HTTP-Auth

Berlin, July 2013

Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

The brief summary:

- ❖ **By participating with the IETF, you agree to follow IETF processes.**
- ❖ **If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.**
- ❖ **You understand that meetings might be recorded, broadcast, and publicly archived.**

For further information, talk to a chair, ask an Area Director, or review the following:

BCP 9 (on the Internet Standards Process)

BCP 25 (on the Working Group processes)

BCP 78 (on the IETF Trust)

BCP 79 (on Intellectual Property Rights in the IETF)

Agenda

- Agenda Bashing + Blue Sheets
- Document Status
- Basic + Digest (Julian, Rifaat)
- Experimental Document Evaluation Criteria
- HOBA + MutualAuth + Extension + SCRAM
  - Stephen, Yutaka, Alexei
- Open Mic

Document Status

- Basic: basicauth-enc-01 posted 30-Jun
- Digest:
  - digest-encoding-02 posted 7-Jul
  - digest-update-04 posted 13-Jul
- HOBA: version -01 posted 15-Jul
- Mutual + extension: version -00 posted 1-Jul
- SCRAM: version -00 posted 1-Jul
- RESTAuth – not yet.

BASIC STATUS

DIGEST STATUS

EVALUATION CRITERIA FOR EXPERIMENTAL DRAFTS

Evaluation Criteria

- This group is chartered to create a bunch of experimental documents.
- The bar can and should be placed lower than it is for proposed standards.
- However, we're not sending protocols to the IESG that are insecure or impractical.
  - At least, not intentionally.
- So we'd like to use this time for a discussion of the criteria we should use in evaluating these proposals.

Evaluation Criteria

- The list we might come up with will be published on the mailing list as recommendations or guidance for evaluators.
- It is not intended to be binding. Comments about issues that are not covered by the criteria are welcome.
- Nor is the criteria list something that the chairs are imposing on the group
  - The list will be the result of this discussion here.

Evaluation Criteria

- Security
  - If the protocol has severe vulnerabilities, it should not progress.
  - If the protocol is only secure under certain conditions or assumptions, these should be listed in the Security Considerations section.
- Clarity
  - can a reasonably competent developer implement on the basis of this document?

Evaluation Criteria

- Implementation Pitfalls
  - Is implementing this unnecessarily difficult?
- Unstated Requirements or Assumptions
  - Does this require a file with password or password equivalents on every server?
  - Does this work only with TLS?
  - Does the server need access to TLS state?
  - Do we require a good random source on either or both sides?
  - Does this make new demands on UI

Evaluation Criteria

- Interaction with Infrastructure
  - Can it be made to work with AAA servers such as RADIUS or DIAMETER? (that's a positive)
  - Does it require them? (that's a negative)
- Performance
  - Does this proposal make extraordinary requirements of resources (CPU, memory, bandwidth)
  - Per authentication, per logged-in user, per defined user.

```
GET / HTTP/1.0
Host: a.example.com

HTTP/1.0 401 Unauthorized
WWW-Authenticate: RA-Basic realm=“foo”, charset=“UTF-8”,\
                  http://a.example.com/basic-auth-002/

POST /basic-auth-002 HTTP/1.0
WWW-ChannelBinding-Type: tls-server-end-point
WWW-SessionBinding-Type: session-ID

QWxhZGRpbjpvcGVuIHNlc2FtZQ==

HTTP/1.0 201 Created

DELETE /basic-auth-002
```

REST-AUTH

HOBA

MUTUAL AUTH + EXTENSION

SCRAM

OPEN MIC