TLS Encrypted Client Certificates

Wan-Teh Chang
IETF 82, 2011-11-17

Introduction

Designer: Adam Langley, Google

Problem: sending client certificates in the clear has privacy concerns.

Solution: a method to send client certificates, encrypted, without resorting to renegotiation

Status: implemented for NSS and OpenSSL

TLS encrypted client certificates extension

Extension type *encrypted_client_certificates* (empty *extension_data*)

Without encrypted client certificates:

Certificate
ClientKeyExchange
CertificateVerify
[ChangeCipherSpec]
Finished

With encrypted client certificates:

ClientKeyExchange
[ChangeCipherSpec]
Certificate
CertificateVerify
Finished

Issues

Incompatible with DH or ECDH certificates (rarely used in practice)

Vulnerable to downgrade attacks if the client does not strictly requires the extension

Requires sending handshake messages between ChangeCipherSpec and Finished