Session Tracking

- The Need
  - shopping cart, personalization, ...
- The Difficulty
  - HTTP is a "stateless" protocol
  - Even persistent connections only last seconds
- The Trick??

General Idea

Three Ways to Implement Session Tracking

- URL Re-writing
  - E.g.
    http://acm.calstatela.edu/forum/viewforum.php?f=2&sid=1188411510a8221d0868

- Hidden form field
- Cookies

Example: GuestBook1

- Track user using hidden form field

Cookies

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

◆ Name, Value
◆ Host/Domain, Path
◆ Require secure connection
◆ Max age
◆ Comment (Version 1)

Servlet Cookie API

◆ Cookie
◆ HttpServletResponse
  ● addCookie( Cookie )
◆ HttpServletRequest
  ● Cookie[] getCookies()

Example: GuestBook2

◆ Track user using cookies

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 associate more information with a session
◆ ... to tell whether the client has already left

Servlet Session Tracking API

◆ HttpServletRequest
  ● HttpSession getSession()
◆ HttpSession
  ● setAttribute( String, Object )
  ● getAttribute( String )
  ● invalidate()
Example: Shopping Cart

- Shopping cart
  - Show a list of products
  - Add a product to the shopping cart
  - Remove a product from the shopping cart
- Using Session Tracking API

Is Session Shared among Servlets?

Example:

<table>
<thead>
<tr>
<th>Username:</th>
<th>Password:</th>
</tr>
</thead>
</table>

Login

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

ServletContext Attributes vs. Session Attributes

- Application Scope variables
- Session Scope variables

Example: SharedRequestCounter2

- Two request counters, one in application scope and one in session scope
- Application scope vs. session scope
  - Similarities??
  - Differences??
  - Usage??

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 <= 0

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