Encrypted Client Hello Deployment Considerations

draft-campling-ech-deployment-considerations-01

IETF 113 Vienna

Andrew Campling Andrew.Campling@419.Consulting
Paul Vixie Paul@Redbarn.Org
David Wright David.Wright@SWGfL.Org.UK

Introduction

- Input from multiple multiple stakeholders with an understanding of end user impacts
- Knowledge of current end user requirements will aid the development of better solutions
- Development of protocols and extensions should work with minimal disruption to the end user experience wherever possible
- Where disruption is deemed to be necessary, effort should be made to validate this via multistakeholder engagement to understand end user priorities

Background

- 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 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 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

User Impacts

Education

- Schools, for example in the US and UK, are required to operate content filtering, make use SNI data
- Enterprise-grade solutions may be beyond their financial or operational capabilities
- Alternative options include
  1) Disabling ECH in client software (where possible) or removing that software
  2) Abandoning BYOD

  Both options will be disruptive, the first has potentially significant cost implications

Enterprises

- SNI aids content filtering in enterprises, including to block access to malicious content via phishing, may also help with compliance requirements
- BYOD is often implemented using transparent proxies, alternatives are generally more complex and more invasive of user privacy
- Loss of visibility of SNI data weakens cyber defences
- Small enterprises lack the financial and operational capabilities of multinationals

Threat Detection & Security Considerations

Threat Detection

- RFC 8404 identifies a number of issues arising from increased encryption of data, some of which apply to ECH
- Draft-ietf-opsec-indicators-of-compromise-00 documents various indicators of compromise, 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

Security Considerations

- The introduction of SNI encryption poses new challenges for threat detection
- These are not 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

Summary: Unintended Consequences for Users and Device Dwners

Desired Effect

Communication with target takes place without observation or interference

Actual Effect

Communication with malicious content
Surveillance by client software
Access to age-inappropriate content
Access to CSAM

NB Better tools exist for “dissidents”, eg Tor etc

Conclusions

- This paper identifies new end-user harms are valid and that have not been fully investigated
- The introduction of SNI encryption also poses new challenges for threat detection, risks harming end user security
- Amongst other points, RFC 8890 states that it is not good practice to avoid identifying harms, nor is it acceptable to ignore them when brought to the IETF's attention