

## CS320 Web and Internet Programming

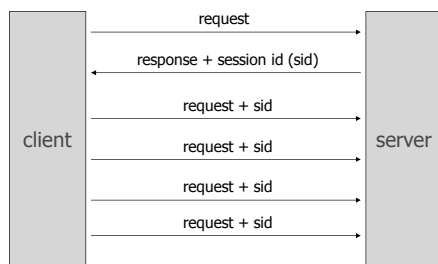
### Cookies and Session Tracking

Chengyu Sun  
California State University, Los Angeles

## 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://csns.calstatela.edu/index.html;jsessionid=748D9512C9B19B0DCC9477696A88CF12`
- ◆ Hidden form fields
- ◆ Cookies

## Cookies

- ◆ Set by the server as a *response header* Set-Cookie
- ◆ Added to each subsequent request by the browser as a *request header* 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
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html><head><title>CSNS</title></head>
... ..
```

## HTTP Request Example

```
GET /img/style/title_bg.gif HTTP/1.1
Host: csns.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-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie: JSESSIONID=7E3019D5D76D41E0B42FC1410B0A
```

## Cookie Attributes

- ◆ Name, Value
- ◆ Host/Domain, Path
  - Controls whether the cookie should be included in a request
- ◆ Require secure connection
- ◆ Max age
- ◆ Comment

## Servlet Cookie API

- ◆ Cookie
  - <http://download.oracle.com/javaee/6/api/javax/servlet/http/Cookie.html>
- ◆ HttpServletResponse
  - addCookie( Cookie )
- ◆ HttpServletRequest
  - Cookie[] getCookies()

## Example: GuestBook with Cookie

- ◆ Use a cookie to store name so a user only needs to enter their name once

## Cookie or No Cookie?

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

## Problems with Cookies

- ◆ Cookies have size limit
- ◆ Malicious users can fake cookie data
- ◆ Sometimes cookie is disabled in browser
- ◆ Cookie API is somewhat tedious to use

## Servlet Session Tracking API

- ◆ HttpServletRequest
  - HttpSession getSession()
- ◆ HttpSession
  - <http://download.oracle.com/javase/6/api/javax/servlet/http/HttpSession.html>
  - setAttribute( String, Object )
  - getAttribute( String )
  - invalidate()

## About Session Tracking API

- ◆ Data is stored on the server, i.e. no size limit
- ◆ Each session is assigned a unique *session id*, which is used to access data associated with the session
- ◆ Session id is randomly generated and hard to fake
- ◆ Session tracking use cookie by default, but can automatically switch to URL rewriting if cookie is disabled

## 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

...

Username: <input type="text"/>	Members Only!
Password: <input type="text"/>	_____
	_____
	_____
	_____

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 <= 0
- ```
<session-config>
  <session-timeout>60</session-timeout>
</session-config>
```