HTTP Signature Authentication Scheme

HTTPbis draft-ietf-httpbis-unprompted-auth-06

IETF 119
16–17 March 2024
Brisbane, Australia

What?

- Provide authenticated HTTP resources without telegraphing you are doing so
    - Client provides correct authentication without any additional flows or…
    - Server fails with generic error (“404”)
- Un-probe-ability

Hackathon Plan

- First Interoperability test!
  - draft-ietf-httpbis-unprompted-auth-06

- Two server implementations, one client
  - Will it blend?

Implementation Reference

★ Guardian Project Java implementation (client+server): https://gitlab.com/guardianproject/httpsignatureauthentation/-/tree/main/http-sigauth-java

- Supports HTTP 1 and 2

★ Guardian Project nginx impl (server): https://gitlab.com/guardianproject/httpsignatureauthentation/-/tree/main/ngx-http-sig-auth-module?ref_type=heads

- Supports HTTP 1, 2, and 3 (limited)

★ François Michel's Go impl (client+server): https://github.com/francoismichel/http-signature-auth-go

- Supports HTTP 1, 2, and 3
- Interops with Guardian's Client impl

David Schinazi's impl (client+server): https://github.com/google/quiche/

- Implemented inside Google's quiche library (a QUIC/HTTP3 implementation)
- Supports HTTP 3
- Interops with François's server (+ vice versa)

★ Tested at IETF119 hackathon

Known Public HTTP Sig. Auth. Servers

- https://sigauth.unready.im/ping
  By: Abel Luck / Guardian Project
  Impl: NGINX, C
  Supports: HTTP 1, 2, 3
  Notes: To add you own pub key
  https://sigauth.unready.im/keydb
- https://sigauth.unready.im:8191/ping
  By: Abel Luck / Guardian Project
  Impl: Jetty, Java
  Supports: HTTP 1, 2 (or 3 via reverse proxy)
  Notes: To add you own pub key
  https://sigauth.unready.im/keydb
- https://httpsignature.francoismichel.be/signature/insecure/draft-ietf-httpbis-unprompted-auth-05
  By: François Michel, Université catholique de Louvain
  Impl: Go
  Supports: HTTP 1, 2, 3
  Notes: Accepts any key-id as long as the signature verifies
- https://httpsignature.francoismichel.be/signature/secure/draft-ietf-httpbis-unprompted-auth-05
  By: François Michel, Université catholique de Louvain
  Impl: Go
  Supports: HTTP 1, 2, 3

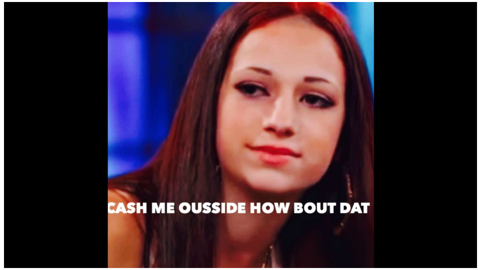
What got done

Server	Client	Success	Fail1	Fail2
GP (w RP)	GP	Y	Y	Y
GP (w/o RP)	GP	Y	Y	Y
FM (w/o RP) (any key)	GP	Y	Y	(Not tested)
FM (w/o RP) (any key)	Google	Y	Y	(Not tested)
Google (w/o RP)	FM	Y	Y	Y

Success - properly formatted request
Fail 1 - badly formatted (or empty) request
Fail 2 - bad credential

What we learned

- Lessons learned from this hackathon:
  - limited, initial test only
    - e.g., not enough failure cases tested
  - Some bothersome practicalities fitting this work into existing protocol stacks (client and server)
    - Cash me outside for much whining…



Wrap Up

Hackathon members:

- Abel Luck (remote)
  - abel@guardianproject.info
- David Oliver (on-site)
  - david@guardianproject.info
- François Michel (remote)
  - francois.michel@uclouvain.be

Spec Authors:

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

First timers @ IETF/Hackathon: Abel

Thanks to Abel and François for the hard work for this hackathon!

Guardian Project thanks David Schinazi and Jonathan Hoyland for pushing this specification forward within HTTPbis.

David Oliver thanks the Public Interest Technology Group (PITG) for funding his participation at this hackathon.