HTTP Transport Authentication

draft-schinazi-httpbis-transport-auth

IETF 114 – Philadelphia – 2022-07-28

David Schinazi – dschinazi.ietf@gmail.com
David Oliver – david@guardianproject.info

Motivation

Client authenticates to server

Using asymmetric cryptography

Server hides the fact that it serves authenticated resources

Why this doesn't exist yet

Asymmetric cryptography requires a unique nonce to sign

When the server sends this nonce, it leaks the fact that it requires authentication

e.g., HOBA uses WWW-Authenticate to send nonce from server to client

Proposed Solution

Use TLS Key exporter to generate nonce

Doesn't leak any information

Can't be replayed on a separate connection

Transport-Authentication Header

Authenticates a single request

Sends:

- auth type (whether Signature or HMAC)
- a: algorithm OID
- u: username
- p: proof (bytes of the signature/HMAC)

```
Transport-Authentication: Signature u="am9obi5kb2U="; a=1.3.101.112; p="SW5zZXJ0I...5IQ=="
```

Intermediaries

Cannot be transparently forwarded

Intermediaries check authentication then communicate result upstream

Next Steps

Independent implementation by Guardian Project

Is this of interest to the HTTPBIS WG?

HTTP Transport Authentication

draft-schinazi-httpbis-transport-auth

IETF 114 – Philadelphia – 2022-07-28

David Schinazi – dschinazi.ietf@gmail.com
David Oliver – david@guardianproject.info