HTTP Digest
HMAC & Salted Hash Proposal

Rifaat Shekh-Yusef
IETF 93, HTTPAuth WG
Prague, Czech Republic
July 20, 2015

Background

- The reviews provided by the **Gen-Art** and **SecDir** for the **HTTP Digest** draft suggested that we add support for **HMAC** algorithms.
- The **STUNbis** team, which is part of the **TRAM WG**, asked to add support for **salted** hash.

Proposal

- **Hashing**
  - H(data) = Hash(data)
  - KD(secret, data) = **HMAC**-Hash(secret, data)
- **A1**
  - username:realm:password:**salt**

Parameters

- **Salt**
  - A new **salt** parameter will be included in the **WWW-Authenticate** header field provided in challenge request from the server.
- **Algorithm**
  - The existing **algorithm** parameter values will be extended to include the **HMAC** algorithms.

Example

- **A1** = username:realm:password:salt
- **H(A1)** = **SHA256**(username:realm:password:salt)
- **Response** =

  KD(H(A1), nonce:nc:cnonce:qop:H(A2)) =

  HMAC-SHA256(H(A1), nonce:nc:cnonce:qop:H(A2))

Questions?