HTTP Unprompted Authentication

draft-ietf-httpbis-unprompted-auth

IETF 116 – Yokohama – 2023-03-28

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

Quick Summary, Motivation, History

Client authenticates to server

Using asymmetric cryptography

Server hides the fact that it serves authenticated resources

Adopted by HTTPBIS last month

Rough Shape of Solution

Use TLS Key exporter to generate nonce

Sign or HMAC the nonce

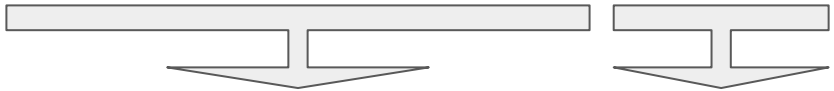
Doesn't leak any information

Can't be replayed on a separate connection

Shape of Header
(this changed since last time)

Unprompted-Authentication: Signature k=:YmFzZW1lbnQ=:;s=7; p=:SW5z...IQ==:

Unprompted-Authentication: HMAC k=:YmFzZW1lbnQ=:;h=6;p=:SW5z...IQ==:



New header 2 new HTTP auth schemes

(Before we had a new concept of "Unprompted auth schemes",
now reuses preexisting HTTP auth schemes)

#2440: Sure, an IANA registry! But which one?

Unprompted-Authentication: Signature k=:YmFzZW1lbnQ=:; s=7; p=:SW5z...IQ==:
Unprompted-Authentication: HMAC k=:YmFzZW1lbnQ=:; h=6; p=:SW5z...IQ==:

Client tells server which signature/hash algorithm is in use

Need some sort of extensible mechanism to allow adding new ones later

- TLS SignatureScheme & HashAlgorithms registries but orphaned by RFC 8447
- Possibility of using JSON Web Algorithms registry (but complexities with "alg")
- Should we just create a new registry?

#2432: New header vs existing Authorization header

Now that we've made HMAC and Signature regular HTTP authentication schemes, do we actually need a separate "Unprompted Authentication" header?

RFC 9110 s11.6.2:

> The "Authorization" header field allows a user agent to authenticate itself with an origin server -- usually, but **not necessarily**, after receiving a 401 (Unauthorized) response.

#2428, #2429: TLS Key Exporter Context

Currently nonce is generated via TLS key exporter with empty context

Should we add the following to the context?

- Signature/hash algorithm
- Key identifier
- Origin
- URL

#2439: Contextualizing Signatures

Currently we just sign the nonce

Could be bad if key are reused

Two solutions:

- Add a fixed context string UnPrOmPtEdAuThFoRfUnAnDpRoFiT
- Tell people not to reuse keys

HTTP Unprompted Authentication

draft-ietf-httpbis-unprompted-auth

IETF 116 – Yokohama – 2023-03-28

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