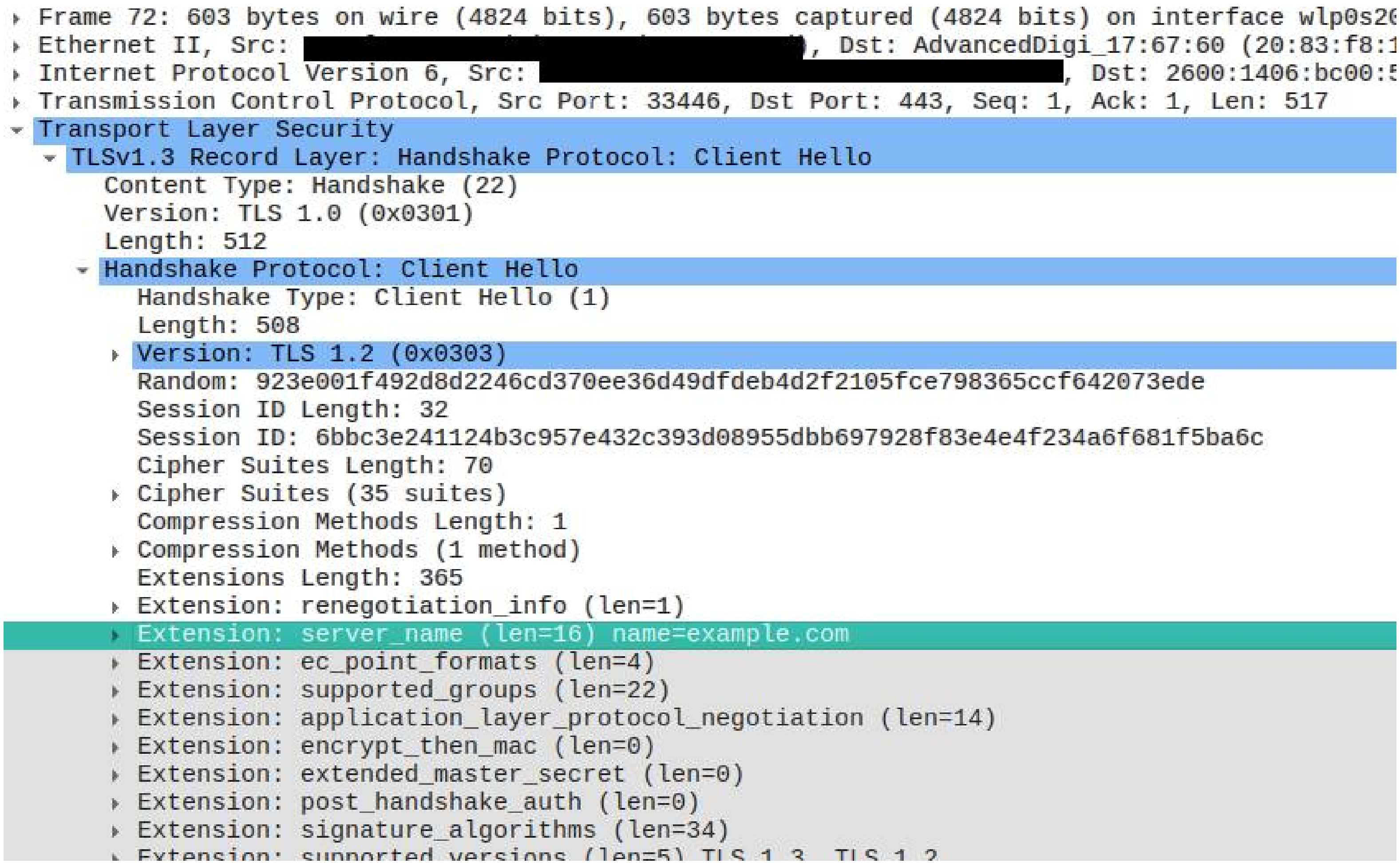
Challenges on closing the last gap in TLS: Encrypted Client Hello

Aaron Kaplan

Sebastian Wagner



```
▸ Frame 72: 603 bytes on wire (4824 bits), 603 bytes captured (4824 bits) on interface wlp0s2
▸ Ethernet II, Src: [redacted], Dst: AdvancedDigi_17:67:60 (20:83:f8:1
▸ Internet Protocol Version 6, Src: [redacted], Dst: 2600:1406:bc00:5
▸ Transmission Control Protocol, Src Port: 33446, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▾ Transport Layer Security
  ▾ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    ▾ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 508
      ▸ Version: TLS 1.2 (0x0303)
        Random: 923e001f492d8d2246cd370ee36d49dfdeb4d2f2105fce798365ccf642073ede
        Session ID Length: 32
        Session ID: 6bbc3e241124b3c957e432c393d08955dbb697928f83e4e4f234a6f681f5ba6c
        Cipher Suites Length: 70
      ▸ Cipher Suites (35 suites)
        Compression Methods Length: 1
      ▸ Compression Methods (1 method)
        Extensions Length: 365
      ▸ Extension: renegotiation_info (len=1)
      ▸ Extension: server_name (len=16) name=example.com
      ▸ Extension: ec_point_formats (len=4)
      ▸ Extension: supported_groups (len=22)
      ▸ Extension: application_layer_protocol_negotiation (len=14)
      ▸ Extension: encrypt_then_mac (len=0)
      ▸ Extension: extended_master_secret (len=0)
      ▸ Extension: post_handshake_auth (len=0)
      ▸ Extension: signature_algorithms (len=34)
      ▸ Extension: supported_versions (len=5) TLS 1.3, TLS 1.2
```

History

- 2003: SNI (**S**erver **N**ame **I**ndication) standardised
- 2018: Experimental **E**ncrypted SNI
- 2020: First ECH **E**ncrypted **C**lient **H**ello draft

    (draft-ietf-tls-esni-24)
- 2020-2025 defo Project funded by OTF
- certtools.github.com/defo-security-analysis/

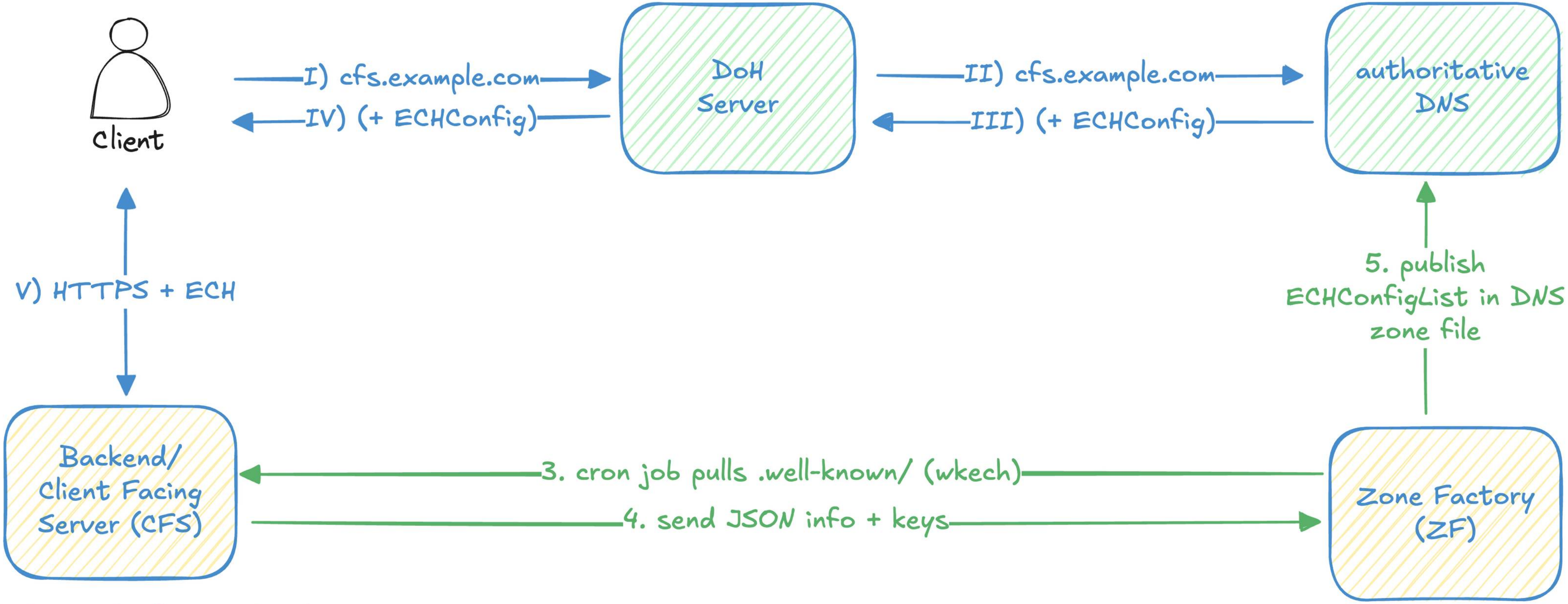
ECH Requirements

- TLSv**1.3+**
- public key **before** starting TLS
- Config/Key is in **DNS**
  - DNS **SVCB** ServiceMode record
  - Clients require **DoH**
  - **DNSSec** recommended

ECHConfig

```
ECHConfig:
   Version
   Length
   ECH Config Contents:
      HPKE Key Config:
           Config ID
           KEM ID
           Public Key
           HPKE symmetric cipher suite
       Maximum Name Length
       Public Name
       ECHConfigExtension …
```

Deployment



Client

I) cfs.example.com

IV) (+ ECHConfig)

DoH Server

II) cfs.example.com

III) (+ ECHConfig)

authoritative DNS

V) HTTPS + ECH

5. publish ECHConfigList in DNS zone file

Backend/ Client Facing Server (CFS)

3. cron job pulls .well-known/ (wkech)

4. send JSON info + keys

Zone Factory (ZF)

1. Server (re-)generates keys
2. Server publishes these in .well-known

Implementation Status

	Servers	Clients & Libraries	Browsers
✔	Lighttpd	BoringSSL, golang Rustls (client) curl	Firefox, Chromium
WIP (Forks, Branches)	Nginx, Apache, HAProxy	OpenSSL, gnuTLS Cpython wget2 Conscrypt, F-Droid	Edge

Split-Mode vs Shared-Mode

```
                +---------------------+              +--------------------+     +---------------------+
                |                     |              |                    |     |                     |
                |   2001:DB8::1111    |              |   2001:DB8::1111   |     |   2001:DB8::EEEE    |
                |                     |   Client <----------------------------->|                     |
Client <----->  | private.example.org |              | public.example.com |     | private.example.org |
                |                     |              |                    |     |                     |
                | public.example.com  |              +--------------------+     +---------------------+
                |                     |               Client-Facing Server            Backend Server
                +---------------------+
                        Server

          (Client-Facing and Backend Combined)

                   Shared Mode Topology                              Split Mode Topology
```

Zone Factory

```
                    +--------------------+
                    |                    |
 TLS                |   2001:DB8::1111   | Client-
Client <----------->|                    | facing
                    |   cfs.example.com  | server
                    | backend.example.com|
                    +--------------------+
                        ^            ^
     (1) ZF reads       |            |  (2) ZF checks
         .well-known    V            V      ECHConfig
                    +--------------------+
                    |                    |
                    |   zf.example.net   | Zone Factory (ZF)
                    |                    |
                    +--------------------+
                              |
                              | (3) ZF publishes new HTTPS RR
                              V
                    +--------------------+
                    |                    |
                    |   ns.example.net   | Authoritative DNS
                    |                    |
                    +--------------------+
```

WKECH Example

```
{
   "regeninterval": 3600,
   "endpoints": [{
       "priority": 1,
       "target": "cdn.example",
       "params": {
           "ech": "AD7+DQA65wAgAC..AA=="
       }
     }, {
         "priority": 1,
         "params": {
             "port": 8413,
             "ech": "AD7+DQA65wAgAC..AA=="
         }
      }
    ]
}
```

Separation issues

- Network separations
- Process separations
- Organizational separations

DoH/DoT

- Blocking prevents ECH use
- Tor Network: Without DoH

Incentives

- Anti-Censor and Anti-Oppression
- Malware/C2
- Pornography
- CDNs
- Small and medium size hosters

Censorship and Blocking

- Russia disallowing CDNs in order to block ECH
  - https://therecord.media/russia-blocks-thousands-of-websites-that-use-cloudflare-service
- China
- South Korea blocks websites by SNI

De-Anonymization

- Correlation
- Legal means