Encrypted Client Hello

DNS-OARC Briefing

Andrew Campling
Andrew.Campling@419.Consulting

419.Consulting

Agenda

- Standards Development Organisations
- Culture, Privacy and the Internet Engineering Task Force
- Some Recent Internet Standard Developments
- Encrypted Client Hello
  - Background
  - Current Status
  - Implications for Network Operators, Enterprises and others
- Next Steps

Standards Development Organisations

A number of standards bodies have oversight over various Internet and related functions. A non-exhustive list of examples includes:

- IGF – Internet Governance Forum
- ICANN - Internet Corporation for Assigned Names and Numbers
- IETF – the Internet Engineering Task Force
- IRTF – Internet Research Task Force
- W3C – the World Wide Web Consortium
- ITU-T - Technical committee of the International Telecommunications Union

The culture, structure and “membership” of the above organisations varies enormously.

Culture, Privacy and the Internet Engineering Task Force

- Participation in the IETF is by individuals not organisations or their representatives

- Libertarian Perspective
  - RFC 2804: IETF Policy on Wiretapping

- The Snowden Revelations
  - RFC 7258 - Pervasive Monitoring Is an Attack
  - Reflections on Ten Years Past The Snowden Revelations

419.Consulting

Some Recent Internet Standard Developments

- Transport Layer Security – TLS 1.3

  "In contrast to TLS 1.2, TLS 1.3 provides additional privacy for data exchanges by encrypting more of the negotiation handshake to protect it from eavesdroppers. This enhancement helps protect the identities of the participants and impede traffic analysis. TLS 1.3 also enables forward secrecy by default which means that the compromise of long term secrets used in the protocol does not allow the decryption of data communicated while those long term secrets were in use. As a result, current communications will remain secure even if future communications are compromised."

- Encrypted DNS - eg DNS-over-HTTPS

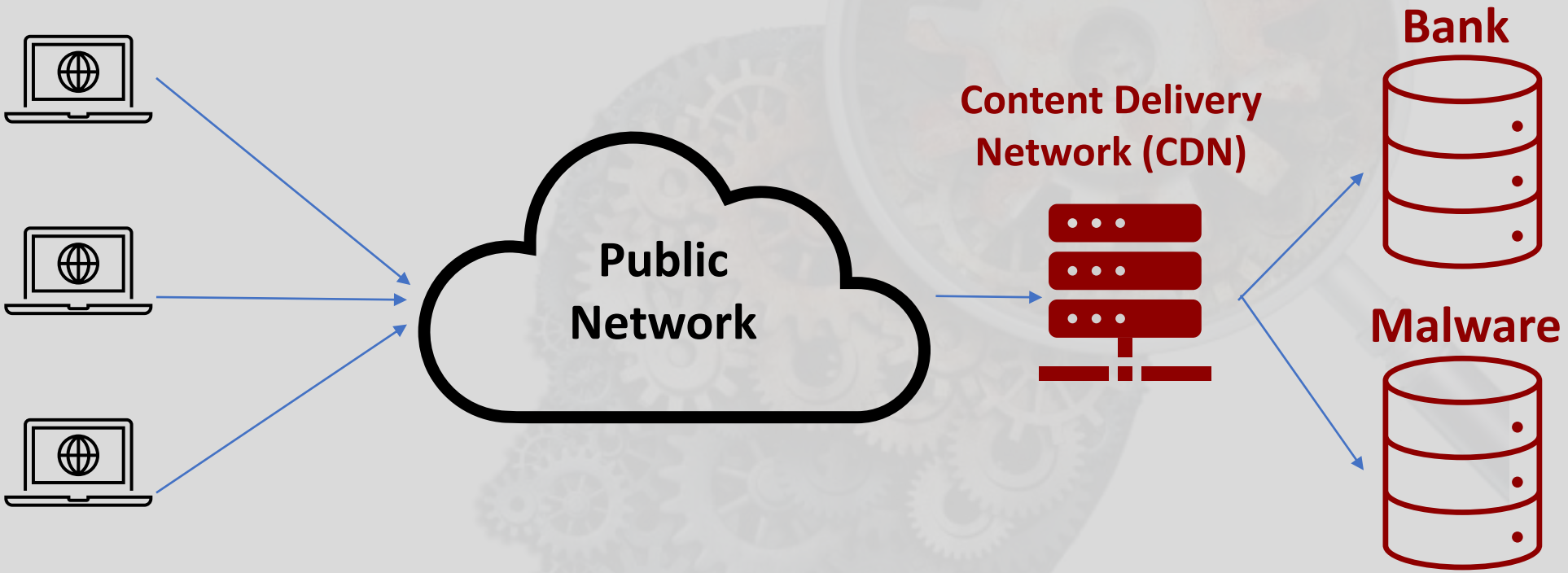
  "Two primary use cases were considered during this protocol's development. These use cases are preventing on-path devices from interfering with DNS operations, and also allowing web applications to access DNS information via existing browser APIs in a safe way"

419.Consulting

Encrypted Client Hello: Background

- The plaintext Server Name Indication (SNI) extension in ClientHello messages, which leaks the target domain for a given connection, is *"perhaps the most sensitive, unencrypted information in TLS 1.3"*
- A new TLS extension, called Encrypted Client Hello (ECH), is under development within the IETF's TLS working group
- ECH allows clients to encrypt their ClientHello when communicating with compliant servers, protecting the SNI and other potentially sensitive data fields, such as the ALPN (Application-Layer Protocol Negotiation) list

Encrypted Client Hello: Background



419.Consulting

Encrypted Client Hello: Background

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

Encrypted Client Hello: Current Status

- Originally efforts within the IETF's TLS working group focused on encrypting the SNI data ("eSNI")
- This evolved into the more comprehensive Encrypted Client Hello (ECH), with interoperability testing and some pre-standard deployments already underway
- The latest draft is accessible at https://datatracker.ietf.org/doc/draft-ietf-tls-esni/
- ECH to become an Internet standard by the end of 2024 / early 2025?

Implications for Network Operators and others

Desired Effect

- Communication with target takes place without observation or interference

Actual Effect

- Content filtering / firewalls bypassed, access policies ignored
- Compliance requirements bypassed
- Unable to differentiate applications using ECH from malware etc
- Potential communication with malicious content
- Potentially undetectable user surveillance and/or data exfiltration by client software
- Access to CSAM, age-inappropriate content etc (eg in schools)

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

419.Consulting

Implications for Network Operators and others

Enterprises

- SNI aids content filtering in enterprises, including to block access to malicious content via phishing, can also help with compliance requirements in regulated sectors
- BYOD is often implemented using transparent proxies, these rely on SNI; alternatives are generally more complex to implement and more invasive of user privacy
- Loss of visibility of SNI data weakens cyber defences as it is used by firewalls as a key indicator of compromise
- Small enterprises generally lack the financial and operational capabilities of multinationals to understand and address these issues

Education

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

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

Implications for Network Operators and others

Public Networks

- Impact to traffic management / steering to fixed and mobile networks - i.e. CDN steering
- Traffic optimisation across mobile radio networks
  - Potential impact to performance and efficiency
  - Quality of Service steering
- Engineering / capacity management becomes more difficult
- Operational support / incident management becomes more challenging
  - Increased complexity
  - Limited monitoring

Implications for Network Operators and others

Public Networks

- Zero rating of content no longer possible, a feature that often benefits the least affluent users
  - Important for fixed and mobile network users with data caps
  - Allows access to, for example, health-related content without impacting on the data cap
  - ECH may cause metering to operate without warning
- Traffic classification for consumers is significantly challenged and will need to change
  - Potential impact to value-added services for parental controls, security etc
- Enterprise network protection services – reduced visibility
  - Blocking websites based on content categories: HR policy on acceptable use policy for Internet usage potentially can't be enforced. For example, adult / violence categorised sites can't be blocked for the users accessing the Internet.
  - Protecting corporate users from web-based threats: By inspecting web traffic, the majority of web based malicious code would normally be monitored and blocked before they reach the user's systems.
  - Disruption of cybersecurity controls / content filters policies

Implications for Network Operators and others

Public Networks

- Legal requirements by regulators and law enforcement agencies
  - May circumvent CSAM blocking
  - Life at risk incidents may be impacted due to reduced / lack of information
  - Disclosure of evidence for courts may be impacted
  - Legal / policy framework may need change

ECH: Next Steps

- Audit internal systems and customer offerings to understand where loss of visibility of SNI data will have an adverse effect

- Engage with security vendors to gauge the latters' knowledge of, and plans for, ECH and validate whether this is sufficient to meet any on-going security and compliance requirements

- Engage with regulators, legislators and others to reduce non-compliance risks
  - Regulatory activity to minimize the potentially negative effects of ECH on security and safety may be necessary

419.Consulting

ECH: Next Steps

- Consider contributing to the text of our informational draft "Encrypted Client Hello Deployment Considerations" – see https://datatracker.ietf.org/doc/draft-campling-ech-deployment-considerations/

- More generally, engage with the IETF so that Internet standards development reflects the needs of a broad range of stakeholders and is built on an understanding of real-world impacts

419.Consulting

Questions?

Don’t forget to join our weekly DNS call, sponsored by DNS-OARC, Mondays at 16:00 UK (currently 15:00 UTC)

Encrypted Client Hello

DNS-OARC Briefing

Andrew Campling
Andrew.Campling@419.Consulting

419.Consulting