A distributed deployment model for Encrypted Client Hello

Ted Johnson, Master in Computer Science
University of Dublin, Trinity College, 2024

Supervisor: Dr Stephen Farrell

Encrypted Client Hello (ECH) is a proposed extension to the Transport Layer Security (TLS) protocol that encrypts information currently leaked during connection, which is now beginning to see implementation and adoption on the Internet. However, typical deployment strategies encourage placing many TLS servers behind a single ECH-service provider to form an anonymity set, which introduces significant network centralisation and limits the types of environments the extension can be operated in.

This report presents a method for distributing the deployment of ECH amongst a loose network of co-operating TLS servers, such that each server functions as an ECH-service provider for all others. This allows for ECH-enabled clients to access services through any co-operating TLS server, greatly strengthening service availability and network flexibility. The effectiveness of this solution is evaluated based on its privacy and security implications, impact to overall network performance and ability to fairly allocate load between participating servers over time.