HTTP Digest Authentication Scheme

Rifaat Shekh-Yusef

IETF 90, HTTPAuth WG, Toronto, Canada

July 24, 2014

Username Hashing

- **OLD**
  - **Server**: H(username | realm)
  - **Client**: H(H(username | realm) | nonce)
- **NEW**
  - **Server**: H(username | realm)
  - **Client**: H(username | realm)

RFC2069 Backward Compatibility

- **Removed** backward compatibility with RFC2069:
  - The **qop** parameter is now **mandatory**.
  - Impacts the calculation of the **response** for the **Authorization Request Header**:
    - **RFC2617**: H(H(A1),nonce:nc:cnonce:qop:H(A2))
    - **RFC2069**: H(H(A1),nonce:H(A2))

Algorithms Preference

- Removed the algorithms preference from the registry.
- The preference must be specified by the document introducing the new algorithm.

Normalization

- Used the text provided by **Julian** for the **Basic** draft:

"The only allowed value is "UTF-8", to be matched case-insensitively (see [RFC2978], Section 2.3). It indicates that the server expects user name and password to be converted to Unicode Normalization Form C ("NFC", see Section 3 of [RFC5198]) and to be encoded into octets using the UTF-8 character encoding scheme ([RFC3629])."

Domain Parameter

- **Domain** is an optional parameter used with the WWW-Authenticate response header.

- Proposal on the mailing list to **deprecate** this parameter, because:
  - “Ignored by Chrome and Firefox”
  - “As currently written, **Domains** has the same security issues as session cookies and cross domain usage.”

- Any thoughts?