HTTP Message Signatures

Justin Richer & Annabelle Backman
IETF 115 - SAAG
November 11, 2022
What is it?

- Detached signatures for HTTP messages
  - Requests and responses
  - Robust against common changes
- Not message encapsulation
- Just past WGLC in HTTPbis
HTTP messages change in flight
Create a common *base* to work from
Example HTTP Message

POST /foo?param=value&pet=dog HTTP/1.1
Host: example.com
Date: Tue, 20 Apr 2021 02:07:55 GMT
Content-Type: application/json
Content-Length: 18

{"hello": "world"}
Sign These Components

POST /foo?param=value&pet=dog HTTP/1.1
Host: example.com
Date: Tue, 20 Apr 2021 02:07:55 GMT
Content-Type: application/json
Content-Length: 18

{"hello": "world"}
Signature Base String

"@method": POST
"@target-uri": https://example.com/fo?param=value&pet=dog
"content-type": application/json
"@signature-params": ("@method" "@target-uri"
    "content-type");created=161884475;keyid="test-key-1"
Signed Request

POST /foo?param=value&pet=dog HTTP/1.1
Host: example.com
Date: Tue, 20 Apr 2021 02:07:55 GMT
Content-Type: application/json
Content-Length: 18

Signature-Input: sig1="@method" "@target-uri"
    "content-type");created=1618884475;keyid="test-key-1"

Signature: sig1=Lu2cC2Ifw3hkpXt8iC9g78qppHzEUo7hPyeFmDNqkMe4AvPzhz8cRhI1+eIBisvM7ceDh40m0RmKjA5CUL5TFs9NuUHC0xuZZeiy5u7THftAZZU6LgwRynMuOZgJAYXYDsgBKfxRkoGVVEX1lSGi7RvhY1/EgWCJzuIbJ9mLeRxzaXRr3pZXz5xRaXcsXItpsK3AnWYHoc6YAT9hP5M3oJPeb3KRHoLAN4nheC0kFoyLzRAf6/BNb4I7JhwqVZMZBlndnI/TKBXoTK7rzYFdpX/Cbtwv+XHgli9QtHktw9hXC4Kv4lp2fCGSPJPHKeyrZ0rhCcfe++eJe0Ykm3FIw==:

{"hello": "world"}
HTTP Message Signatures

This site allows you to try out HTTP Message Signatures interactively. This page works in two modes: signing and verifying, both working in four steps. To sign, add an HTTP message to the form, choose which components should be signed, choose the signing key and algorithm, and view the signed results. To verify, add a signed HTTP message to the form, choose which signature to verify, supply the verification key material, and verify the results.

```
POST /foo?param=value&pet=dog HTTP/1.1
Host: example.com
Date: Tue, 20 Apr 2021 02:07:55 GMT
Content-Type: application/json
Content-Digest: sha-256=XX48E9gOokqqrvtts8nOJRJN3OWDlUoyWx8f7kbu9DBPE=
Example-Dict: a=1, b=3, c=4; aa=bb, d=5 6; valid
Content-Length: 18

{"hello": "world"}
```

https://httpsig.org/
What do we need?

• Review and implementation!
  – Especially from the security community

• This is a hard space with weird corners
  – Are there issues we've missed?

• Who else is implementing this?