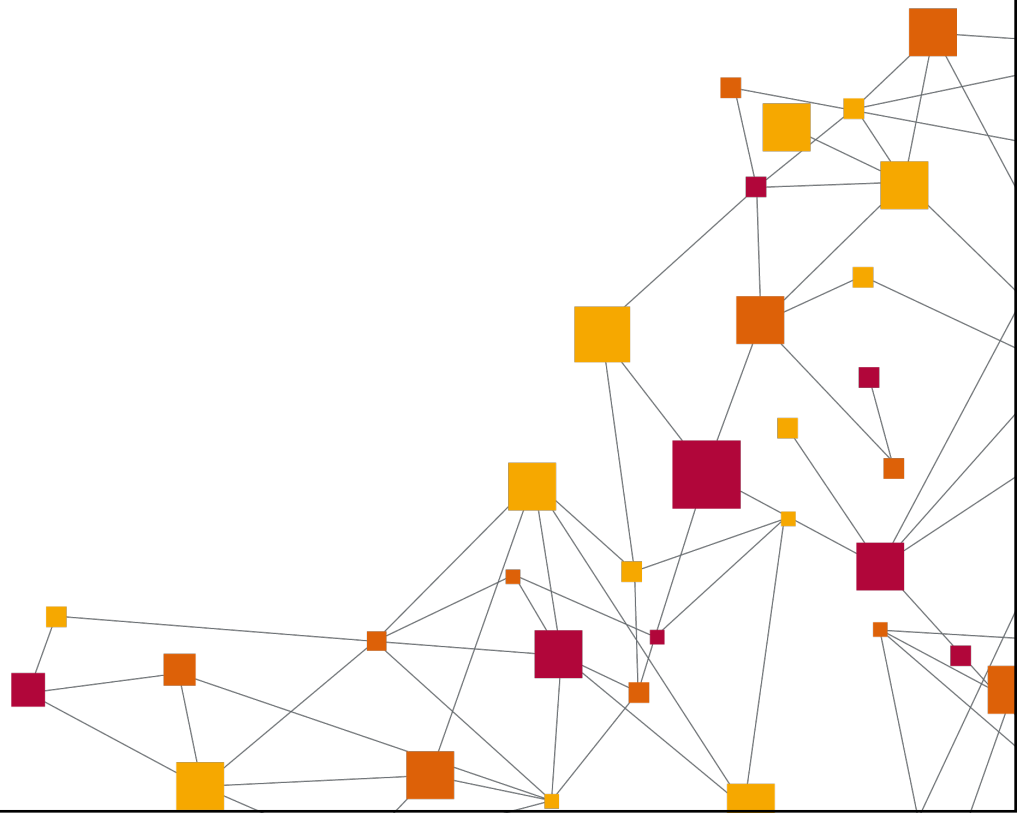
→ Privacy benefits of ECH rely on usage of private DNS (DoH/DoT/…)

- GREASE: Clients include randomized ECH extensions (prevent middlebox ossification)



HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

# Measurement study



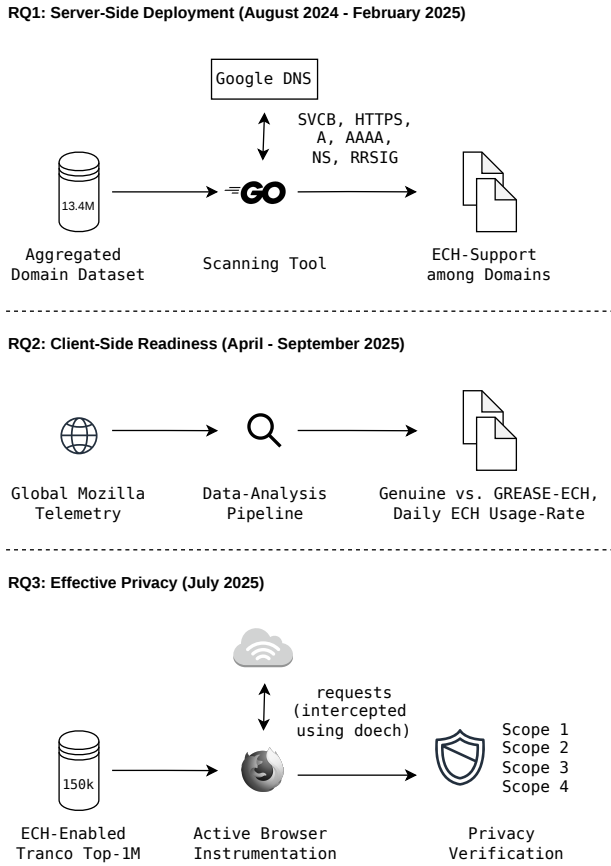
**Design IT.**
**Create Knowledge.**

www.hpi.de

# Measurement study

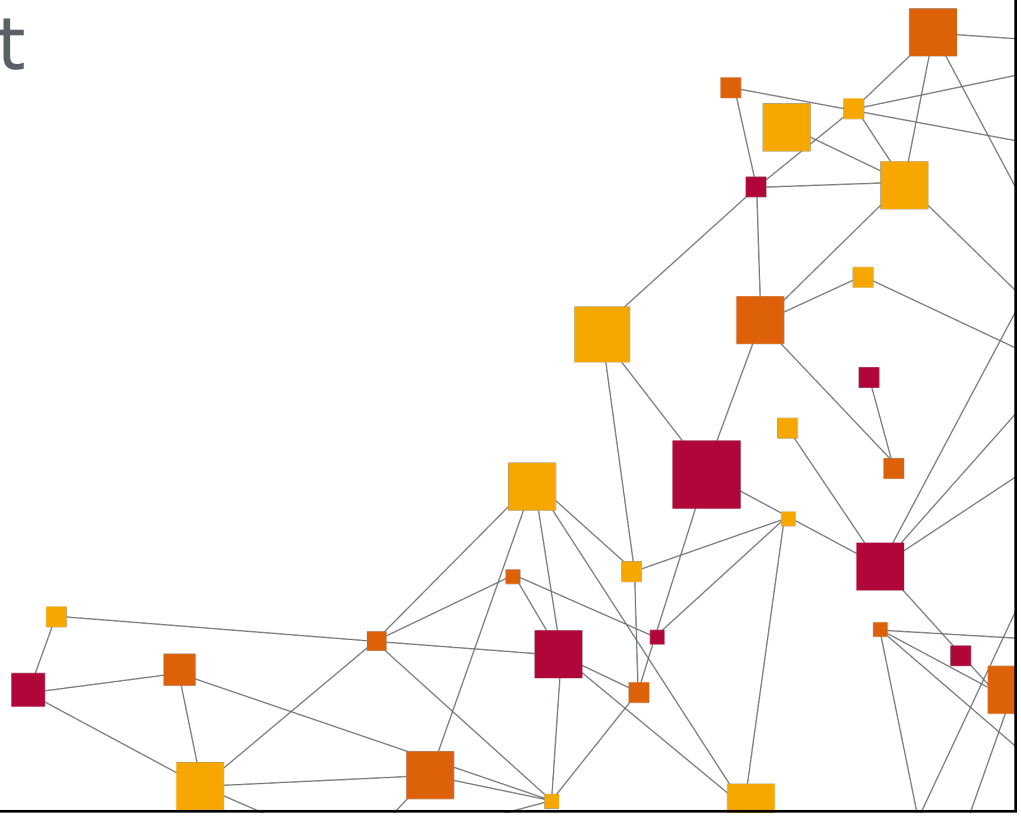
**Goal**: Analyze the global ECH ecosystem across three distinct vantage points

1. **Server-Side Deployment Landscape:**
   How many sites publish ECH configurations via DNS?
2. **Client-Side Readiness:**
   What's the actual usage rate in the wild?
3. **Effective privacy:**
   Do privacy promises hold true across complex page loads?



HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

# RQ1: Server-Side Deployment Landscape



**Design IT.**
**Create Knowledge.**

www.hpi.de

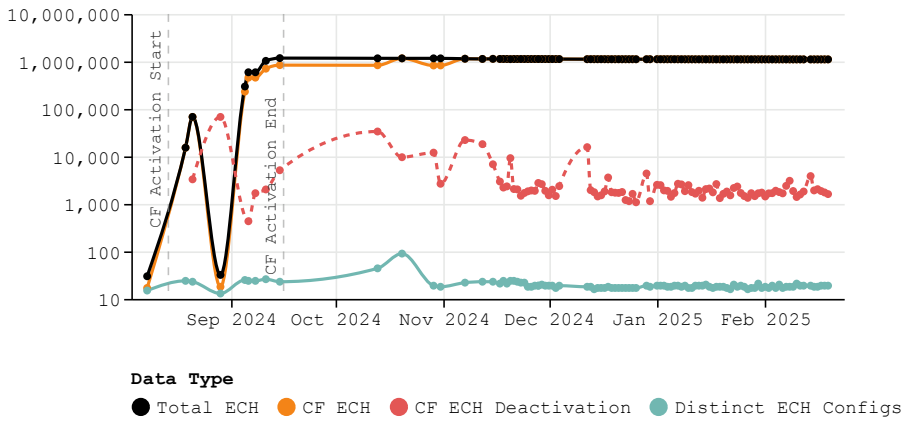
# RQ1: Server-Side Deployment Landscape

**Methodology**:

- Compiled aggregated dataset of around 13.4M domains from different top-lists
- Custom Go-Scanning tool querying DNS records

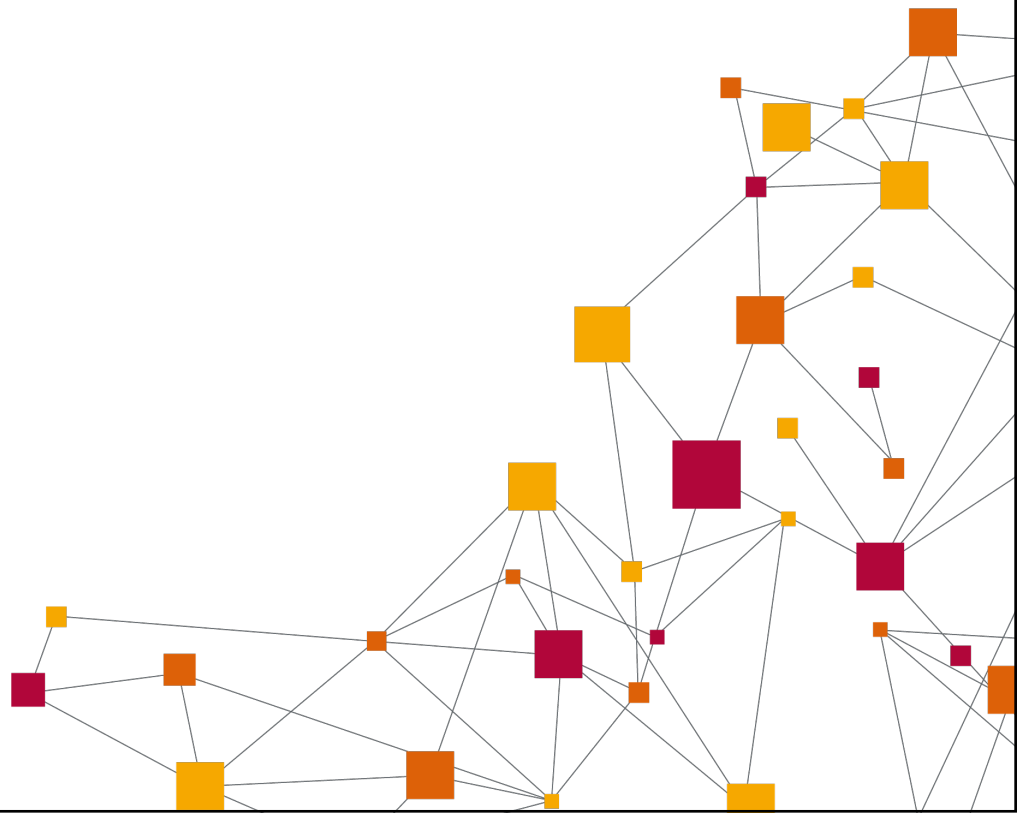
**Results (August 2024 – February 2025):**

- Roughly 1.1M active ECH deployments (15 with DNSSec)
- Highly centralized (99.99% Cloudflare; huge anonymity sets) → individual deployments with very small anonymity sets
- Near-total homogenization of cryptographic parameters



Hasso Plattner Institut
Digital Engineering · Universität Potsdam

# RQ2: Client-Side Readiness



**Design IT.**
**Create Knowledge.**

www.hpi.de

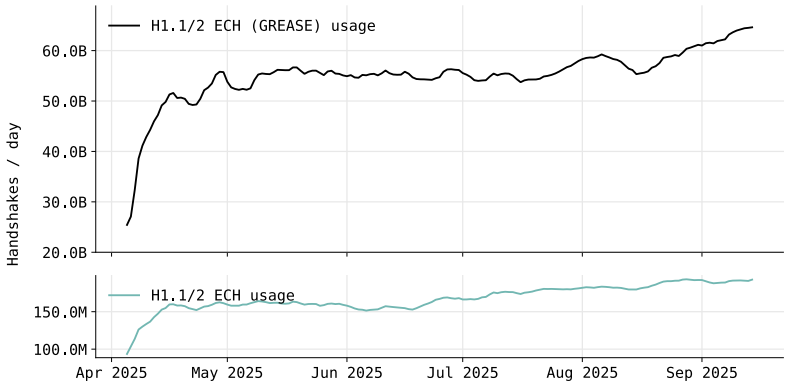
# RQ2: Client-Side Readiness

**Methodology**:

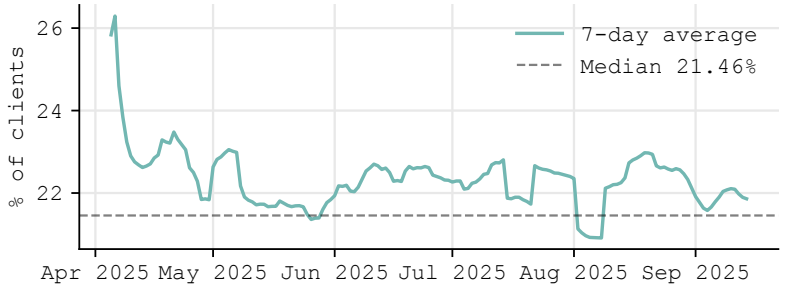
- Analysis of aggregated Firefox Telemetry provided by Mozilla
- Data from 237 countries/territories, reflecting roughly 45M clients (nearly ¼ of all clients in that timeframe)

**Results (April – September 2025):**

- Two orders of magnitude difference between GREASE and real ECH handshakes
- Roughly 1 in 5 Firefox users used ECH daily



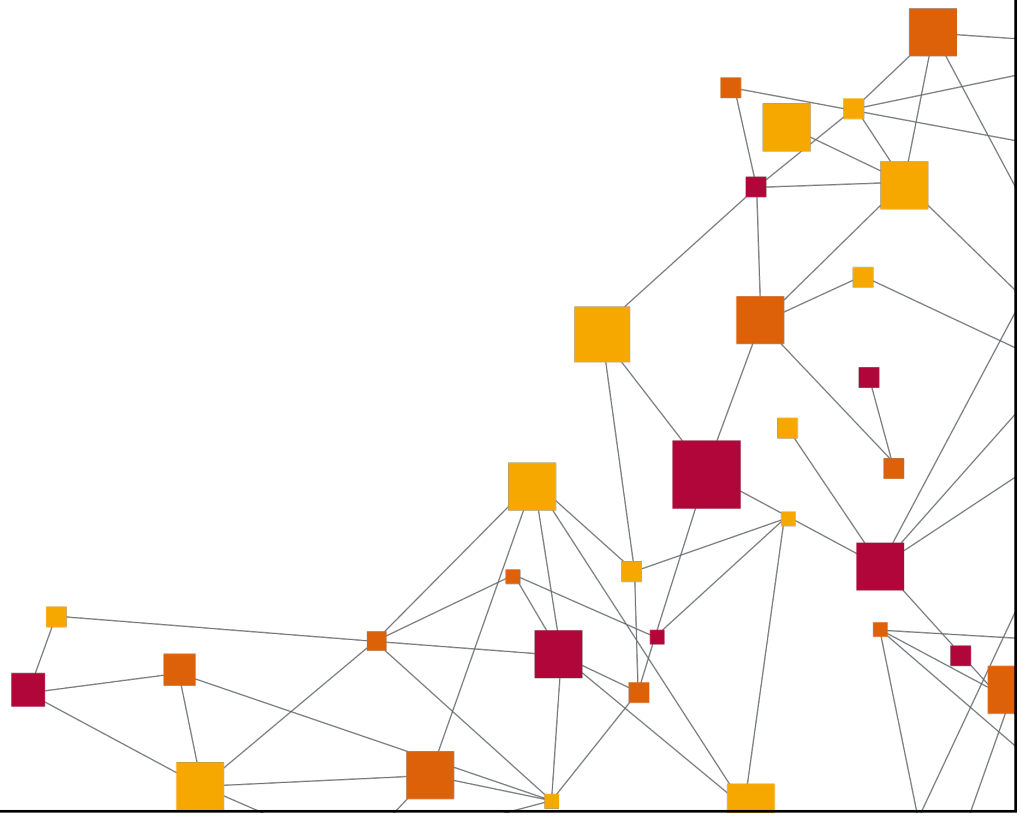

Share of GREASE vs. real ECH handshakes




Global share of Firefox users using real ECH at least once a day

Hasso Plattner Institut
Digital Engineering · Universität Potsdam

# RQ3: Effective privacy



**Design IT.**
**Create Knowledge.**

www.hpi.de

# RQ3: Effective privacy

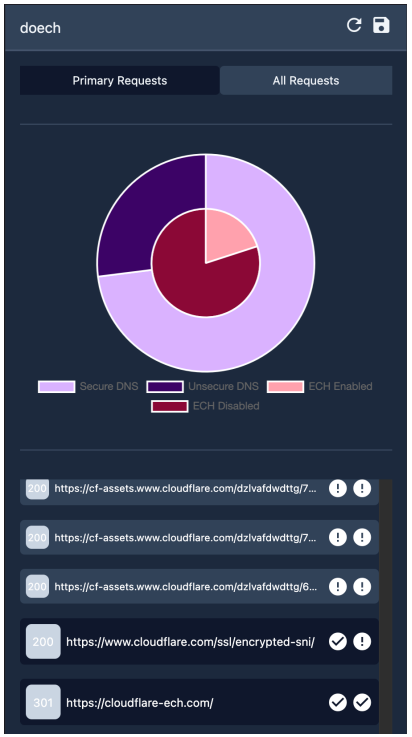
Hostname privacy does not stop at initial request

→ every request to registered domain (e.g., www, api, cdn) during full page load needs to use private DNS & ECH

**Methodology**:

- Built Firefox extension to check DoH & ECH usage on a per-request level (doech)
- Automated Firefox using Selenium
- Overhead of active browser instrumentation

  → limited analysis to 154k domains from Tranco Top-1M indicating ECH support




Sidebar of our custom doech extension (available in Firefox extension store)

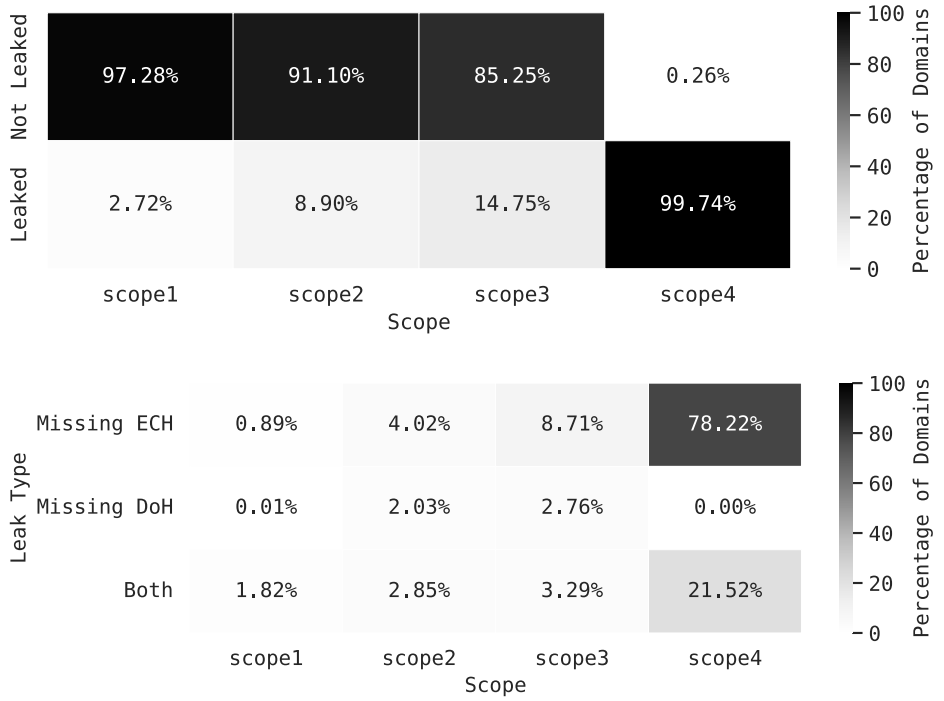
# RQ3: Effective privacy

Defined four cumulative privacy-scopes for evaluating hostname leakage:

**1. Initial Connection:**

False advertisement occurred rarely

2. Same Registered Domain
3. Redirect Chain
4. Full-Page Load




Leakage across different scopes and leakage reasons

# RQ3: Effective privacy

Defined four cumulative privacy-scopes for evaluating hostname leakage:

1. Initial Connection
2. **Same Registered Domain:**

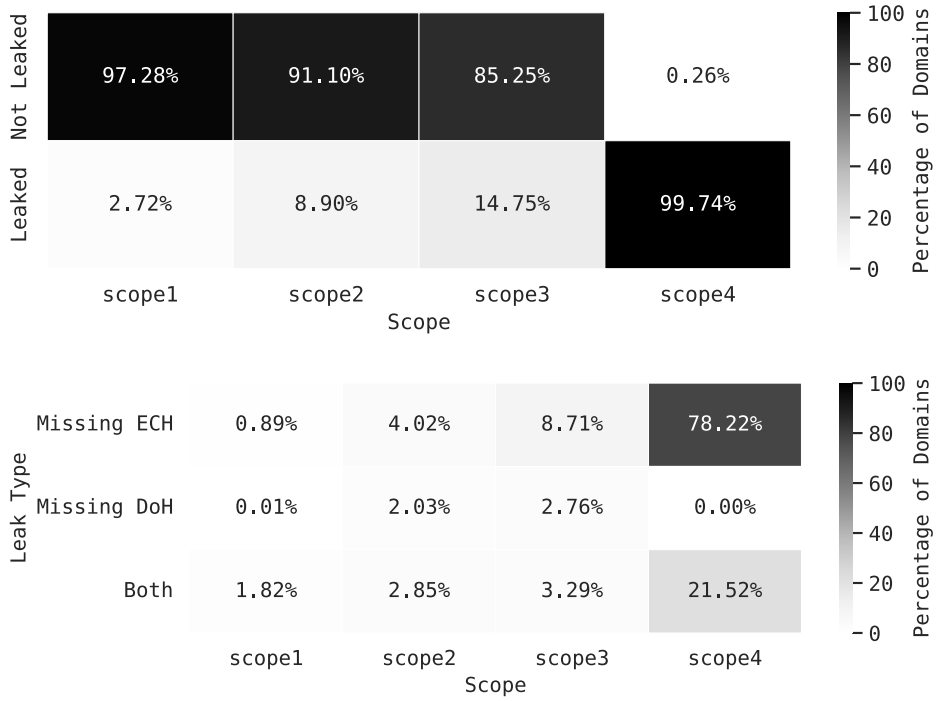
Distinct increase in leakage rate (6505 systematic)

→ 80% solely on subdomains

Top offenders (cases):

www (1677), cdn (392), api (221)

3. Redirect Chain
4. Full-Page Load




Leakage across different scopes and leakage reasons

# RQ3: Effective privacy

Defined four cumulative privacy-scopes for evaluating hostname leakage:

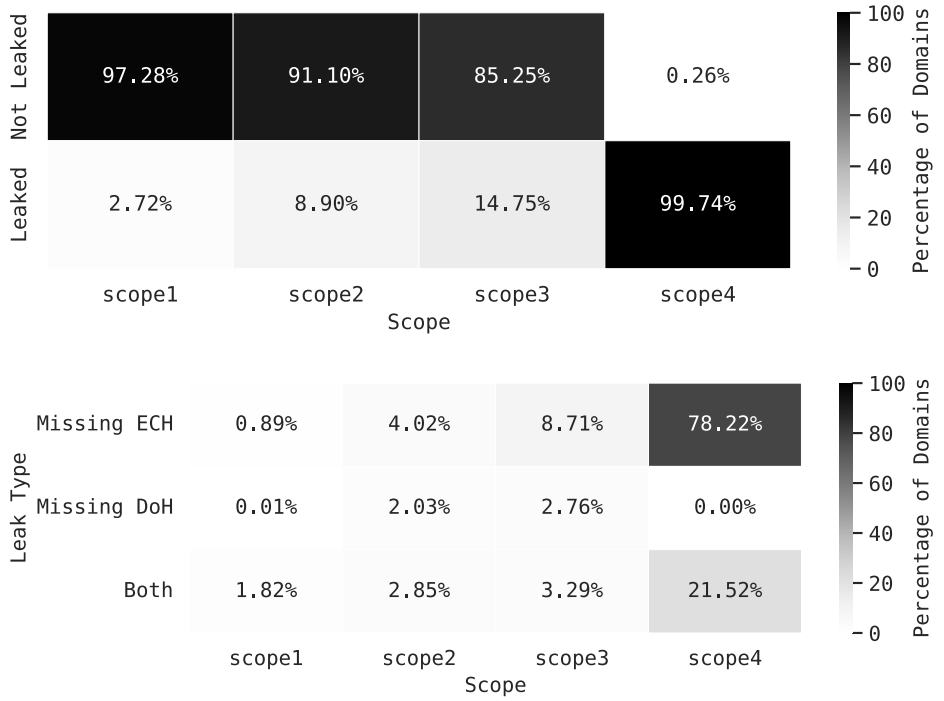
1. Initial Connection
2. Same Registered Domain
3. **Redirect Chain:**

Again: Further increase in leakage rate

Privacy impact? Depends on relationship

Example: cloudflare-ech.com → cloudflare.com

4. Full-Page Load




Leakage across different scopes and leakage reasons

# RQ3: Effective privacy

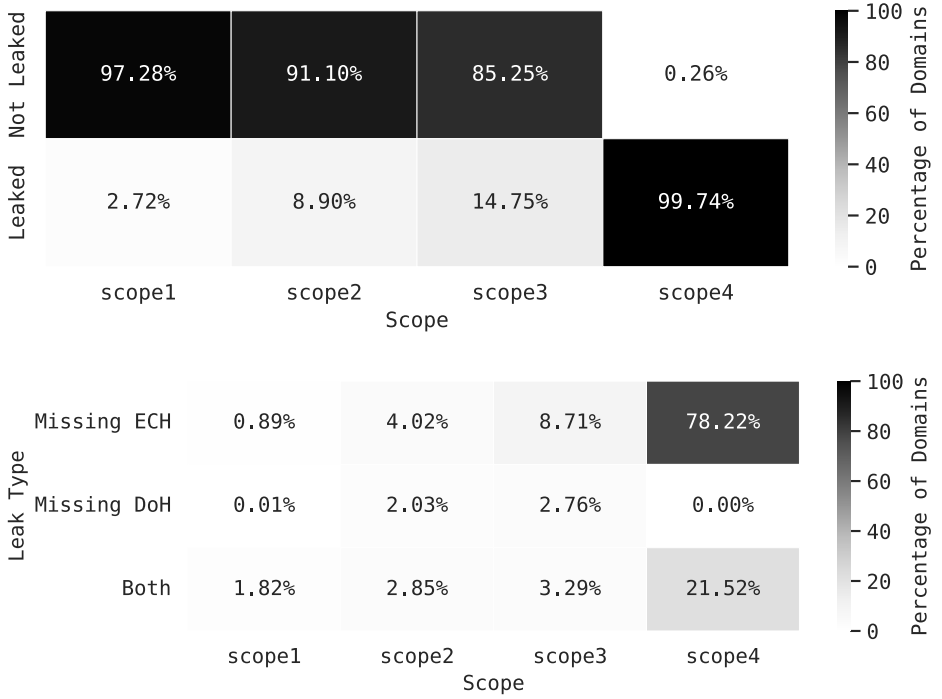
Defined four cumulative privacy-scopes for evaluating hostname leakage:

1. Initial Connection
2. Same Registered Domain
3. Redirect Chain
4. **Full-Page Load:**

Near total leakage rate → Third-Party Reality

Does not imply ineffectiveness of ECH

Distinct increase in missing DoH




Leakage across different scopes and leakage reasons

# Discussion and Future Work

Cloudflare monoculture & Supply-Demand Gap

→ other providers need to follow

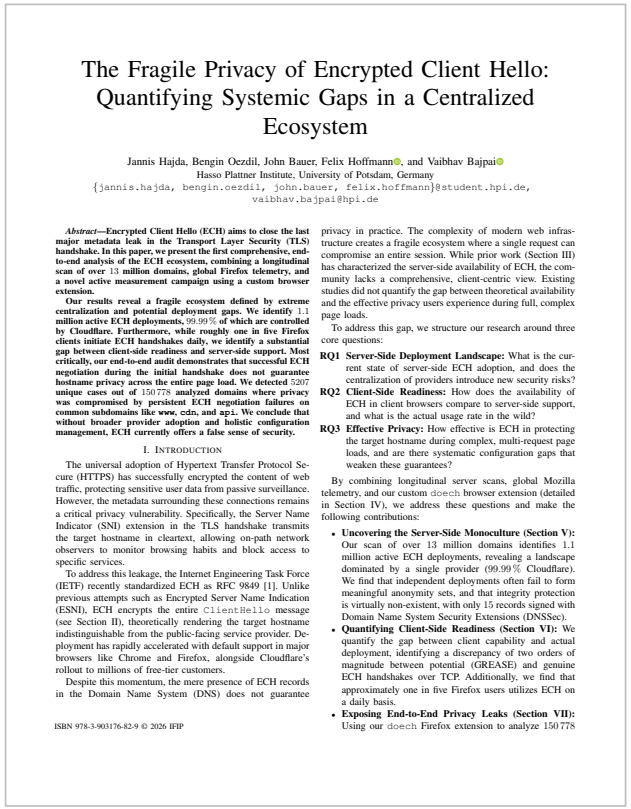
False sense of security

→ holistic configuration management by all parties across entire infrastructure stack

Next steps:

Build combined pipeline to broaden analysis

Analyze fingerprinting capabilities based on Scope 3 + 4



The Fragile Privacy of Encrypted Client Hello: Quantifying Systemic Gaps in a Centralized Ecosystem

Jannis Hajda, Bengin Oezdil, John Bauer, Felix Hoffmann, and Vaibhav Bajpai
Hasso Plattner Institute, University of Potsdam, Germany
{jannis.hajda, bengin.oezdil, john.bauer, felix.hoffmann}@student.hpi.de, vaibhav.bajpai@hpi.de

***Abstract*—Encrypted Client Hello (ECH) aims to close the last major metadata leak in the Transport Layer Security (TLS) handshake. In this paper, we present the first comprehensive, end-to-end analysis of the ECH ecosystem, combining a longitudinal scan of over 13 million domains, global Firefox telemetry, and a novel active measurement campaign using a custom browser extension.**

**Our results reveal a fragile ecosystem defined by extreme centralization and potential deployment gaps. We identify 1.1 million active ECH deployments, 99.99% of which are controlled by Cloudflare. Furthermore, while roughly one in five Firefox clients initiate ECH handshakes daily, we identify a substantial gap between client-side readiness and server-side support. Most critically, our end-to-end audit demonstrates that successful ECH negotiation during the initial handshake does not guarantee hostname privacy across the entire page load. We detected 5207 unique cases out of 150 778 analyzed domains where privacy was compromised by persistent ECH negotiation failures on common subdomains like `www`, `cdn`, and `api`. We conclude that without broader provider adoption and holistic configuration management, ECH currently offers a false sense of security.**

I. Introduction

The universal adoption of Hypertext Transfer Protocol Secure (HTTPS) has successfully encrypted the content of web traffic, protecting sensitive user data from passive surveillance. However, the metadata surrounding these connections remains a critical privacy vulnerability. Specifically, the Server Name Indicator (SNI) extension in the TLS handshake transmits the target hostname in cleartext, allowing on-path network observers to monitor browsing habits and block access to specific services.

To address this leakage, the Internet Engineering Task Force (IETF) recently standardized ECH as RFC 9849 [1]. Unlike previous attempts such as Encrypted Server Name Indication (ESNI), ECH encrypts the entire `ClientHello` message (see Section II), theoretically rendering the target hostname indistinguishable from the public-facing service provider. Deployment has rapidly accelerated with default support in major browsers like Chrome and Firefox, alongside Cloudflare's rollout to millions of free-tier customers.

Despite this momentum, the mere presence of ECH records in the Domain Name System (DNS) does not guarantee privacy in practice. The complexity of modern web infrastructure creates a fragile ecosystem where a single request can compromise an entire session. While prior work (Section III) has characterized the server-side availability of ECH, the community lacks a comprehensive, client-centric view. Existing studies did not quantify the gap between theoretical availability and the effective privacy users experience during full, complex page loads.

To address this gap, we structure our research around three core questions:

**RQ1 Server-Side Deployment Landscape:** What is the current state of server-side ECH adoption, and does the centralization of providers introduce new security risks?

**RQ2 Client-Side Readiness:** How does the availability of ECH in client browsers compare to server-side support, and what is the actual usage rate in the wild?

**RQ3 Effective Privacy:** How effective is ECH in protecting the target hostname during complex, multi-request page loads, and are there systematic configuration gaps that weaken these guarantees?

By combining longitudinal server scans, global Mozilla telemetry, and our custom `doech` browser extension (detailed in Section IV), we address these questions and make the following contributions:

- **Uncovering the Server-Side Monoculture (Section V):** Our scan of over 13 million domains identifies 1.1 million active ECH deployments, revealing a landscape dominated by a single provider (99.99% Cloudflare). We find that independent deployments often fail to form meaningful anonymity sets, and that integrity protection is virtually non-existent, with only 15 records signed with Domain Name System Security Extensions (DNSSec).
- **Quantifying Client-Side Readiness (Section VI):** We quantify the gap between client capability and actual deployment, identifying a discrepancy of two orders of magnitude between potential (GREASE) and genuine ECH handshakes over TCP. Additionally, we find that approximately one in five Firefox users utilizes ECH on a daily basis.
- **Exposing End-to-End Privacy Leaks (Section VII):** Using our `doech` Firefox extension to analyze 150 778

ISBN 978-3-903176-82-9 © 2026 IFIP

Hasso Plattner Institut
Digital Engineering · Universität Potsdam

# The Fragile Privacy of Encrypted Client Hello:

## Quantifying Systemic Gaps in a Centralized Ecosystem

## Key-Findings:

- Highly centralized infrastructure (Cloudflare)
- Supply-Demand Gap
- Deployment gaps undermining privacy

Interested in a PhD position?

Visit our website or let's have a chat!

https://hpi.de/bajpai

**Design IT.**
**Create Knowledge.**

www.hpi.de