Simple Authentication and Security Layer (SASL) WG

Chairs: Tom Yu, Kurt Zeilenga

IETF 65

Thursday, March 23, 2006

15:10–16:10

Agenda

- Intro, scribe, agenda bashing – 5 min
- Document status – 5 min
- GSSAPI / GS2 – 20 min
- DIGEST-MD5 (rfc2831bis) – 20 min
- Discuss milestones – 10 min
- Open mike – remaining time

Document Status

- `draft-ietf-sasl-crammd5-06.txt`
- `draft-ietf-sasl-gssapi-04.txt`
- `draft-ietf-sasl-gs2-00.txt`
- `draft-ietf-sasl-plain-08.txt` – IESG eval.
- `draft-ietf-sasl-rfc2222bis-15.txt` – approved
- `draft-ietf-sasl-rfc2831bis-08.txt`

GSSAPI / GS2

DIGEST-MD5 (rfc2831bis)

DIGEST-MD5 Open Issues

- Do we need an IANA registry for channel bindings?
- HTTP Digest vs DIGEST-MD5 reauthentication nonce differences?
- New text on AES in counter mode uses implicit initial counter (like in SSH), is this Ok?
- Does timing attack still apply to AES in Counter mode?
- Which cipher is mandatory to implement? Simon has concerns about security of RC4.
- Drop downconversion to ISO-8859-1 stuff in favor of UTF-8? This is what people have suggested for HTTP Digest.

DIGEST-MD5 To Do

- Add saslprep=true option, as use of SASLPrep on username/password affects the DIGEST-MD5 hash

- Clarify that multiple qop options (sent from the server to the client) must be amalgamated and treated as a single qop option containing the combined list. (Interop issue discovered during review of HTTP Digest use in Radius)

- Some SASLPrep related cleanup is needed.

- Cleanup ABNF section and update references.

Milestones

DONE	SASL (+ EXTERNAL) to IESG
Jun 05	CRAM-MD5 to IESG
Jul 05	DIGEST-MD5 to IESG
Aug 05	GSSAPI mech to IESG
Oct 05	Implementation report plan (with milestones)
Nov 05	Revise charter or conclude

Open Mike