ABFAB Core Specs

Sam Hartman

Painless Security, LLC

IETF 82

November 18, 2011

PROGRESS

- ➜ Significant review comments recieved for GSS-EAP, GSS-EAP-NAMINg and AAA-SAML
- ➜ Documents updated to reflect most comments; reviewers indicated significant improvement
- ➜ Updates to reflect implementation experience
- ➜ Some issues remain

Current Status

- GSS-EAP: multiple reviewers say "very close," small issues remain
- GSS-EAP-Naming: IANA assignments and URN components remain
- AAA-SAML: ongoing discussions

GSS-EAP

IMPROVEMENTS

- Significant cleanups to token exchanges and naming
- Filled in IANA sections
- Added proxy behavior section
- Outstanding comments from Alexey

Open Issues

- Fill in TBDs
- Internationalization
- RFC 3961 MIC or RFC 4121 MIC
- Remove EAP Identity/request?
- Acceptor naming
- RADIUS attributes

TBDs to Fill in

- OID: waiting to resolve open protocol changes
- OID for name
- Error codes registry
- RADIUS registrations

INTERNATIONALIZATION

- GSS-EAP names may have user-entered components in the form of hostnames
- Recommendation from Applications ADs is to give our callers recommendations on how to handle hostnames but do nothing ourselves
- An EAP server MAY perform IDNA-sensitive comparison on hostname and realm portions
- Need to clearly specify any slots that are specifically U-labels or A-labels

RFC 3961 AND RFC 4121

- The mechanism uses MACs for GSS channel bindings and to protect negotiation
- Currently RFc 4121 tokens are used
- Using RFC 3961 tokens saves space avoids sequence number issues but requires an RFC 3961 library
- Chairs say we have enough support for this we can adopt unless there are objections

Removing EAP Identity Round trip

- Currently acceptor sends an EAP identity request with no content, initiator responds
- Wastes an entire round trip
- Proposal: recover this round trip
- send identity in its own subtoken

Removing EAP Identity Round trip (2)

- If client knows acceptor identity then EAP conversation starts with second message
- Need to allow initiator to learn acceptor identity before committing to an initiator identity
- Add complexity
- We need to decide if this is worth it

Acceptor Identity

- Today we recommend that if the client sends the acceptor name the acceptor does not say what name is actually used
- Jim wants the acceptor to return its name whenever it knows who it is
- Also, currently acceptor name is only protected by EAP channel binding; good enough?

RADIUS Attributes

- Proper RADIUS namespace to use is defined in draft `radext-radius-extensions`
- Currently not approved; also currently not many implementations
- Looks like this is a viable option
- Some danger that implementations of ABFAB will not match the specs if standardization or implementations of these attributes take too long

GSS-EAP-NAMING

IMPROVEMENTS

- ➜ Aligned with naming extensions in KITTEN
- ➜ Restructured so that other SAML mechanisms can use this.

Open Issues

- Need to choose URN names
- IANA registration