Cookies and Session Tracking

CS320 Web and Internet Programming

Chengyu Sun
California State University, Los Angeles

The Need
- shopping cart, personalization, ...

The Difficulty
- HTTP is a "stateless" protocol
- Even persistent connections only last seconds

The Trick?

Session Tracking

Three Ways to Implement Session Tracking

General Idea

client
request
response + session id (sid)
request + sid
request + sid
request + sid
request + sid
request + sid

server

Three Ways to Implement Session Tracking

URL Re-writing
- E.g.
  http://csns.calstatela.edu/index .html;jsessionid=748D9512C9B19B0 DCC9477696A88CF12

Hidden form fields
Cookies

Cookies

- Issued by the server
  - HTTP Response: Set-Cookie
- Part of the next client request
  - HTTP Request: Cookie

HTTP Response Example

HTTP/1.1 200 OK
Date: Mon, 11 Apr 2011 16:53:26 GMT
Set-Cookie: JSESSIONID=7E3019D5D76D41E0B42FC1410B0A; Path=/
Content-Type: text/html; charset=ISO-8859-1
Content-Language: en-US
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 2208
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive

<html><head><title>CSNS</title></head>
...
HTTP Request Example

GET /img/style/title_bg.gif HTTP/1.1
Host: cns.calstatela.edu
User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:2.0) Firefox/4.0
Accept: image/png, image/*; q=0.8, */*; q=0.5
Accept-Language: en-us, en; q=0.5
Accept-Charset: ISO-8859-1, utf-8; q=0.7, *; q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie: JSESSIONID=7E3019D5D76D41E0B42FC1410B0

Cookie Attributes

- Name, Value
- Host/Domain, Path
- Require secure connection
- Max age
- Comment

Servlet Cookie API

- Cookie
- HttpServlet
  - addCookie(
  - HttpServlet
  - getServlet
  - Cookie[] getCookies()

Example: GuestBook with Session Using Cookies

- A user only needs to enter their name once
- Generate session id
  - sessionId
- Store session specific data
  - Map<String, Map<String, Object>>
  - sessionData

Cookie or No Cookie?

- Is cookie a potential security problem?
  - Virus?
  - DoS?
- How about privacy?
  - Cookie manager in Mozilla/Firefox
  - Internet Options in IE

It’s Not Easy ...

- ... to generate unique and random session id’s
- ... to tell whether the client has already left
- ... to track sessions when cookie is disabled
Servlet Session Tracking API

- HttpServletRequest
  - HttpSession getSession()
- HttpSession
  - setAttribute( String, Object )
  - getAttribute( String )
  - invalidate()

Example: GuestBook Using Session Tracking API

- Session is shared among servlets
  - Servlet context attributes (a.k.a. application scope variables) vs. session attributes (a.k.a. session scope variables)
    - Similarities??
    - Differences??
    - Usage??

Example: Login and Members

... Example: Login and Members

Username: [ ]
Password: [ ]

Members Only!

Login
Members

... Example: Login and Members

- Login
  - Validate username and password
    - Failed: redirect to error page
    - Succeeded: set a session attribute "username", and redirect to Members
- Members
  - Check session attribute "username"
    - null: redirect to Login
    - otherwise display content

Session Configuration in web.xml

- Default session timeout in Tomcat is 30 minutes
- Session timeout can be changed in web.xml
  - The timeout value must be an integer
  - Session never timeout if value \( \leq 0 \)

```xml
<session-config>
  <session-timeout>60</session-timeout>
</session-config>
```