HTTP Message Signing

IETF 92

Justin Richer

What is it?

- Method for generating and validating detached HTTP signatures
- Method for communicating a signature alongside an HTTP message
  - Analogous to Bearer Token Usage
  - This (trivial) part's not in the draft yet

Why do we need this?

- Desire to tie an OAuth token and signature to a specific HTTP request
  - Message-level signatures!
  - Belt-and-suspenders alongside TLS
- OAuth 1.0 can do it

How do you generate a signature?

1. Figure out what you want to sign
   - Query parameters, headers, body, host, port, …
2. Combine and hash these values
3. List out what you signed
4. Put everything inside of a JWT
5. Sign the JWT with JWS
6. Send the JWT to the RS

How do you check a signature?

1. Get a JWT at the RS
2. Validate the JWT's signature with JWS
3. Pull apart the body of the JWT to find out what was hashed
   - Query parameters, headers, body, host, port, …
4. Re-generate the hashes for the components indicated in the JWT body (and only those)
5. Compare the hashes to the ones in the JWT

Why do it this way?

- Don’t mess with the original HTTP
- Don’t duplicate the original HTTP
- Don’t wrap the HTTP into a container
  - Avoid “Just put everything in a JWT!”
- Be robust against parameter orders and insertion
- Be clear about what was signed and what wasn’t signed

What now?

- There are a few different takes on this same process that exist, do we use one of these?
  - OAuth 1.0
  - AWS signed messages
  - Etc.
- Is anyone willing to build this out and get hands-on experience with it?