Encrypted Client Hello and Network Operators

OARC 44

Andrew Campling, Paul Vixie, David Wright, Arnaud Taddei, Simon Edwards

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

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 for Operators & Others

- 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

ECH: Next Steps for Operators & Others

- 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

ECH: Current Status

- Standard
  - *Draft has completed Working Group Last Call*
  - *Authors responding to Area Director Review*
  - *Has yet to be submitted to the IESG*

- *Client Software*
  - *Implemented by Chrome, Firefox, BoringSSL*
  - *Can be disabled on managed Chrome devices*

- *Server Side*
  - *Implemented by Cloudflare**
  - *Configurable on paid-for tiers, enabled but not configurable on free tiers*

ECH: Current Status

November 07, 2024

We recommend that you cancel the CloudFlare CDN service

In October, the American company CloudFlare, a provider of CDN services, enabled the TLS ECH (Encrypted Client Hello) extension on its servers by default. This technology is a means of bypassing restrictions on access to information banned in Russia. Its use violates Russian law and is limited to technical means of countering threats (TSPU).

We recommend that owners of information resources disable the TLS ECH extension or, more correctly, use domestic CDN services that provide reliable and secure functioning of resources and protection against computer attacks.

In particular, the National System for Countering DDoS Attacks (NSA) can provide protection against DDoS attacks. Since its operation (since March 2024), more than 10.5 thousand DDoS attacks on various organizations in the country have been repelled.

Please note that CloudFlare was one of the BigTech companies that the US State Department convened in September to discuss a comprehensive and organized counteraction to countries that actively defend their information sovereignty (source).

ECH: Current Status

Daryna Antoniuk

November 8th, 2024

Russia's internet watchdog blocks thousands of websites that use Cloudflare's privacy service

Russia's media censor, Roskomnadzor, has blocked thousands of local websites that use an encryption feature from the U.S. company Cloudflare, designed to improve privacy and security for internet users.

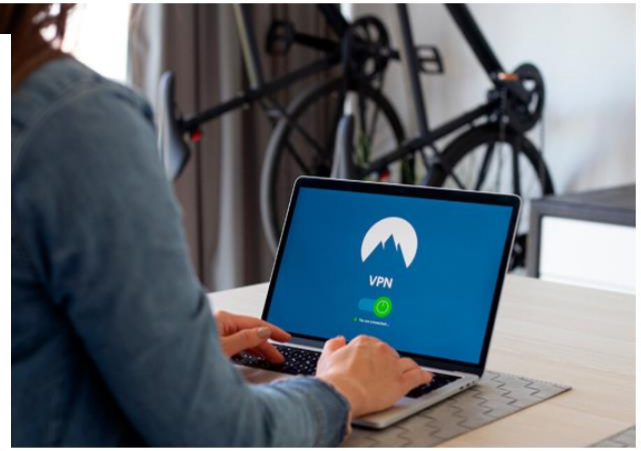
According to local media reports, the websites were blocked overnight on Oct. 6. All of them use Cloudflare's security feature called Encrypted Client Hello (ECH), which protects user information during the initial stages of a secure connection. ECH makes it more difficult for third parties to track which sites users are visiting.

In a statement on Thursday, Roskomnadzor urged Russian website owners to stop using Cloudflare's Content Delivery Network (CDN) service, as the company recently enabled the default use of the ECH extension.

Roskomnadzor blocked thousands of websites using ECH encryption overnight

The Insider

6 November 2024 06:44



night of November 6, Roskomnadzor blocked all sites using Encrypted Client ECH) encryption. This was reported by resources such as Habr and VC.ru.

th ago, the largest cloud provider Cloudflare for the second time enabled tion technology for its customers, which allows you to bypass blocking. ECH logy hides the domain of the site to which the user connects from the provider. se of this, some of the blocked sites became available to Russians.

hat, Roskomnadzor began mass blocking of sites using ECH technology.

ding to users, the number of blocked sites is already in the thousands, the er of complaints is only multiplying.

ECH: Further Information

- The latest draft is accessible at https://datatracker.ietf.org/doc/draft-ietf-tls-esni/
- Encrypted Client Hello (ECH) and Its Impact on Privacy - https://medium.com/@kyodo-tech/encrypted-client-hello-ech-and-its-impact-on-privacy-08acbdd80a22
- Statement from Roskomnadzor, Russia's media censor – here
- Recorded Future briefing - https://therecord.media/russia-blocks-thousands-of-websites-that-use-cloudflare-service
- Cloudflare with the ECH again - https://blog.trnck.dev/cloudflare-with-ech-again/

Questions?

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

Encrypted Client Hello and Network Operators

OARC 44 Briefing

Andrew Campling, Paul Vixie, David Wright,
Arnaud Taddei, Simon Edwards

Andrew.Campling@419.Consulting