HTTP Digest Authentication Scheme

Rifaat Shekh-Yusef
IETF 91, HTTPAuth WG
Honolulu, Hawaii, USA
November 14, 2014

Status

- Finished WG Last Call
- Great reviews and feedbacks from:
  - Stephen Farrell, Michael Sweet, Benjamin Kaduk, Brett Tate, Julian Reschke, and Alexey Melnikov.
- No major issues
- Few open issues to discuss today

Stale

- A case-insensitive flag, indicating that the previous request from the client was rejected because the nonce value was stale. If stale is TRUE, the client may wish to simply retry the request with a new encrypted response, without reprompting the user for a new username and password. **The server should only set stale to TRUE if it receives a request for which the nonce is invalid but with a valid digest for that nonce (indicating that the client knows the correct username/password).** If stale is FALSE, or anything other than TRUE, or the stale parameter is not present, the username and/or password are invalid, and new values must be obtained.

A1

- If the "algorithm" parameter's value is "<algorithm>-sess", e.g. "SHA-256-sess", **then A1 is calculated using the initial nonce [value provided in the challenge from the server,] and cnounce value from the first request by the client following receipt of a WWW-Authenticate challenge from the server. It uses the server nonce from that challenge, herin called nonce-prime, and the first client nonce value [from the response] to construct A1, herin called cnonce-prime as follows**:

```
A1 = H( unq(username) ":" unq(realm) ":" passwd ) ":"
     unq(nonce-prime) ":" unq(cnonce-prime)
```

Net Unicode & NFC

- Should RFC 5198 (Net Unicode) be recommended for use on top of NFC?
  - For example, it discourages use of Unicode Control characters

- Is it Ok to fail authentication if a username is not in NFC?
  - If yes, it would be good to mention how the server should respond in such case.

Quoted Strings

- The following two paragraphs can be added to section 3.3:
  - For historical reasons, a sender MUST only generate the quoted-string syntax values for the following parameters: realm, domain, nonce, opaque, and qop.
  - For historical reasons, a sender MUST NOT generate the quoted-string syntax values for the following parameters: stale and algorithm.
- The following two paragraphs can be added to section 3.4:
  - For historical reasons, a sender MUST only generate the quoted-string syntax for the following parameters: username, realm, nonce, uri, response, cnonce, and opaque.
  - For historical reasons, a sender MUST NOT generate the quoted-string syntax for the following parameters: algorithm, qop, and nc.
- …

charset

- Should the draft mention what the default character set is if the parameter is not present? ISO 8859-1?

cnonce

- Currently, the value of the cnonce parameter is implementation dependent.
- Should a more specific recommendation be added? If so, what is the added value?