Briefing

Notes From A Roundtable Discussion About Encrypted Client Hello (ECH)

Andrew Campling

4th June 2021

419.Consulting

(This page is intentionally blank)

Notes From A Roundtable Discussion About Encrypted Client Hello (ECH)

1. Foreword

The proposed Encrypted Client Hello (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[1].

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 benign applications noted within the IETF's RFC 8744 document[2].

The following notes were taken during a discussion about ECH. It covered the implications of ECH for sectors such as education and finance, before considering possible mitigations. The discussion was held under the Chatham House Rule[3] and the comments do not necessarily reflect the views of the author.

The notes from the discussion are in italics, complemented by clarifications added post-meeting in the form of footnotes in plain text. The headings have been added to improve readability, with some text highlighted to draw attention to particular issues or conclusions drawn by the participants.

[1] See https://tools.ietf.org/html/draft-ietf-tls-esni-10
[2] See section 2.1 of RFC 8744 at https://datatracker.ietf.org/doc/rfc8744/
[3] See https://www.chathamhouse.org/about-us/chatham-house-rule

2. Introduction

What is ECH?

ECH is the latest IETF initiative to protect SNI data in TLS connections, superseding previous efforts undertaken within the IETF's TLS working group, and is an extension to TLS 1.3. Interoperability testing of various early implementations has just begun (all of which should be based on the working group's draft -10 specification). A number of technology companies have been involved in the work developing ECH, however engagement with or representation from other enterprises and groups of affected users to understand any operational impacts of encrypting SNI data[4] does not appear to have happened to a meaningful extent within the working group.

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.

General Impact

There is an option that is available for devices that are not explicitly configured for a proxy, often referred to as a "transparent proxy[5]". This option is commonly used by organisations to provide content filtering for devices they don't own that are connected to their networks. For example, some education environments use transparent proxies to implement support for BYOD (Bring Your Own Device). Transparent proxies used for filtering commonly use SNI data to understand whether a user is accessing inappropriate data, so encrypting the SNI field will disrupt the use of these transparent proxies.

[4] 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.
[5] See https://nordvpn.com/blog/transparent-proxy/ for an explanation of transparent proxies

Timescales for Deployment

If the IETF keeps to its published schedules for developing the ECH specification, then it may be live as an early technology release in consumer products in 18-24 months[6]. Companies currently active in the development of the ECH standard include Cloudflare, Google and Mozilla. Some browser vendors have indicated that they may deploy ECH in a manner where it is not possible to switch it off, rather like support for HTTPS has been deployed in the past[7].

Early Mitigations

Towards the latter part of 2020, reports indicated that the government of China had implemented measures to block encrypted HTTPS traffic that used TLS 1.3 with eSNI enabled[8]. Whilst it is too soon to know for sure, this could indicate the likely path that the country will take when ECH is deployed at scale[9].

[6] Experimental releases are likely much earlier than this

[7] For example Google in the Chrome browser, see https://419.consulting/encrypted-dns/f/proto-typing-encrypted-client-hello-in-the-chrome-browser

[8] See for example https://www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/

[9] It also illustrates that ECH is not an effective anti-censorship technology

3. Impact on the Education Sector

Initial Views

ECH 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[10]. Schools in England and Wales have obligations to provide "appropriate levels of content filtering", including for BYOD. http://testfiltering.com/ is a simple test that has been developed to test the effectiveness of school filtering solutions in England and Wales – it tries to reach dummy pages that should be blocked if the software is working correctly.

Some providers of content filtering capabilities have indicated that their solutions may be able to function successfully despite recent developments such as encrypted DNS and may also be able to overcome the challenges posed by ECH[11]. Testing will be required to see whether content filtering continues to function despite ECH and there is no guarantee that all providers will be able to identify suitable mitigations. ***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 security and privacy of people using the Internet is important, however measures like ECH are being introduced that will impact the ability to protect children online. It is not clear that dialogue has taken place with affected parties, how can we ensure that we are not taking a step back in our ability to protect children online? What are the potential mitigations, if any, to maintain current levels of protection?

A multistakeholder review is needed to see whether the impacts that developments like ECH could have on child protection are understood by all concerned.

[10] See for example https://blog.mozilla.org/netpolicy/files/2021/06/20210120-204354-0000049-Mozilla-DoH-Response.pdf, pages 2-3

[11] See for example https://blogs.infoblox.com/security/esni-ech-impact-on-content-filtering/

Possible Mitigations

Stop the use of BYOD in schools and other pre-university education establishments, limit software on allowed devices to tightly locked-down applications that either don't support ECH or have the functionality disabled, potentially excluding applications like the Chrome browser. Blocking of BYOD will not typically have a major impact on schooling for 5–18 year-olds, although some establishments will suffer more than others. One exception could be where schools currently encourage the use of their wifi network by phones to ensure that content filtering is applied, rather than being bypassed by the carrier network.

Allowing the network and device to negotiate filtering preferences via IETF standards as part of the network joining process could be one longer-term solution, albeit that this would take several years to achieve. Of course, some IETF participants are opposed to the idea of the IETF supporting filtering, at least at the network level, instead suggesting that such activities are undertaken via enterprise management, but this is far from universal and wouldn't solve the problem of BYOD.

The ADD[12] charter[13] allows for the delivery of information to the client so that it can make decisions. If this information, which is supplied during the DNS discovery process, included details on content filtering then the client could decide whether and how to act on it. This would require discussion and consensus within the working group, followed by suitable implementation proposals.

If the major browser and operating system companies decided that they wanted to support any mechanism for a network to signal that it wanted filtering to be in place then it could be implemented, whether or not it was adopted as a standard[14]. ***To achieve a long-term solution, this issue needs to be taken forward as a multi-stakeholder policy (and possibly regulatory) discussion that includes 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 filtering for a wide range of use cases, for example including BYOD.***

Other Issues

How can those voices that rely on filtering be helped to engage constructively in the debate in the IETF? ***The multi-stakeholder policy discussion ideally needs to happen before the ECH standard is finalised and adopted by the IETF.***

[12] The IETF has created the Adaptive DNS Discovery (ADD) working group to focus on discovery and selection of DNS resolvers by DNS clients in a variety of networking environments.
[13] See https://datatracker.ietf.org/wg/add/about/
[14] A standards-based solution is preferable as this is open and does not rely on ad-hoc support from vendors

4. Impact on the Finance Sector

Initial Views

Filtering is an important tool within the finance sector, with uses including stopping accidental access to malicious content due to phishing etc. In the enterprise market, a number of vendors use transparent proxy solutions, often combined with DNS filtering, to give stronger protections, with the proxy capability requiring unencrypted SNI[15].

BYOD is arguably even more important with the current reliance on working from home, which is another area where the use of transparent proxies can help. Alternative solutions are available but will require the use of more invasive software to be installed onto the guest device. This will also affect and contractors or other third parties that need to connect to an enterprise network.

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. This illustrates privacy-focused protocols can undermine security, at least at the enterprise level. ***Before a new protocol is introduced that is intended to increase privacy, like DoH or ECH, the impact across the whole ecosystem needs to be understood. Any such review will need input from a range of stakeholders if it is to be effective, especially when considering operational and policy impacts, rather than relying exclusively on the views of technology companies.***

Related to the drive to increase privacy, a requirement in the finance sector is the need to have clear audit trails of any communications between parties. If it becomes possible for communications to take place without an audit trail (often a regulatory requirement), or any visibility to the enterprise, then there is increased scope for abuse to take place[16]. For example, in financial markets, if a trader can communicate from the dealing room to a client without a trace then the potential for insider trading or fraud to go undetected rises considerably.

In addition to concerns about the loss of visibility of deliberate activity by users, the loss of visibility of potential command and control and other activity by malicious software is of concern to enterprises. In such cases, the lack of visibility from these privacy protections could lead to negative impacts on security and privacy for the enterprise, its employees or customers.

[15] For example, some software uses SNI to identify which data needs closer analysis and which data can be passed without further examination

[16] Non-compliance with regulatory requirements could have financial or other consequences

Overall, the balance between transparency and privacy is changed by ECH and, by undermining security measures, there are ramifications for the integrity of the operations of enterprises.

Possible Mitigations

ECH is being developed within the IETF's TLS working group as an extension to TLS 1.3. An alternative version of TLS 1.3, called ETS (Enterprise Transport Security), was developed within the ETSI standards body[17]. Can clients supporting ECH function on ETS and are the ECH capabilities affected?[18]

Similarly, whilst large numbers of websites are hosted by large CDN (Content Delivery Network) operators that are likely to upgrade their software to support features such as ECH, there are equally large numbers of websites hosted on small platforms or by themselves that may not support ECH (or even TLS 1.3). Therefore, clients will almost certainly need to work in environments where ECH is not supported for some time to come.

As already discussed, 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.

[17] See https://www.etsi.org/deliver/etsi_ts/103500_103599/10352303/01.02.01_60/ts_10352303v010201p.pdf
[18] Subsequent investigation has suggested that ETS should interoperate correctly with ECH

5. Broader Points

Individual vs Collective Privacy

Privacy and security at the transport layer can simply ensure that personal data is privately and securely delivered to entities that track users and monetise their data, resulting in loss of their privacy and security. This is a consequence of the focus on communications rather than on the end-points; it's a forty-year-old approach that is not fit for today's much more complex world.

Multistakeholder Debate

The level of discussion in this area needs to be raised to shift the focus to the privacy and security of the overall system rather than just considering the network. This needs the different parts of the industry to come together, along with other stakeholders, to have discussions that cover a broader range of matters including operational and policy considerations.

In addition, too many European stakeholders either don't show up to standards bodies or, if they do so, don't engage fully in the debate. This needs to change, with a more assertive approach being taken to ensure that important considerations are both represented and not dismissed out of hand by the mainly US-based technology companies that are well-represented in many of the Internet standards fora.

Whether stakeholders from outside of the technology sector have the necessary information to engage in the debate needs due consideration. For example, 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.

Is this an issue that should be addressed within the IETF using the multi-stakeholder process suggested but not detailed by RFC 8890[19]? How can a broader range of stakeholders be brought into discussions at an early stage, allowing the full ramifications of proposed protocol developments to be considered before any changes are made?

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

Privacy vs Safety

More generally, a better balance needs to be struck between privacy and safety. The IETF and Internet Society are prioritizing privacy, do not appear to be taking into account the potential negative impact that this can have on safety.[20]

Where does filtering happen?

Given an unwillingness to build filters into browsers, operating systems or websites, content filtering solutions have evolved at the network level instead. Whilst there seems to be some resistance to content filtering in the US market, such services are in widespread use elsewhere.

By introducing more pervasive encryption, network-level filtering is more likely to be bypassed, which could refocus attention away from the network and back on to the application/web layer. *Are software companies such as browser vendors prepared for renewed scrutiny on this topic? Will they take steps to protect users from harmful content if their software prevents existing content filtering from working effectively?*

[20] End-to-end encryption can obscure the transmission of child sexual abuse material, causing harm to existing victims and placing additional children in danger.

6. Final Thoughts

Education

One option to mitigate the impact of ECH would be to remove browsers that support the ECH protocol from networks. ***If Google Chrome were removed then this could undermine the significant investment made by Google in Google Classroom, together with associated support into remote learning.*** *The concerns that institutions may have could override the attractions of using the Google Chrome browser, resulting in moves to alternatives (assuming that these exist).*

More Generally

Where it is not possible to remove affected software completely, other options might be to introduce far more intrusive solutions such as full proxies and certificates, including in BYOD environments. The ability to take such steps will depend on the level of control that an organization can exert – this may work with employees, but would not be possible with customers.

The Market

There are many content filtering companies serving the market. They will have to adapt to remain in operation so will have to find innovative solutions to overcome the challenges posed by ECH and other such developments. ***The downside is that such solutions are likely to be significantly more intrusive than those currently in operation and it does depend on those content filtering companies being aware that developments like ECH are on the horizon.***

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 outside of the technology sector is relatively limited and their potential impact is even less well understood. When consideration is extended to the users that may be impacted, it is simply not realistic to expect them to be able to make informed decisions.

In the absence of market pressure from knowledgeable users able to exert sufficient power, regulatory interventions may be needed.

419.Consulting