Security properties of HTTP and its associated mechanisms

[Inspired by draft-sayre-http-security-variance-00.txt]

Alexey Melnikov
<alexey.melnikov@isode.com>

IETF 70, Vancouver
Existing HTTP access authentication mechanisms (1)

- Using WWW-Authenticate/Authorization headers
  - **Basic** (RFC 2617)
    - cleartext
  - **Digest** (RFC 2617)
    - password based
  - **Negotiate (Kerberos)** (RFC 4559)
    - typically password based, but can be used with certificates, etc.
  - Other mechanisms proposed: NTLM (Microsoft), SRP (Mozilla), Mutua (Yahoo! Japan), etc.
Existing HTTP access authentication mechanisms (2)

- **Cookies** (RFC 2109, Netscape spec, RFC 2965)+HTML forms
  - forms used with POST and GET requests
  - cookies/hidden elements in forms are used to pass some authentication state from server to client
  - application/x-www-form-urlencoded body (for POST) or attributes in the query part of an HTTP URL (GET) are used to pass authentication state back
  - attributes in URLs/Cookies contain some kind of access token once authentication is complete
  - More sophisticated variants are deployed by Yahoo!, Google, Microsoft, etc.
Existing HTTP access authentication mechanisms (3)

• TLS
  – Provides both access authentication and connection integrity & confidentiality
  – Can be used for mutual authentication of client and server, if client-side certificate is requested & required by the server
  – Can also be combined with Basic, Digest (rarely) or Cookies + Forms
    • typically when no client certificate is provided
• Web Services
  – Things layered on top of HTTP: WS-Security, etc.
Connection integrity & confidentiality

• Digest has message integrity mode
• TLS
  – Hop-by-hop:
    • On a separate port (RFC 2818)
    • Using Upgrade mechanism (RFC 2817)
  – CONNECT can be used to establish end-to-end tunnel
    • Move CONNECT to 2616bis?
Next steps

• Find editor(s)
• Use draft-sayre-http-security-variance-00.txt as the base?
Other bits

- HTTPBis is not charted to work on new authentication mechanisms, but
  - Should it fix Internationalization in Basic?
  - Should the WG extract access authentication framework from RFC 2617 and move it to 2616bis?
- Section 1.2 + some security considerations from RFC 2617
- Clarify how multi-round trip authentication must be done
- Specify a set of requirements on access authentication methods (?)
  - e.g. internationalization, session-id