HTTP Digest Access Authentication

Rifaat Shekh-Yusef

IETF 89, HTTPAuth WG, London

March 3, 2014

Overview

- **Draft**
  - **draft-ietf-httpauth-digest-05**
  - **Standards Track**
  - **Obsoletes RFC2617***
- **Changes**
  - **Algorithms Agility**
  - **Internationalization**
  - **Username Protection**

*Together with Basic & Authentication drafts

Algorithms Agility

- **New Algorithms**
  - SHA-256
  - SHA-512/256
- **Explicitly allows multiple Authenticate headers with the same scheme.**
- **New IANA Registry.**

“HTTP Digest Hash Algorithms” Registry

Hash Algorithm	Digest Size	Preference	Reference
MD5	32	1.0	RFC XXXX
SHA-512-256	64	2.0	RFC XXXX
SHA-256	64	3.0	RFC XXXX

Update Policy: Specification Required.

Internationalization

- **charset**
  - A new optional parameter to be used to indicate the encoding used by the server.

- The only allowed value is **UTF-8**.

- The approach is aligned with **Basic**.

Username Protection

- **userhash**
  - A new optional parameter.
  - **Usage**:

    Server: indicates it supports username hashing.

    Client: indicates that username has been hashed.
  - Valid value are: "**true**" or "**false**".

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

Backward Compatibility

- **RFC2617**
  - H (H(A1) | nonce | **nc** | **cnonce** | **qop** | H(A2))
- **RFC2069**
  - H (H(A1) | nonce | H(A2))

- **Is backward compatibility needed?**
- **Are there many servers that:**
  - Support RFC2069, but not RFC2617?
  - Support RFC2617, but do not send “qop”?

Feedback?

- **IANA Registry**
- **Backward Compatibility**
- **Normalization**