

Encrypted Client Hello Deployment

Considerations on Encrypting TLS Server Name Indication

Paul Vixie, RITE 2026

Russia wants to ban the use of secure protocols x +

zdnnet.com/article/russia-wants-to-ban-the-use-of-secure-protocols-suc... | 40

EDITION: US ▼

ZDNet 🔍

IOT CLOUD AI SECURITY MORE ▼ NEWSLETTERS ALL WRITERS

📖 MUST READ: Contact tracing: New NHS COVID-19 app launches in England and Wales

Russia wants to ban the use of secure protocols such as TLS 1.3, DoH, DoT, ESNI

Amendment to IT law would make it illegal to use encryption protocols that fully hide the traffic's destination.

🗨️ in 📺 f 🐦 ✉️

By  Catalin Cimpanu for Zero Day | September 22, 2020 -- 12:33 GMT (05:33 PDT) | Topic: Security

MORE FROM CATALIN CIMPANU

 Security
Polish police shut down hacker super-group involved in

Timeline

- 2013 Edward Snowden flies to Hong Kong, then to Russia
- 2014 RFC7258 *Pervasive Monitoring Is an Attack*
- 2016 RFC7858 *DNS over Transport Layer Security (TLS)*
- 2018 RFC8446 *Transport Layer Security 1.3 (ECH)*
- 2018 RFC8484 *DNS Queries over HTTPS (DoH)*
- 2020 RFC8890 *The Internet is for End Users*
- 2021 RFC9000 *A UDP-Based Multiplexed and Secure Transport*

On TLS Itself

- TLS is how almost all encryption is done on Internet traffic
 - HTTPS, SMTPS, QUIC
- TLS sessions begin with a Client Hello message
 - Includes Server Name Indicator (SNI)
- After startup, client and server behave as without TLS
 - Requests, responses, errors, etc.
- Role of TLS is to make protocol private vs. on-path actors
 - Historically, Client Hello was not considered private

Who Are The On-Path Actors?

- Could be parental or school controls in the WiFi gateway
 - Perhaps to enforce no-porn or similar rules
- Could be corporate controls in the Internet gateway
 - Protect against malware, tunnels, or botnets
 - Enforce local law (like allowing online banking)
 - Support compliance or cyber-insurance goals
- Could be a hotel, coffee shop, or ISP
- Could be an authoritarian national government
- Could be the maker of a device, app, or browser

Encrypting Client Hello

- In TLS 1.3 it is possible to encrypt the Client Hello message
- Either endpoint can insist on this, to assure end to end privacy
- This disintermediates all on-path actors, no matter good or evil
- To restore pre-ECH visibility requires an explicit outbound proxy
 - This exposes all content not just Client Hello to inspection
 - That's against national law in some places
 - Gateway operators have no likeable choices

What Else is Coming?

- TLS 1.3 with ECH is the minimum requirement for QUIC
- QUIC (on UDP/IP) is expected to broadly replace TCP/IP
- QUIC is not observable by operating system kernels
- This means network operator visibility will further decline
- Which means, all policy will be in the endpoints

Fini

For later discussion if desired:

paul@redbarn.org