CS7NS5 Security and Privacy
AS1 Security and privacy considerations

Ted Johnson
School of Computer Science and Statistics
Trinity College Dublin

19 April 2024

Introduction

In this report, I present the security and privacy considerations I have made within my dissertation. I first include a short description of my research question, followed by its contributions to the fields of security and privacy. An outline of the security and privacy aspects of relevant background work is then given. The security and privacy challenges that influence the design of my solution are provided as well as the steps taken to address them. Finally, I discuss various security and privacy implications of the design which may impact its users and service operators.

Project overview

The title of my research topic is "A distributed deployment model for Encrypted Client Hello". Encrypted Client Hello (ECH) is a proposed extension to the Transport Layer Security protocol version 1.3 (TLS 1.3) which has begun to see implementation and adoption on the Internet [1, 2]. ECH seeks to allow encryption of the ClientHello message, which can contain potentially sensitive information such as the Service Name Indication (SNI) and Application-Layer Protocol Negotiation (ALPN) extensions. This is partially achieved through serving many private domains behind a common ECH-service provider to form an anonymity set that conceals the true domain requested by the client.

Mark Nottingham has previously cautioned against the introduction of centralisation through Internet standards [3]. Of particular relevance to ECH is his highlight of the adverse effect centralisation can have on infrastructure resilience and service availability through reliance on a single entity. This is especially detrimental to ECH where the effectiveness of its anonymity set grows with the number of private domains served by a single ECH-service provider. Nottingham also writes on susceptibility of centralisation to stifle "permissionless" innovation and

induce an unhealthy monoculture which may result in less overall technological progress and robustness of the ECH protocol.

Additionally, allowing entirely independent servers to co-operate from across the Internet to provide ECH support for each other enables several distinct organisations and entities to work together to offer improved user privacy for all without the requirement for co-located servers nor the dependence of any on the availability on another. Consider here global networks of whistleblower services, investigative journalists and human rights non-profit organisations who share an interest in protecting the confidentiality of their members and users from persecution and retaliation.

For these reasons, my research work has been on identifying and evaluating practical models for deployment of ECH amongst several co-operating TLS servers, where each server operates both as the origin server of its own domains as well as an ECH provider for other participating servers. The model must address a number of implementation challenges, predominately related to ensuring the security of the protocol is not compromised and minimising the performance impact to the connection while strengthening service availability.

Background security and privacy aspects

the security and privacy aspects present within the background work to my research. We will TODO

TODO background security aspects: - tlsv1.3 extensions - dns over https - ech with hpke

TODO The provider first generates an public and private ECH encryption key pair and some associated metadata. This public key and metadata, referred to as an ECH configuration or ECHConfig, may then be shared out-of-band to ECH-enabled clients though secure means like DNS over HTTPS. A client may then use this to construct a ClientHello message, named the ClientHelloOuter, holding unremarkable values for the provider along side an encrypted ClientHello, named the ClientHelloInner, itself holding the real values for a private domain. To establish a TLS connection to the origin server of this domain, the client sends the ClientHelloOuter to the provider, which decrypts and relays the contained ClientHelloInner to the origin server, which itself completes the TLS handshake with the client through the provider. The protocol supports two modes of operation named “Shared Mode” and “Split Mode”.

Design considerations

TODO design considerations, primary threat model is survalience and correlation - dns enables co-operation, may not require it: still tls, dns allows for retrying (availability) - echconfig sharing is bad: use https rr to have distinct ech keys between hosts - side channel traffic correlation (pervasive monitoring, ml): backend comms encryption and padding (DoS)

Further discussion

TODO - dns records show which servers are working together + co-operation requires confidentiality: tls servers can see which user goes where - tls servers have larger attack surface: both front-end and back-end interface - know client is using ech (greasing, colleagues working on hidden ech)

Summary

This report has illuminated a number of security and privacy considerations relevant to the background and design of my research project on distributed deployment of ECH. We have seen how the security properties of ECH are coupled with those of TLS 1.3 and DoH to deliver protection of potentially sensitive client information such as the SNI and the ALPN list. An overview of the security and privacy challenges associated with the project which motivated the design of the solution was provided, namely not compromising service availability, avoiding widely shared secrets, and distrusting traffic correlation attacks. Finally, a discussion on the impacts to the security and privacy of the users and service operators of the solution was given, including the assumption of amity among co-operating TLS servers, acknowledgment of an increased attack surface for co-operating TLS servers, and recognition that usage of ECH is currently easily detectable.

References

[1] Zisis Tsiatsikas, Georgios Karopoulos, and Georgios Kambourakis. "Measuring the adoption of TLS encrypted client hello extension and its forebear in the wild". In: *European Symposium on Research in Computer Security*. Springer. 2022, pp. 177–190.

[2] Christopher Wood Achiel van der Mandele Alessandro Ghedini and Rushil Mehra. *Encrypted Client Hello - the last puzzle piece to privacy*. Sept. 2023. URL: https://web.archive.org/web/20240324023814/https://blog.cloudflare.com/announcing-encrypted-client-hello (visited on 03/24/2024).

[3] Mark Nottingham. *Centralization, Decentralization, and Internet Standards*. RFC 9518. Dec. 2023. DOI: 10.17487/RFC9518. URL: https://www.rfc-editor.org/info/rfc9518.