HTTP(-)Auth

BoF

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

- Agenda Bashing, Blue Sheets
- Problem Statement – Chairs
- Proposals
- Charter Bashing, Interest gauging

Problem Statement

Chairs

HTTP Authentication

- HTTP (both version 1.0 and 1.1) can run over either a secure or an insecure transport.
- By default, the user is not identified or authenticated.
- But HTTP does contain a framework for user authentication.
- This is described in section 2 of draft-ietf-httpbis-p7-auth.

HTTP Authentication

- Existing standards provide two authentication methods:
  - Basic: analogous to PPP's PAP
  - Digest: analogous to CHAP or MD5-Challenge
- Both are considered to be insecure today.
- We're looking for something better.

HTTP Authentication - example

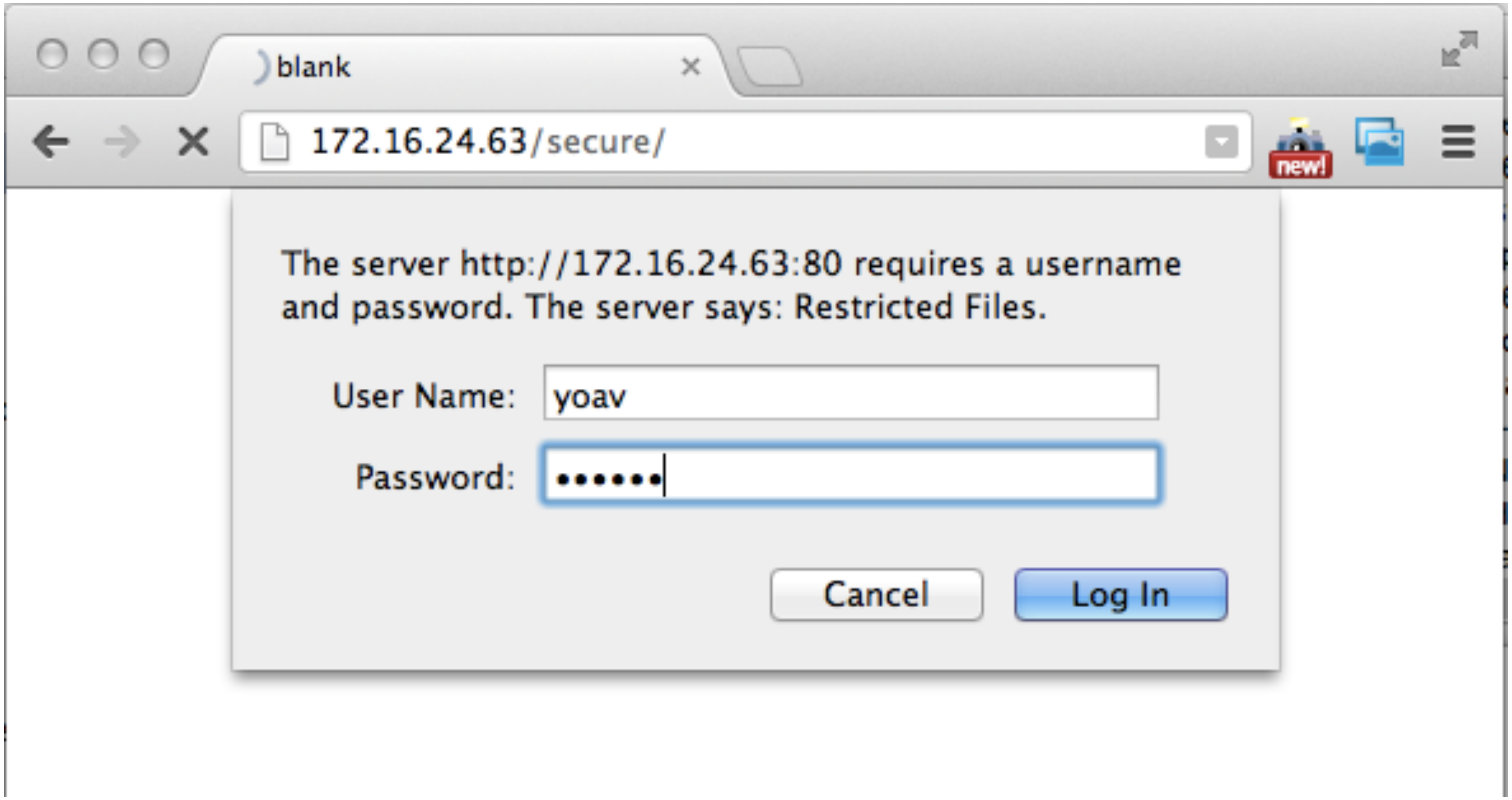
```
GET /secure/ HTTP/1.1
Host: 172.16.24.63
Connection: keep-alive
User-Agent: Mozilla/5.0 …
Accept: text/html, application/xhtml+xml,…
Accept-Encoding: gzip, deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: Session=_dd5162e1f3854eff3044b0f54500681c
```

HTTP Authentication - example

```
HTTP/1.1 401 Unauthorized
Date: Tue, 30 Oct 2012 09:17:04 GMT
Server: Apache/2.4.3 (Unix) OpenSSL/1.0.1
WWW-Authenticate: Basic realm=“Restricted Files”
Content-Length: 381
Keep-Alive: timeout=5 max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC “-//IETF//DTD HTML 2.0//EN”>
<html><head><title>401 Unauthorized</title></head><body>
<h1>Unauthorized</h1><p>This server could not verify that
you are authorized to access the document</p></body></html>
```

HTTP Authentication - example



The server http://172.16.24.63:80 requires a username and password. The server says: Restricted Files.

User Name: yoav

Password: ••••••

HTTP Authentication - example

```
GET /secure/ HTTP/1.1
Host: 172.16.24.63
Connection: keep-alive
Authorization: Basic eW9hdjpzbGlua3k=
User-Agent: Mozilla/5.0 …
Accept: text/html, application/xhtml+xml,…
Accept-Encoding: gzip, deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: Session=_dd5162e1f3854eff3044b0f54500681c
```

HTTP Authentication - example

```
HTTP/1.1 200 OK
Date: Tue, 30 Oct 2012 09:17:17 GMT
Server: Apache/2.4.3 (Unix) OpenSSL/1.0.1
Last-Modified: Tue, 30 Oct 2012 08:41:36 GMT
Etag: “56-4cd42c101cd91”
Accept-Ranges: bytes
Content-Length: 61
Keep-Alive: timeout=5 max=99
Connection: Keep-Alive
Content-Type: text/html;

<html><body>hello there. This is a secure page.</body></html>
```

HTTP Authentication

- This kind of authentication is rarely used.
- There are some UI issues:
  - Credentials are used with every request, so they are stored
  - No logoff
  - The authentication dialog is over a blank page, or the previous page
  - No control of “user experience”
  - Even worse when authentication is required for a resource rather than the main page

HTTP Authentication

- This does not mean there is no authentication.
- Here are some alternatives:
  – Authenticate with a web form, and store a cookie
  – Authentication in TLS
  – Federations with authentication through URLs
    - OpenID, WebID, OAuth, etc.
  – All have advantages and disadvantages
- In this BOF we will try to see if there's still interest in updating HTTP authentication with modern methods.

Problem Statement

- Vague on purpose. Different problems require different solutions.
  - – HTTP authentication in neither secure nor used.
  - – Obsolete crypto (or none at all)
  - – Only supports passwords
  - – Not “skinnable” (“personalizable”?)
  - – No session management (log off from either side)
- Let’s do better for the web
  - – At least in some circumstances.

Proposal Presentations

Proposal Presentations

- These presentations are ***short***
  - So is the time to discuss them
- Please avoid technical nits, encoding etc.
  - When (if) this is a WG draft, there will be plenty of time for that
- Clarifications and fitness-for-purpose are on-topic
  - So is security, roundtrips, etc.

Show Proposal Presentations Now

Charter Discussion

Charter Discussion

- The presentations we've just seen are candidates for a WG, should one be formed.
- Before we dive in, let's see a show of hands how many people would be willing to do work (writing, reviewing documents) in such a group
  - And how many think such a WG would be a terrible idea.
- How many think such a group should not be formed.

Charter Discussion

- The next few slides will show the draft charter as proposed by Sean.
- We will pause at the end of each slide for people to come to the mike and say why this is a terrible idea.
- Again, this is separate from choosing initial documents for the working group.
  - That will come later

Proposed Charter (1/5)

HTTP authentication [draft-ietf-httpbis-p7-auth] is currently used for user authentication by some web sites. While form-based user authentication is currently much more commonly used, there is utility in providing better documentation for existing HTTP user authentication schemes that are in use, and for documenting experimental HTTP user authentication schemes that might offer security benefits for future uses.

Proposed Charter (2/5)

The httpbis WG recently issued a call for proposals for HTTP authentication schemes as part of its work in further developing HTTP, including work on HTTP/2.0. While a number of proposals were made, there is at present no consensus to adopt any of those as standards-track work items within the httpbis WG.

The http-auth WG will develop a set of informational or experimental RFCs for HTTP user authentication schemes that could, following experimentation, be widely adopted as standards-track schemes for HTTP user authentication.

Proposed Charter (3/5)

All schemes to be developed in the http-auth WG must be usable with the existing HTTP authentication framework, or with evolutions of that framework as developed in the httpbis WG. That is, the evolution of the HTTP authentication framework is to be done in the httpbis WG and not in the http-auth WG.

However, the http-auth WG may document requirements for changes or additions to the HTTP authentication framework and any schemes developed in the http-auth WG that would benefit from such changes or additions to the HTTP authentication framework must document those changes or additions as an inherent part of their specifications. Any such schemes must however also be usable with the existing unmodified HTTP authentication framework.

Proposed Charter (4/5)

The http-auth WG will work closely with the httpbis and tls WGs and WGs in W3C to ensure that the outcomes from the http-auth WG do not conflict with work done elsewhere.

The initial list of work items will be:

- *We'll add those in later…*

Adoption of additional work items will require a re-charter.

Proposed Charter (5/5)

The following are out of scope:

- changes to HTTP
- changes to TLS
- definition of authentication mechanisms that do not work with the current HTTP authentication framework
- authentication of devices or components of web services.

not sure about this bit, we don't want to boil any oceans, but maybe "just web sites" is too limiting?

Selecting Proposals

- For each of the presentations you've seen, we're going to ask the usual questions:
  - Why should we ***not*** adopt it – is it terrible?
  - How many would be willing to contribute?
  - How many would be willing to review?
- We are not here to pick a winner.
  - We're not going to crown the one an only authentication method for the Web.
  - We would like to work on several different proposals.

Selecting Proposals

- HOBA – Farrell / Hoffman
- MutualAuth - Oiwa
- RESTauth – Williams
- SCRAM – Melnikov
- Multilegged - Montenegto