Simple Authentication and Security Layer (SASL) WG

Chairs: Tom Yu, Kurt Zeilenga

IETF 67

Tuesday, November 7, 2006

17:40–19:50

Agenda

- Intro, scribe, agenda bashing
- Document status
- CRAM-MD5
- DIGEST-MD5 (rfc2831bis)
- GS2
- Discuss milestones
- Open mike

Document Status

- `draft-ietf-sasl-crammd5-07.txt`
- `draft-ietf-sasl-gs2-02.txt`
- `draft-ietf-sasl-gssapi-08.txt` – RFC editor queue
- `draft-ietf-sasl-plain-09.txt` – RFC 4616
- `draft-ietf-sasl-rfc2831bis-10.txt`

DIGEST-MD5: editorial changes

- ABNF cleanup
- Replaced MD5(x) with H(x), as MD5() construct is not defined (thanks to Dave Cridland for pointing this out)
- Reworded the text about authorization identity verification to be non normative (as it is a protocol matter).
- Clarified that cnonce must be the same on reauthentication (this differs from HTTP Digest).
- Cleanup list of changes since HTTP Digest and RFC 2831.

DIGEST-MD5: non-editorial

- Replaced RC4 with AES-CTR as mandatory to implement.
- Added qop and cipher to the new client/server nonce (with channel binding), so that they can be protected
- Moved ABNF reference to the Normative References section.
- Replaced the text about CBC mode attack with some general description of attacks on padding.
- Added response-v2 option: client now generates two hashes; server verifies either. (Thanks to Jeffrey Hutzelman regarding this change)
- Cleaned up description of prep directive. Username/password prep now done on both client and server.

DIGEST-MD5: open issues/todo

- Add some text why RC4 is no longer mandatory to implement (?)
- Reference to the document describing channel binding for TLS needs to be corrected.
- Backward compatibility with RFC 2831 needs to be clarified (.e.g. when charset directive is present and the prep directive is not)
- Interaction between the new prep and the old charset directives needs to be clarified
- The charset directive is kind of optional, but in practice it is not. Should it just be made mandatory?
- Updated examples to match the new text

GS2

Milestones

Sep 06 GS2 to IESG

Sep 06 CRAM-MD5 to IESG

Sep 06 DIGEST-MD5 to IESG

Oct 06 Implementation report plan (with milestones)

Nov 06 Revise charter or conclude

Open Mike