Workgroup: Secdispatch
Internet-Draft:
draft-campling-ech-deployment-considerations-01
Published: 7 March 2022
Intended Status: Informational
Expires: 8 September 2022

Authors: A.J. Campling
419 Consulting Limited
P. Vixie
Red Barn
D. Wright
UK Safer Internet Centre

Encrypted Client Hello Deployment Considerations

Abstract

This document is intended to inform the development of the proposed Encrypted Client Hello (ECH) standard that encrypts Server Name Indication (SNI) and other data. Data encapsulated by ECH (ie data included in the encrypted ClientHelloInner) is of legitimate interest to on-path security actors including anti-virus software, parental controls and consumer and enterprise firewalls.

The document includes observations on current use cases for SNI data in a variety of contexts. It highlights how the use of that data is important to the operators of private networks and shows how the loss of access to SNI data will cause difficulties in the provision of a range of services to many millions of end-users.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

As noted above, this document includes observations on current use cases for SNI data in a variety of contexts. It highlights how the use of that data is important to the operators of private networks and shows how the loss of access to SNI data will cause difficulties in the provision of a range of services to many millions of end-users.

The Internet was envisaged as a network of networks, each able to determine what data to transmit and receive from their peers. Developments like ECH mark a fundamental change in the architecture of the Internet, allowing opaque paths to be established from endpoints to commercial services, some potentially without the knowledge or permission of the device owners. This change should not be undertaken lightly given both the architectural impact on the Internet and potentially adverse security implications for end users. Given these implications, it certainly should not be undertaken without either the knowledge or consultation of end users, as outlined in RFC 8890 [RFC8890].

NB Whilst it is reasonable to counter that VPNs also establish opaque paths, a primary difference is that the use of a VPN is a deliberate act by the user, rather than a choice made by client software, potentially without either the knowledge and/or consent of the end-user or device owner.

RFC 7258 [RFC7258] discusses the critical need to protect users' privacy when developing IETF specifications and also recognises that making networks unmanageable to mitigate pervasive monitoring is not an acceptable outcome.

RFC 8404 [RFC8404] discusses current security and network operations as well as management practices that may be impacted by the shift to increased use of encryption to help guide protocol development in support of manageable and secure networks. As RFC 8404 notes, "the implications for enterprises that own the data on their networks or that have explicit agreements that permit the monitoring of user traffic are very different from those for service providers who may be accessing content in a way that violates privacy considerations".

This document considers the implications of ECH for private network operators including enterprises and education establishments. The data encapsulated by ECH is of legitimate interest to on-path security actors including anti-virus software, parental controls and consumer and enterprise firewalls. This document will focus specifically on the impact of encrypting the SNI data by ECH on private networks, but it should be noted that other elements will be relevant for some on-path security methods.

2. Encrypted Server Name Indication

RFC 8744 [RFC8744] describes the general problem of encrypting the Server Name Identification (SNI) TLS extension. The document includes a brief description of what it characterises as "unanticipated" usage of SNI information (section 2.1) as well as a brief (two paragraph) assessment of alternative options in the event that the SNI data is encrypted (section 2.3).

The text in RFC 8744 suggests that most of the unanticipated SNI usage "could also be implemented by monitoring DNS traffic or controlling DNS usage", although it does then acknowledge the difficulties posed by encrypted DNS protocols. It asserts, with limited evidence, that "most of [the unanticipated usage] functions can, however, be realized by other means", although without considering or quantifying the affordability, operational complexity, technical capability of affected parties or privacy implications that might be involved. It is unclear from the document whether any stakeholders that may be impacted by the encryption of SNI data have been consulted; it does not appear to be the case.

The characterisation of "unanticipated usage" of SNI data could be taken to imply that such usage was not approved and therefore inappropriate in some manner. The reality is that the development of the Internet has many examples of permissionless innovation and so these should not be dismissed as lacking in importance.

This document is intended to address the above limitations of RFC 8744 by providing more information about the issues posed by the introduction of ECH due to the loss of visibility of SNI data on private networks. To do so it considers the situation within schools and enterprises, building on information previously documented in a report from a roundtable discussion [ECH_Roundtable].

3. The Education Sector

3.1. Context

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 encrypted DNS protocols such as DNS over HTTPS [RFC8484].

Content filtering that leverages SNI information 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 by client software on devices will be problematic and may compromise duties placed on education establishments: for example, schools in the England and Wales have obligations to provide "appropriate filtering systems in place" [KCSE]; schools in the US use Internet filters and implement other measures to protect children from harmful online content as a condition for the receipt of certain federal funding, especially E-rate funds [CIPA].

3.2. Why Content Filtering Matters to Schools

The impact that ineffective content filtering can have on an educational institution should not be underestimated. For example, a coroner in the UK in 2021 ruled that a school's failure to prevent a pupil from accessing harmful material online on its equipment contributed to her taking her own life [Coroner]. In this particular case, the filtering software installed at the school was either faulty or incorrectly configured but it highlights the harmful risks posed if the filtering is bypassed by client software using ECH.

3.3. Mitigations

Whilst it may be possible for schools to overcome some of the issues ECH raises by adopting similar controls to those used by enterprises, it should be noted that most schools have a very different budget for IT compared to enterprises and usually have very limited technical support capabilities. Therefore, even where technical solutions exist that may allow them to continue to meet their compliance obligations, affordability and operational expertise will present them with significant difficulties.

Absent funding and technical expertise, schools will need to consider the best way forward that allows them to remain compliant. If client software does not allow ECH to be disabled, any such software that implements support for ECH may need to be removed from school devices and replaced, assuming that suitable alternatives are available. This will have a negative impact on budgets and maybe operationally challenging if institutions have made a significant investment in the deployment and use of particular applications and technologies.

There are instances where policies in education establishments allow for the use of equipment not owned by the institution, including personal devices and the devices of contractors and site visitors. These devices are unlikely to be configured to use the institution's proxy but can nevertheless connect to the school network using a transparent proxy (see below). Transparent proxies used for filtering will typically 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.

In the event that transparent proxies are no longer effective, institutions will either have to require more invasive software to be installed on third party devices before they can be used along with ensuring they have the capability to comprehend and adequately manage these technologies or will have to prevent those devices from operating. Neither option is desirable.

4. Transparent Proxies

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.

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 content without the need to inspect data beyond the SNI field. Because of this, encryption of the SNI field, as is the case with ECH, will disrupt the use of transparent proxies.

5. Enterprises

Filtering is an important tool within many enterprises, with uses including the prevention of 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 information. BYOD is arguably even more important with the current reliance on remote working, 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.

Any restrictions on the use of BYOD will also affect contractors and other third parties that need to connect to one or more enterprise networks on a temporary basis. In such circumstances, requiring software or custom configurations to be installed on those devices may be problematic, especially for contractors that work across multiple organisations. One solution could be for dedicated equipment for each client, however this will have potentially significant cost considerations.

Clear audit trails of any communications between parties are required in the finance sector amongst others for compliance purposes. If it becomes possible for communications to take place without an audit trail or any visibility to the enterprise, then there is increased scope for abuse to take place, including insider trading or fraud.

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, suppliers and customers.

When considering the operational and cost implications for enterprises, it should be remembered that the resources available will vary significantly between a multinational organisation and a small to medium-sized enterprise. It should not be assumed that a solution that can be absorbed financially and operationally by the former is practical for the latter. The needs of both need to be taken into account when evaluating potential solutions.

6. Threat Detection

[To be completed, additional input welcome]

RFC 8404 identifies a number of issues arising from increased encryption of data, some of which apply to ECH. For example, it notes that an early trigger for DDoS mitigation involves distinguishing attacker traffic from legitimate user traffic.; this become more difficult if traffic sources are obscured.

The various indicators of compromise (IoCs) are documented in draft-ietf-opsec-indicators-of-compromise-00, which also describes how they are used effectively in cyber defence. For example, section 4.1.1 of the document describes the importance of IoCs as part of a defence-in-depth strategy; in this context, SNI is just one of the range of indicators that can be used to build up a resilient defence (see section 3.1 in the same document on IoC types and the 'pyramid of pain').

In the same Internet-Draft, section 6.1 expands on the importance of the defence in depth strategy. In particular, it explains the role that domains and IP addresses can play, especially where end-point defences are compromised or ineffective, or where endpoint security isn't possible, such as in BYOD, IoT and legacy environments. SNI data plays a role here, in particular where DNS data is unavailable because it has been encrypted; if SNI data is lost too, alongside DNS, defences are weakened and the attack surface increased.

7. Mitigations

Access to SNI data is sometimes necessary in order for institutions, including those in the education and finance sectors, to discharge their compliance obligations. The introduction of ECH in client software poses operational challenges that could be overcome on devices owned by those institutions if policy settings are supported within the software that allows the ECH functionality to be disabled.

Third-party devices pose an additional challenge, primarily because the use of ECH will render transparent proxies inoperable. The most likely solution is that institutions will require the installation of full proxies and certificates on those devices before they are allowed to be connected to the host networks. They may alternatively determine that such an approach is impractical and instead withdraw the ability for network access by third-party devices.

An additional option that warrants further consideration is the development of a standard that allows a network to declare its policy regarding ECH and other such developments. Clients would then have the option to continue in setting up a connection if they are happy to accept those policies, or to disconnect and try alternative network options if not. Such a standard is outside of the scope of this document but may provide a mechanism that allows the interests and preferences of client software, end-users and network operators to be balanced.

8. Security Considerations

In addition to introducing new operational and financial issues, the introduction of SNI encryption poses new challenges for threat detection which this document outlines. These do not appear to have been considered within either RFC 8744 or the current ECH Internet-Draft [draft-ietf-tls-esni-14] and should be addressed fully within the latter's security considerations section.

9. Acknowledgements

In addition to the authors, this document is the product of an informal group of experts including the following people:

10. Informative References

[CIPA] FCC, "Children's Internet Protection Act (CIPA)", 30 December 2019, <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act/>.

[Coroner] Henderson, "Prevention of future deaths report", 26 November 2021, <https://www.judiciary.uk/publications/frances-thomas-prevention-of-future-deaths-report/>.

[ECH_Roundtable] 419 Consulting, "Encrypted Client Hello - Notes from an ECH Roundtable", 18 August 2021, <https://419.consulting/encrypted-client-hello/>.

[KCSE] DfE, "Keeping children safe in education 2021", 1 September 2021, <https://419.consulting/encrypted-client-hello/>.

[RFC7258]
Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

[RFC8404] Moriarty, K., Ed. and A. Morton, Ed., "Effects of Pervasive Encryption on Operators", RFC 8404, DOI 10.17487/RFC8404, July 2018, <https://www.rfc-editor.org/info/rfc8404>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC8744] Huitema, C., "Issues and Requirements for Server Name Identification (SNI) Encryption in TLS", RFC 8744, DOI 10.17487/RFC8744, July 2020, <https://www.rfc-editor.org/info/rfc8744>.

[RFC8890] Nottingham, M., "The Internet is for End Users", RFC 8890, DOI 10.17487/RFC8890, August 2020, <https://www.rfc-editor.org/info/rfc8890>.

Authors' Addresses

Andrew J Campling
419 Consulting Limited

Email: Andrew.Campling@419.Consulting
URI: https://www.419.Consulting/

Paul Vixie
Red Barn

Email: paul@redbarn.org
URI: http://www.redbarn.org/

David Wright
UK Safer Internet Centre

Email: david.wright@swgfl.org.uk
URI: https://saferinternet.org.uk/