Briefing

The Impact of the Proposed Encrypted Client Hello Standard on the Education and Finance Sectors

Andrew Campling
18th August 2021

419.Consulting

(This page is intentionally blank)

The Impact of the Proposed Encrypted Client Hello Standard on the Education and Finance Sectors

1. Foreword

A series of technologies are currently being developed that are intended to improve the privacy of the Internet by updating or extending some of the core standards that underpin its operation. These changes are being led within various working groups of the Internet Engineering Task Force (IETF), leveraging the expertise of developers drawn from across the industry.

A recent roundtable discussion looked in detail at one of the proposed enhancements, Encrypted Client Hello (ECH), bringing together technologists with experts from the education and finance sectors. The purpose of the discussion was to evaluate the impact of ECH and identify whether these caused any unintended consequences that would have operational or other adverse impacts for the two sectors.

This document summarises elements of the roundtable in order to highlight some of the key impacts of ECH as well as the steps that need to be taken in order to mitigate the negative consequences of its introduction, for example to protect user privacy and operational security. The conclusions and recommendations are based on the content of the discussion, augmented where necessary with additional detail whilst retaining the spirit of the points raised during the roundtable.

For those interested in more information, an explanation of ECH is included as an annex to this document, along with an explanation of transparent proxies, one of the tools adversely affected by the introduction of ECH. Detailed notes from the roundtable are available separately[1].

[1] See https://419.consulting/encrypted-client-hello

2. What is the Likely Impact of ECH?

As noted in the foreword, a recent roundtable discussion looked in detail at one of the developments being considered by the IETF to improve privacy, Encrypted Client Hello (ECH). The roundtable brought together technologists with experts from the education and finance sectors to discuss the likely operational impacts of ECH.

The industry and technical experts concluded that the introduction of ECH is likely to cause disruption in both the education and finance sectors. They raised concerns related to child safety in education settings whilst focusing on the implications for security and fraud in the finance sector.

The Education Sector

Focusing specifically on the education sector, the primary issue caused by ECH is that it is *"likely to circumvent the safeguards applied to protect children through content filtering, whether in the school or home environments, adding to adverse impacts already introduced through the use of DNS-over-HTTPS."* [2]

Content filtering is used by education establishments to protect children from exposure to malicious, adult, extremist and other content that is deemed either age-inappropriate or unsuitable for other reasons. Any bypassing of content filtering will be problematic and may compromise duties placed on education establishments: for example, schools in the UK have obligations to provide "appropriate levels of content filtering"[3], including in instances where policies allow for the use of equipment not owned by the institution, "Bring Your Own Device" (BYOD).

[2] See https://419.consulting/encrypted-client-hello pp 4

[3] See for example "Keeping children safe in education (2020): Statutory guidance for schools and colleges", https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/954314/Keeping_children_safe_in_education_2020_-_Update_-_January_2021.pdf pp 103 and "National Action Plan on Internet Safety for Children and Young People" https://www.gov.scot/binaries/content/documents/govscot/publications/strategy-plan/2017/04/national-action-plan-internet-safety-children-young-people/documents/00516921-pdf/00516921-pdf/govscot%3Adocument/00516921.pdf pp 15

The experts discussed various mitigations to address these issues, concluding that *"where they are available, alternative solutions would require more restrictions being placed on client devices, potentially combined with more intrusive software being loaded than is currently the case."* The need to load more intrusive software onto user devices in order to overcome issues caused by a standards development intended to improve user privacy is unwelcome; it may be necessary however if education establishments are to continue to meet their statutory obligations.

The Finance Sector

In the finance sector, the industry experts taking part in the roundtable noted that "*the introduction of new protocols like DoH into the corporate environment has resulted in the circumvention of many controls intended to keep people safe or control certain security postures."*[4]

Of particular concern was the ability for changes in Internet protocols to allow them to bypass systems designed to ensure that there is a clear audit trail of any communications between parties. These audit trails are an important safeguard to, for example, address concerns relating to fraudulent or insider trading: non-compliance with regulatory requirements could have financial or other consequences for financial services companies.

The other impact of ECH that caused concern was the loss of visibility of potential command and control and other activity by malicious software. This *"could lead to negative impacts on security and privacy for the enterprise, its employees or customers".* Cybersecurity is of concern to any enterprise, however the consequences of a successful attack for financial institutions can be particularly severe. It should be noted that financial services was the sector most targeted by cyber espionage in 2020[5].

The experts concluded that, as with the issues identified in the education sector, *"if ECH cannot be bypassed in these situations, it is possible that the issues it causes may have to be mitigated by significantly more invasive measures undertaken at end-points."*[6]

[4] See https://419.consulting/encrypted-client-hello pp 6
[5] See https://www.statista.com/statistics/221293/cyber-crime-target-industries/
[6] See https://419.consulting/encrypted-client-hello pp 7

Mitigating the Impacts

Ideally client software that implements support for ECH will provide device or network administrators with the ability to disable the feature. This would address some of the more significant concerns in a straightforward manner. If not, any software supporting ECH may need to be removed, assuming that suitable alternatives are available.

Where it is not possible to modify or replace software, the alternative is to introduce full proxies and certificates, including in BYOD environments. The ability for an organisation to do this will depend on the level of control that an organization is able to exert – for example, this may work with employees but would not be possible with customers. Such solutions are far more intrusive than current arrangements typically adopted in many organisations, leading to a situation where more user data needs to be examined in order to overcome problems caused by an Internet standard that is supposed to improve user privacy.

The Importance of Engaging Affected Stakeholders

On this point, roundtable participants discussed whether stakeholders from outside of the technology sector are aware of developments like ECH or know how to engage in discussions with standards bodies like the IETF[7]. This is an issue that has come up within the IETF itself, with the need for multi-stakeholder engagement identified within RFC 8890 "The Internet is for End Users"[8].

What seems to be missing in the development of ECH, and similar protocols, is a broad, multistakeholder debate to understand the full range of technical implications of such developments as well as other consequences, including in the area of public policy. At present, bodies like the IETF tend to focus on a narrow set of technical considerations, leaving those deploying and using the protocols to deal with their impacts.

The roundtable focused on education and finance, however it is possible that other sectors may see different impacts. Therefore, if the full ramifications of the introduction of ECH are to be understood, a broad range of stakeholders will need to be convened to consider both the operational and policy implications of its deployment. This review needs to include regulators, legislators, browser vendors, the sectors that use filtering, civil society and others to make sure that an architecture is developed that can reasonably work to support features such as content filtering for a wide range of use cases, for example including BYOD.

[7] See https://419.consulting/encrypted-client-hello pp 8
[8] See https://www.rfc-editor.org/rfc/rfc8890

3. Conclusions

The primary conclusions that can be drawn from the analysis of the implications of the deployment of ECH in the education and finance sectors are as follows:

1. There is **no evidence that the significant, negative impacts arising from the introduction of ECH have been thoroughly evaluated** by the group developing the ECH standard[9];
2. Where they are available, solutions to mitigate the introduction of ECH will require more restrictions being placed on client devices, possibly including the withdrawal of BYOD options, potentially combined with more intrusive software being loaded on client devices than is currently the case. Thus, **the privacy of end-users will likely be eroded rather than improved** if it is not possible to disable ECH;
3. Looking specifically at the education sector, the introduction of ECH raises **significant concerns relating to child safety**;
4. Looking specifically at the finance sector, the introduction of ECH raises significant concerns relating to both **increased opportunities for fraud and greater exposure to cybersecurity risks**;

These concerns may well be mirrored in other sectors, hence additional stakeholder engagement is needed.

[9] ECH is being developed by the TLS (Transport Layer Security) working group within the IETF (Internet Engineering Task Force), see https://datatracker.ietf.org/wg/tls/charter/

4. Recommendations

The above conclusions in turn led to the following recommendations during the roundtable discussion:

1. **Multi-stakeholder engagement** is required to properly understand the full implications of the introduction of ECH as well as the availability and suitability of mitigations.
2. If multi-stakeholder engagement does not lead to a satisfactory outcome for end-users, **regulatory or legislative interventions** may be required to address the significant imbalance of knowledge and power between the technology sector and those end-users in commercial, social and consumer environments.
3. If standards developments like ECH are pushed through that bypass content filtering, software companies such as browser vendors should be required to take steps to protect users from harmful content through the **introduction of effective content filtering** in their software.

These actions are expanded upon in the following section.

5. Next Steps

Multi-Stakeholder Review

It is apparent that discussions relating to the development of ECH within the IETF have largely comprised of individuals working within the technology sector, with representation from a more diverse range of industries largely lacking. Whilst some consideration of the operational impacts of the deployment of ECH took place, the details provided by the IETF working group within RFC 8744 are at best superficial[10]. For example, a total of two paragraphs are devoted to alternatives to using SNI data in the event that it is encrypted, with no reference either to the operational challenges that could be involved[11] or to the effectiveness of the suggested solutions. In addition, no reference is provided to consideration of the non-technical implications of the deployment of ECH.

The participants in the roundtable discussion identified the importance of multi-stakeholder engagement when making significant changes in the way that Internet protocols function. As noted previously in this document, RFC 8890[12], "The Internet is for End Users", written by the IAB (Internet Architecture Board), describes how the IETF can improve its outcomes through such multi-stakeholder engagement. In the context of this topic, consideration should be given to the best means of eliciting true multi-stakeholder input in order to properly understand the real consequences of the introduction of ECH.

The discussion questioned whether stakeholders from outside the technology sector are likely to have the necessary information to engage in the debate. The participants noted that these stakeholders may lack awareness that the debate is happening, may lack the ability to navigate the various pathways into the IETF and other Internet standards bodies and may also lack the bandwidth to sustain a debate against a much better resourced and financed tech sector. These are all issues that would need to be overcome if an effective multi-stakeholder engagement is to take place.

[10] See RFC 8744 sections 2.1 and 2.3, https://datatracker.ietf.org/doc/rfc8744/

[11] Taking into account aspects including the affordability and practicality of solutions as well as the privacy implications of their deployment

[12] See https://www.rfc-editor.org/rfc/rfc8890

The roundtable discussion also noted that any review needs to consider both the operational and policy implications of the deployment of ECH, noting that the IETF typically focuses on the technical effects of its standards. Since a key effect of ECH relates to content filtering, this review needs to include regulators, legislators, browser vendors, the sectors that use content filtering, civil society and others to make sure that an architecture is developed that can reasonably work to support filtering for a wide range of use cases, for example including BYOD.

To be effective, any multi-stakeholder review needs to happen before the ECH standard is finalised and adopted by the IETF so that any outputs of the review are taken into account in the standard. The review could produce updates to sections 2.1 and 2.3 of RFC 8744 or the production of a new document that provides a more insightful view of current usage of SNI information as well as a much more rounded consideration of alternatives.

More generally, learning from the experience of both ECH and DoH (DNS-over-HTTPS)[13], before any new protocol is introduced that is intended to increase privacy through the use of encryption, the impact across the whole ecosystem needs to be understood. The emergence of ECH, largely without the knowledge or input of affected parties, underlines the inadequacy of the current approach and the need for the IETF and associated bodies to significantly improve multi-stakeholder engagement.

Potential Regulatory Intervention

The roundtable participants noted that, in markets where customers are well informed, companies that choose a direction that is not favoured by those customers are likely to lose business. However, this assumes that the customers are knowledgeable whereas visibility of developments like ECH is relatively limited and their potential impact is even less well understood. Noting this, it is neither realistic to expect those users to be able to make informed decisions nor is it likely that suitable alternatives will be readily available in all cases.

In the absence of market pressure from knowledgeable users able to exert sufficient power to influence the development of Internet standards or of software that doesn't cause operational concerns, regulatory interventions may be needed to protect the use cases outlined above. Recent experiences have shown that national regulators are able to exert sufficient pressure on technology companies to cause them to pause and rethink development plans[14].

[13] See RFC 8484, https://datatracker.ietf.org/doc/rfc8744/

[14] See "Google delays Chrome's blocking of tracking cookies to late 2023", https://www.reuters.com/technology/google-delays-chromes-blocking-tracking-cookies-late-2023-2021-06-24/

Given the potential ramifications of ECH on the wider ecosystem, competition authorities should engage in and carefully track the progress of the multi-stakeholder review. This is because changes to, or extensions of, protocols can disrupt markets, to the detriment of some and potentially to the advantage of others including the proponents of those changes. In the case of ECH, companies providing content filtering software would be one example of those that could suffer detriment, with companies operating content delivery networks likely to gain an advantage. If this review does not lead to action to address the concerns of the affected parties, the competition authorities should consider possible interventions into the process of Internet standards development.

Content Filtering

ECH is the latest in a series of standards developments that negate the effectiveness of content filtering software that (i) protects end-users from harm by blocking access to malicious content; (ii) prevents access to specific content, for example in the form of parental controls or to implement enterprise policies; (iii) ensures that enterprise regulatory requirements are met. Prior to ECH, the most recent challenge posed to content filtering software was the introduction of the DNS-over-HTTPS standard.

The combination of DoH and ECH make it increasingly difficult for content filtering solutions to work effectively. Notwithstanding the multi-stakeholder review proposed above, if technology companies are to continue down the path of bypassing content filtering, either deliberately or as an unintended consequence of their actions, they will need to put forward proposals for a viable alternative, if necessary, through the introduction of effective content filtering capabilities in their own software (for example, within operating systems and browsers).

This would clearly have significant implications for those companies that currently provide content filtering solutions, effectively removing them from the market. Competition authorities may take an interest in this aspect to determine whether it raises any antitrust concerns.

Annex: Background Information

A The Encrypted Client Hello (ECH) Standard

A1 Introduction

The proposed ECH standard is being developed within the Internet Engineering Task Force (IETF), specifically its Transport Layer Security (TLS) working group. ECH is a mechanism in TLS version 1.3 or later for encrypting a Client Hello message under a server public key[15].

The main focus of the ECH initiative has been to encrypt the Server Name Indication (SNI) extension in ClientHello messages as part of a wider focus on encryption. SNI data has been utilised in various ways, with some of the applications noted within the IETF's RFC 8744 document[16]. Note that a previous attempt at encrypting the SNI data, called eSNI, has already been implemented by some companies, including Mozilla (within its Firefox browser) and by Cloudflare.

A2 Which Companies are Involved?

Individuals working for, or closely with, a number of technology companies have been involved in the development of ECH, for example Cloudflare, Fastly, Google and Mozilla. However, engagement with or representation from other enterprises and groups of affected users to understand any operational impacts of encrypting SNI data[17] does not appear to have happened to a meaningful extent within the working group. It is probable that a more diverse group of stakeholders would have led to a better understanding of the impacts of the introduction of ECH in different environments.

Section 2.1 of RFC 8744 contained a limited amount of information about different ways that SNI data is currently used. Unfortunately, very little consideration was given in section 2.3 of the same document to the practicalities of the alternatives that it suggests are used in place of SNI-based applications. As noted above, engagement with a broader set of stakeholders would have led to a richer debate and more informed view about these alternatives, including a better understanding of some of the operational considerations, including privacy-related issues. It is probable that a wider stakeholder group would have taken a different stance on financial

[15] See https://tools.ietf.org/html/draft-ietf-tls-esni-10
[16] See section 2.1 of https://datatracker.ietf.org/doc/rfc8744/
[17] As noted above, section 2.1 of RFC 8744 did contain a small amount of information about ways that SNI data is currently used. However only limited consideration was given in section 2.3 of the same document to the practicalities of the alternatives that it suggests could be used in place of SNI-based applications.

considerations, noting that many industries have longer depreciation and replacement timescales than the technology sector.

A3 What are the Timescales for Deployment?

At the time of writing, interoperability testing of various early implementations is about to begin (all of which should be based on the working group's draft -13 specification[18]). If the IETF keeps to its published schedules for developing the ECH specification, it may be live as an early, pre-standard, technology release in consumer products within the next 6-12 months, with the final version of the standard following.

Some browser companies have indicated that they are considering early deployment of ECH in their products, in a manner where it is not possible to switch it off, rather like support for HTTPS has been deployed in the past. For example, this is the path that Google has indicated it is likely to take for its Chrome browser[19].

B Proxy Servers

A proxy server is a server application that acts as an intermediary between a client requesting a resource and the server providing that resource. Instead of connecting directly, the client directs the request to the proxy server which evaluates the request before performing the required network activity. Proxies are used for various purposes including load balancing, privacy and security.

Traditionally, proxies are accessed by configuring a user's application or network settings, with traffic diverted to the proxy rather than the target destination. With "transparent" proxying, the proxy intercepts packets directed to the destination, making it seem as though the request is handled by the target destination itself.

[18] See https://mailarchive.ietf.org/arch/msg/tls/p6-TRdg0Fv-cZLANsFt8us2X3p0/

[19] See https://419.consulting/encrypted-dns/f/proto-typing-encrypted-client-hello-in-the-chrome-browser, from a discussion held on 2nd November 2020

A key advantage of transparent proxies is that they work without requiring the configuration of user devices or software. They are commonly used by organisations to provide content filtering for devices that they don't own that are connected to their networks. For example, some education environments use transparent proxies to implement support for BYOD without needing to load software on third-party devices.

Transparent proxies use SNI data to understand whether a user is accessing inappropriate data. Therefore encryption of the SNI field, as is the case with ECH, will disrupt the use of transparent proxies.