Encrypted Client Hello Deployment Considerations

Andrew Campling Andrew.Campling@419.Consulting

Arnaud Taddei Arnaud.Taddei@broadcom.com

Simon Edwards Simon.Edwards@broadcom.com

Paul Vixie Paul@Redbarn.Org

David Wright David.Wright@SWGfL.Org.UK

Context

- Encrypted Client Hello (ECH) is “a mechanism in Transport Layer Security (TLS) for encrypting a ClientHello message under a server public key”
- Builds on the previous Encrypted Server Name Indication (eSNI) proposal
- Being developed within the IETF’s TLS working group
- See https://datatracker.ietf.org/doc/draft-ietf-tls-esni/ for the latest version (currently draft -15)

What is the Issue?

- RFC 7258: discusses the critical need to protect users’ privacy when developing IETF specifications, 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.

  > “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…”

- The data encapsulated by ECH is of legitimate interest to on-path security actors including anti-virus software, parental controls [and other content filtering] and consumer and enterprise firewalls.

RFC 8744 – “Issues and Requirements for Server Name Identification (SNI) Encryption in TLS”

- Includes a brief description of what it characterises as "unanticipated" usage of SNI information (section 2.1)
- A brief (two paragraph) assessment of alternative options in the event that the SNI data is encrypted (section 2.3)
- Asserts, with limited evidence, that "most of [the unanticipated usage] functions can, however, be realized by other means“
- Does not consider or quantify the affordability, operational complexity or technical capability of affected parties or the privacy implications that might be involved

If This Interests You….

- Draft currently in development that documents the operational impact of ECH for various use cases
  - https://datatracker.ietf.org/doc/draft-campling-ech-deployment-considerations/
  - To be updated with an -03 version shortly
- Side meeting tomorrow evening to discuss this further
  - When: Monday 7th December, 19:00-20:00 UTC
  - In-Person: Richmond 6
  - Remote: https://us02web.zoom.us/j/84216816172?pwd=R0Y5NHEwenNYTjZmUWJnL29lSE5LUT09&from=addon

Thank You

Andrew.Campling@419.Consulting