IETF Hackathon
HTTP Transport Authentication

IETF 113
19-20 March 2022
Vienna, Austria

Hackathon Plan

- Dust off and complete a dormant implementation of HTTP Transport Authentication for Google Conscrypt (TLS for Java/Android)
  - draft-schinazi-httpbis-transport-auth-05
- How?
  - Migrate early implementation to Conscrypt & verify
  - Document and open source it

For Reference

- Why HTTP Transport Authentication?
  - Authenticate connection for traffic that is not HTTP request/response (CONNECT)
    - Modern use cases (incl HTTP/3, WebTransport, MASQUE)
  - Authenticate TLS session without leaking user information in ClientHello
    - Authentication scheme options supporting range of use cases
  - Runs alongside standard HTTP services in web server
- How?
  - Utilizes key material derived from TLS connection establishment to symmetrically-encrypt an authentication token presented on the HTTP CONNECT request (via a new HTTP header)
  - Success case returns standard 200 HTTP Connection Established
  - Failure case returns standard 405 Method Not Allowed

What got done

- Objective Achieved!
  - Implemented PoC in Conscrypt/Java
  - Mapped out how to implement in Python, Cronet
  - Looking for inter-op partner
  - Did not implement full proxy flow (yet)
- SEE: https://github.com/guardianproject/conscrypt/tree/MASQUE

What we learned

- Language support for keying materials export
  - Languages implementing OpenSSL/BoringSSL
    - e.g. Conscrypt/Java, Cronet
  - Python via PyOpenSSL library
    - Python has an open issue relative to native language support
  - Go
  - rust (rustls)
  - Microsoft TLS library
  - Mozilla NSS

Wrap Up

Team members:

Hans-Christoph Steiner
hans@guardianproject.info
David Oliver
david@guardianproject.info

https://guardianproject.info
Draft
repo