National Institute of
Advanced Industrial Science
and Technology
AIST

RCIS
Research Center for
Information Security

Overview of HTTP Mutual authentication protocol proposal

Yutaka OIWA

RCIS, AIST

July 26, 2010

Motivation

- Current HTTP authentication is weak both
  - In security:
    - Basic: plain-text authentication
    - Digest: off-line attack, not well implemented
    - TLS Client cert: too complex for most users
  - In functionality:
    - No log-off
    - Modal dialog for authentication
    - Authentication “enforced”
      - No good support for guest users

… Many people just avoids use of Basic auth and…

Problem

- In reality, form-based auth is widely-used
  - Having many problems
    - Plain-text only
    - Very weak against phishing attacks
- To solve, a “better” HTTP auth is required.
  - Solves both security and the feature-lacking problems at once

HTTP “Mutual” auth.

- New access authentication method for HTTP
  - Secure (↔ HTTP Basic/Digest, HTML Form)
    - No offline password dictionary attack possible from received/eavesdropped traffic
  - Easy to use (↔ TLS client certificates)
    - Just a short password for authentication!
  - Provides *Mutual authentication*: clients can check server’s validity
    - Authentication will ONLY succeed with servers possessing valid authentication secrets
    - Rogue (phishing) servers can’t make authentication to succeed

Basic design

- Implemented on top of RFC2617
- Password-based Mutual authentication
  - Using PAKE as underlying crypto primitive
- Authentication only
  - Can be used both with HTTP and HTTPS
  - Encryption/integrity provided by HTTPS
- Easy to manage
  - Client-side: *no* keys/storage required, just a pwd
  - Server-side: just a user/secret table required
    - Drop-in replacement to Basic and Digest

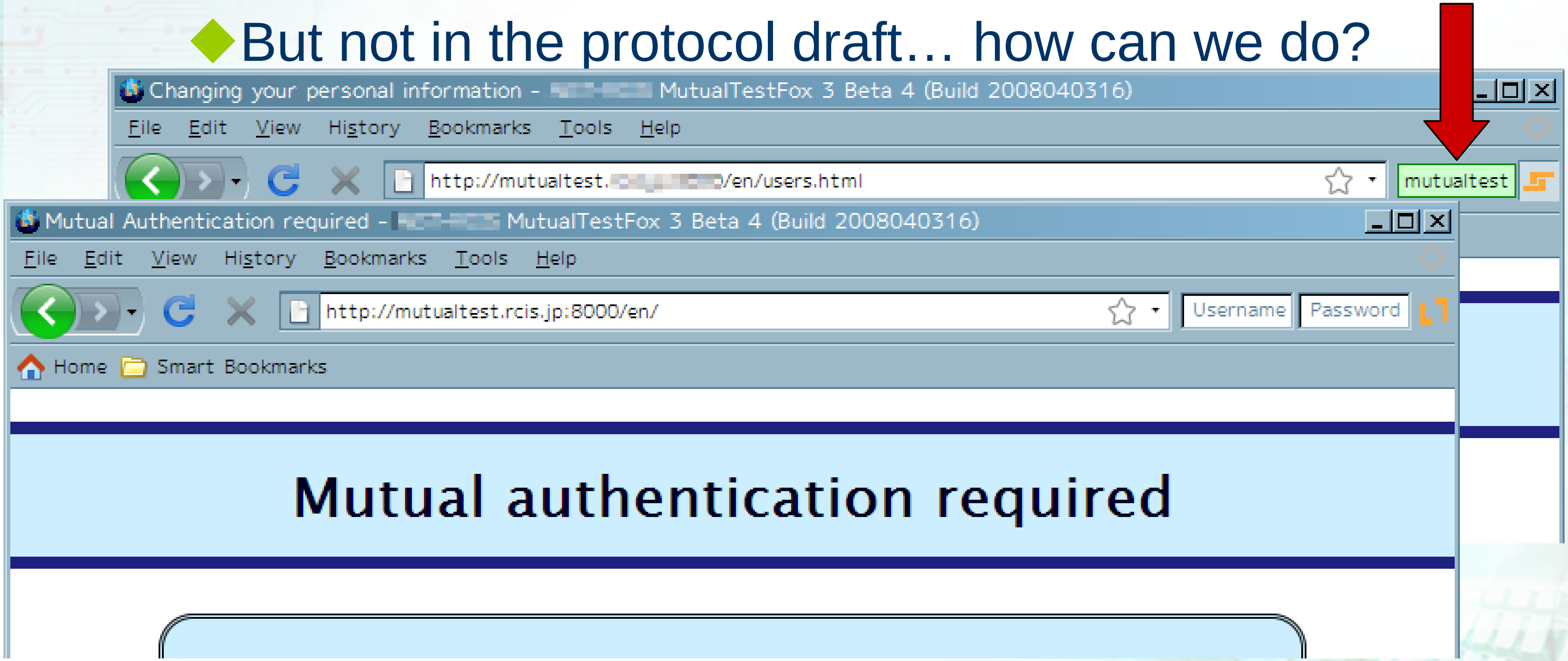
Rich application control for authentication

- Supports for recent Web application design
  - Explicit support for non-modal authentication
  - Optional authentication
    - Single URI can serve both auth/unauth contents
    - Support for sites like Slashdot, Google or Yahoo
  - Timed/server-initiated logout
  - log-on/log-off page redirection

  - Solving the “feature-lacking” problem of current HTTP auth

UI consideration

- Trusted display for mutual authentication result will be needed
  - We propose new UI for this auth scheme
    - But not in the protocol draft… how can we do?



Changing your personal information - [redacted] MutualTestFox 3 Beta 4 (Build 2008040316)

http://mutualtest.[redacted]/en/users.html

Mutual Authentication required - [redacted] MutualTestFox 3 Beta 4 (Build 2008040316)

http://mutualtest.rcis.jp:8000/en/

Mutual authentication required

Some project statuses

- Draft: draft-oiwa-http-mutualauth-06
  - -07 will be in August, in preparation
- Implementations:
  - Server-side: Apache module, Webrick/Ruby
  - Client-side: Mozilla patch, Ruby ref. impl.
- Other influences:
  - ◆Korean government agency have shown interest on the technology – adopted -04 draft as a local std.

Demo

- Off-site/off-time readers:
  - Trial Website on our project page.
    You can try it by yourself.
  - I will post a Flash movie on our website soon.

Request for “Comments”

- Comments for -07 draft are requested!
  - To appear in August.
  - (Of course, comments to -06 is welcome, but likely to be modified.)
- For security/HTTP transport experts:
  - Please give me a comment
    for the whole flow of the protocol.
- For application-layer experts:
  - Please review my proposal for Authentication-control features!
    - I have an intent to make it general for HTTP.
    - Feature requests are welcome!

Thank you

- More resources
  - Our project homepage: https://www.rcis.aist.go.jp/special/MutualAuth/
  - Draft:
    - Official: https://datatracker.ietf.org/drafts/draft-oiwa-http-mutualauth/
    - Some preliminary drafts (before submission) may be on our homepage