An introduction to Encrypted Client Hello:

Balancing privacy benefits with potential unintended network and customer experience consequences.

Chris Box, Andy Fidler

UKNOF 2nd November 2020

What is Encrypted Client Hello

- **ISP customers are using HTTPS for nearly every website, but the name of the website you are visiting is still visible at the start of every connection.**
- **Encrypted Client Hello (ECH) is a new standard being developed in the IETF to hide the true Server Name Indication (SNI) for extra privacy.**
- **It works by encrypting the sensitive name and wrapping this in an outer envelope with a public name, such as that of the CDN, written on the front.**

- By analogy, in a traditional letter the name of the person you're writing to is visible on the envelope. Encrypted Client Hello still has a visible name on the envelope but it's generic such as "Hosting company, London". However inside the envelope there is a second envelope, with the genuine destination name "Sensitive website" written on it.

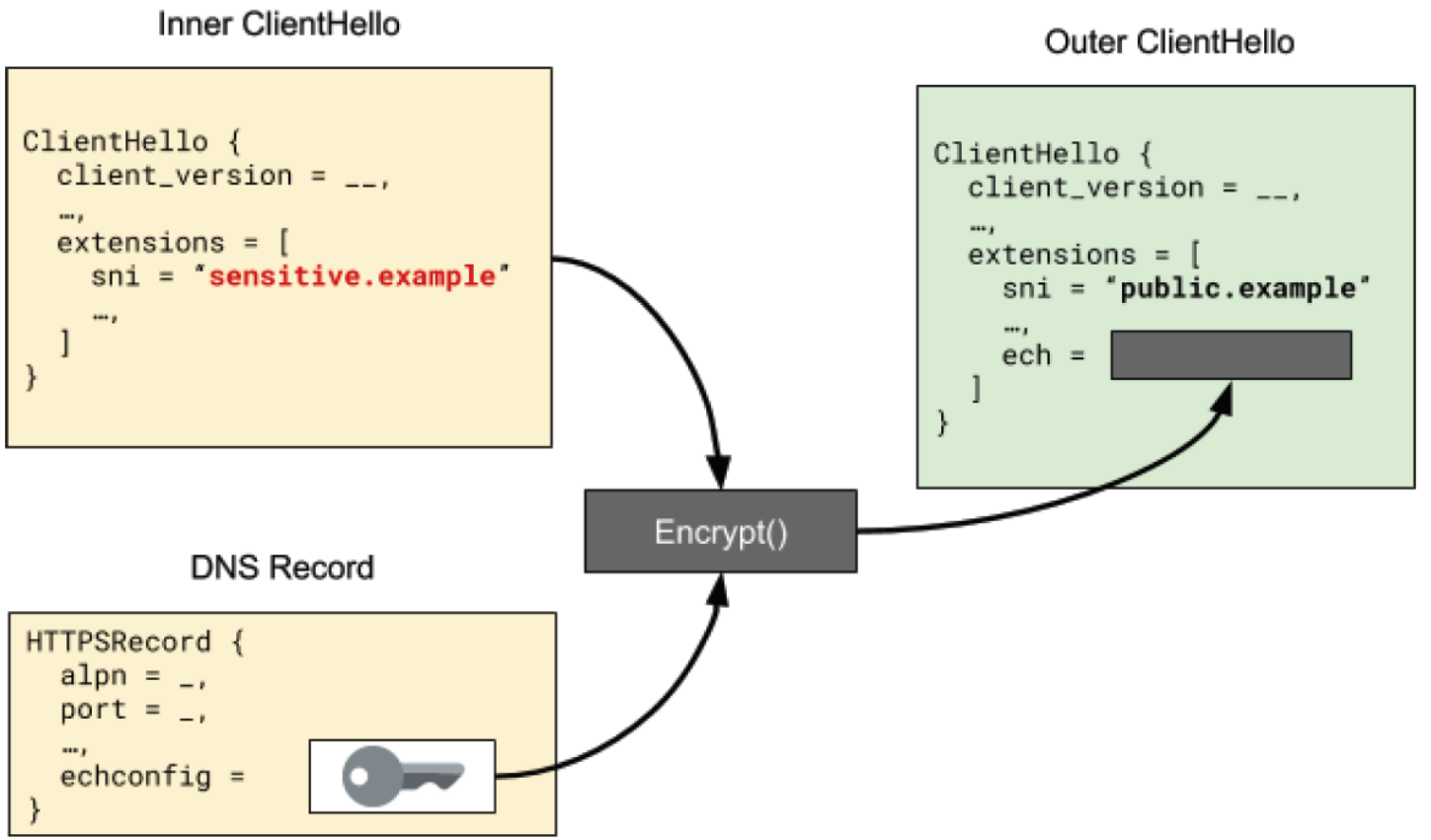

Image source: Chrome https://docs.google.com/document/d/1jOwfbFMJx_tP9ppoS7TQxPlsgwarWVL9YzGMoX_Ww3M/

How it works

- **New TLS 1.3 extension, so it's possible to see when ECH is being used.**
- **The aim is to "not stick out", so this will eventually be used by the majority of ISP traffic.**
- **The necessary details to use ECH are published in an *HTTPS* record.**

What's one of those?

HTTPS is a new DNS record type (65) that tells clients all the ways in which they can contact a website.
iOS14 is already using it. For example this record says that both HTTP/2 and HTTP/3 are possible, on port 443.
example.com 3600 IN HTTPS 1 . alpn="h3,h2", port=443

Cloudflare automatically added support for HTTPS records across their base (https://blog.cloudflare.com/speeding-up-https-and-http-3-negotiation-with-dns/) and mention intending to support ECH too.

```
# dig cloudflare.com TYPE65
cloudflare.com.        300     IN      TYPE65  \# 76 000100000100150568332D32390568332D32380568332 ... (rest deleted)
```

This actually means:

```
cloudflare.com.        300     IN      HTTPS 1 . alpn="h3-29,h3-28,h3-27,h2" ipv4hint="104.17.175.85,104.17.176.85"
                                        ipv6hint="2606:4700::6811:af55,2606:4700::6811:b055"
```

ECH would enhance the above record, along these lines:

```
cloudflare.com.        300     IN      HTTPS 1 . alpn="h3-29,h3-28,h3-27,h2" ipv4hint="104.17.175.85,104.17.176.85"
                                        ipv6hint="2606:4700::6811:af55,2606:4700::6811:b055"
                                        echconfig="(visible public name to use; which encryption keys can be used)"
```

ECH – implications for network operators

Benefits

- **Enhanced privacy for customers.**
- **Realises the ambition of TLS that no man-in-the-middle should be able to observe significant details of communications.**

Known government responses

- **Russia proposed legislation that would make hiding the name of the destination illegal.**
- **China's firewall has been reported to be blocking the previous version of ECH (ESNI).**

In countries where it is permitted/encouraged, what are the potential unintended consequences requiring investigation and mitigation?

- **Impacts any parental control / content filtering solutions that are based on DPI inspection of HTTPS.** All such solutions will only see the visible public name, such as the name of the CDN hosting the content.
- **Reduces effectiveness of customer support tools and network diagnostics that look at HTTPS.**
- **Limits operator ability to make certain traffic free of charge, e.g. NHS COVID-19 app. Would require the content provider to be willing to exclude themselves from ECH, or use another mechanism such as static IPs.**
- **Complicates ability of public hotspot operators to white list content within a captive portal.**
- **Makes enforcement of security policy, such as blocking malware, more difficult.**

BT

Conclusion

- **BT looks favourably on new capabilities that enhance privacy and security for our customers.**
- **However whilst increasing privacy, Encrypted Client Hello risks creating significant unintended consequences to customer experience and network support.**
- **BT would welcome industry dialogue on the optimal way of offering new privacy features whilst still mitigating the network and customer experience consequences.**

Appendix - notes on protocol adoption

- **Current IETF draft:** https://tools.ietf.org/html/draft-ietf-tls-esni-08, with the DNS publication details in https://tools.ietf.org/html/draft-ietf-dnsop-svcb-https-01#section-8
- **Chrome have started to share their plans around prototyping ECH -** https://docs.google.com/document/d/1jOwfbFMJx_tP9ppoS7TQxPlsgwarWVL9YzGMoX_Ww3M/edit#
- **Mozilla are working on supporting the current draft of ECH.**
- **The ECH protocol design is still evolving, so public deployments for testing are not yet available.**