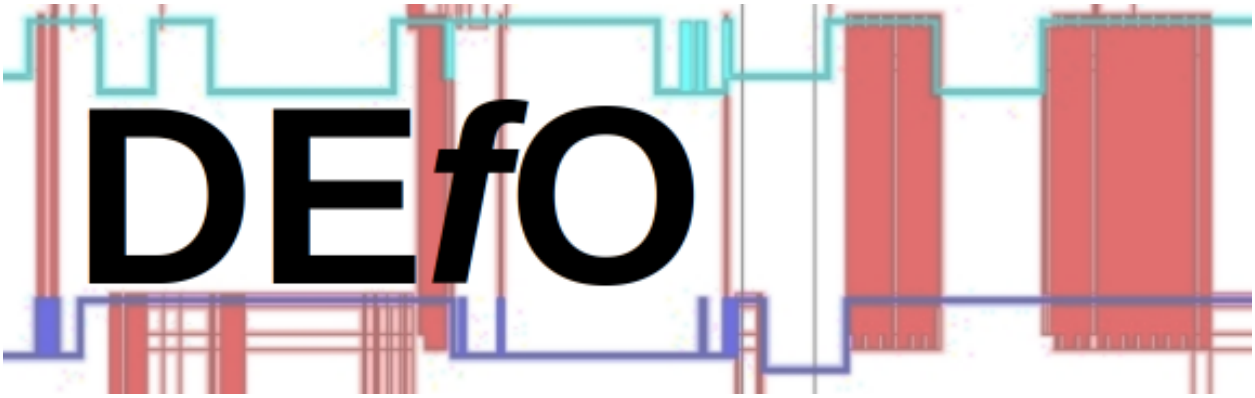

ECH Interoperability Report

Stephen Farrell

Trinity College Dublin/Tolerant Networks Ltd.

stephen.farrell@cs.tcd.ie

work-in-progress

Abstract

The abstract.

Index Terms

Encrypted Client Hello (ECH), Interoperability

I. Introduction

Deployments of the Transport Layer Security (TLS [**?**]) protocol expose the name of the server (e.g. the web site DNS name) via the Server Name Indication (SNI) field in the first message sent (the ClientHello). The Encrypted Client Hello (ECH) [1] extension to TLS is a privacy-enhancing scheme that aims to address this leak.

This report describes the current state of ECH interoperability.

Stephen Farrell is with Trinity College, Dublin 2, Ireland (email: stephen.farrell@cs.tcd.ie, https://www.cs.tcd.ie/Stephen.Farrell/)

ACKNOWLEDGEMENTS

Thanks to DEfO folks, OTF...

REFERENCES

[1] E. Rescorla, K. Oku, N. Sullivan, and C. A. Wood, “TLS Encrypted Client Hello,” Internet Engineering Task Force, Internet-Draft draft-ietf-tls-esni-22, Sep. 2024, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-esni/22/