Problems with HTTP state management

IETF HTTP WG BoF, Chicago 2007

Yngve N. Pettersen
Opera Software ASA

Background

In HTTP is there is no direct way to indicate that two requests belong together in a session.

Client-Server sessions are currently maintained using

- Cookies
- HTTP Authentication

Client-side sessions are managed using

- Browse window history
- Cache

Problem descriptions

Two basic problems with current session/state management mechanisms:

- Limiting which servers receive cookies, particularly in ccTLDs, with domains like city.state.us.

  A cookie set by www.malicious.city.state.us to city.state.us can be used to track a user across the city.state.us domain, and might be used to attack how specific service inside the domain.

- No general method for informing the client about session's state and its associated data.

Cookie domain problems

HTTP Cookies can be sent to all servers in the server-specified domain.

- Netscape and RFC 2965 tried limiting distribution of cookies
- Netscape's method never implemented fully due to practical issues
- Both methods still permit undesirable distribution
- Clients use various rules to solve this problem

Similar problems exist for the cookie Path attribute.

Cookie domain solutions

Possible candidates are:

- DNS heuristics
- Lists of TLD domain hierarchies
- New cookie specification

Managing sessions

- Sensitive sites have sessions that consist of "log in", "perform tasks", "log out"
- Some services want "log out" to mean documents in the session are no longer accessible to the user, even in the history
- No "log out" in HTTP caused these sites to use various methods to emulate it
- Most workarounds increase network traffic, and reduce usability of the websites

Solving the session problem

Provide a mechanism to the websites allowing them to group their resources and control storage

- Associate URLs with a named context
- Include cookies and other credentials in the context
- A server-controlled expiration mechanism
- An automatic expiration mechanism

Drafts

DNS-related cookie domain proposals

- draft-pettersen-dns-cookie-validate-02.txt
- draft-pettersen-subtld-structure-02.txt

New cookie specification

- draft-pettersen-cookie-v2-01.txt

Cache context proposal

- draft-pettersen-cache-context-01.txt