Salted Challenge Response Authentication Mechanism (SCRAM) SASL authentication mechanism

draft-newman-auth-scram-10.txt
draft-newman-auth-scram-gs2-01.txt

Abhijit Menon-Sen <ams@oryx.com>
Chris Newman <chris.newman@sun.com>
Alexey Melnikov <alexey.melnikov@isode.com>
Simon Josefsson <simon@josefsson.org>

IETF 74, San Francisco

SASL Framework

- Specified in RFC 4422
- Used by application layer protocols
  - IMAP – RFC 3501
  - POP3 – RFC 5034
  - LDAP – RFC 4510
  - SMTP – RFC 4954
  - ManageSieve – RFC-ietf-sieve-managesieve-09.txt
  - XMPP – RFC 3920
  - BEEP – RFC 3080
  - And few others
- Not used by HTTP

Existing password based SASL mechanisms (1 of 3)

- **PLAIN**
  - Doesn't support server authentication
  - And sends username/password in the cleartext, so it relies on encryption provided by lower- level security services (e.g., TLS)
  - Can be used with most authentication databases
  - Allows “bad” servers to reuse the password in order to break into other user's accounts

Existing password based SASL mechanisms (2 of 3)

- **CRAM-MD5**
  - Doesn't send password in cleartext
  - But doesn't support server authentication
  - Doesn't support some modern SASL features like
    - Internationalization
    - Acting on behalf of other users
    - Channel bindings
  - So it is simple to implement, but not considered secure anymore (e.g. it allows connection hijacking)

Existing password based SASL mechanisms (3 of 3)

- **DIGEST-MD5**
  - Doesn't send password in cleartext
  - Supports server authentication
  - Was designed to be compatible with HTTP-Digest but in practice this compatibility is limited
  - Difficult to implement fully and correctly
    - Too many options
    - Interoperability is not good

SASL WG objective

- Design a "better" password-based SASL mechanism:
  - Doesn't send password in cleartext
  - Supports server authentication
  - Supports modern SASL features:
    - Supports internationalized usernames and passwords
    - Supports optional channel bindings to TLS
    - Uses more modern crypto (HMAC-SHA-1 instead of HMAC-MD5)
  - Simpler to implement than DIGEST-MD5
- Result: **SCRAM** (Salted Challenge Response Authentication Mechanism)

Status of SCRAM

- The core authentication protocol is complete
- Some members of the SASL WG want to use GSS-API Framing for the document
  - So that the same authentication mechanism can be used in protocols like NFS and HTTP **as is**
  - Note that if this happens, the protocol would **still be text based**
  - Further debate is going to be in SASL WG meeting this week
- Some **early implementations** starting to appear

What's next for SCRAM

- Once SCRAM is finished, need to investigate about the best way of integrating it into HTTP