HTTP Unprompted Authentication

draft-schinazi-httpbis-unprompted-auth

IETF 115 – London – 2022-11

David Schinazi – dschinazi.ietf@gmail.com
David Oliver – david@guardianproject.info
Jonathan Hoyland – jonathan.hoyland@gmail.com

History

This is the successor to draft-schinazi-httpbis-transport-auth

Modified to fit better into HTTP semantics

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

Unprompted-Authentication Header

Authenticates a single request

Sends:

- auth type (whether Signature or HMAC)
- s/h: signature/hash algorithm (uses TLS value)
- u: username
- p: proof (bytes of the signature/HMAC)

```
Unprompted-Authentication: Signature u=:am9obi5kb2U=:;s=7;p=:SW5…5IQ==:
```

Intermediaries

Cannot be transparently forwarded

Intermediaries check authentication then communicate result upstream

What we changed since IETF 114

Renamed draft to "Unprompted Authentication"

Removed use of OIDs

Clarified security concerns discussed at 114

Added Jonathan as coauthor

Switched to structured fields

Editorial work

Next Steps

Independent implementation by Guardian Project

Is this of interest to the HTTPBIS WG?

HTTP Unprompted Authentication

draft-schinazi-httpbis-unprompted-auth

IETF 115 – London – 2022-11

David Schinazi – dschinazi.ietf@gmail.com
David Oliver – david@guardianproject.info
Jonathan Hoyland – jonathan.hoyland@gmail.com