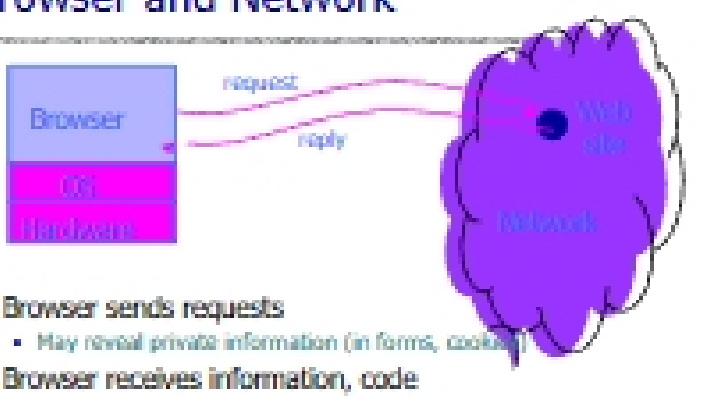
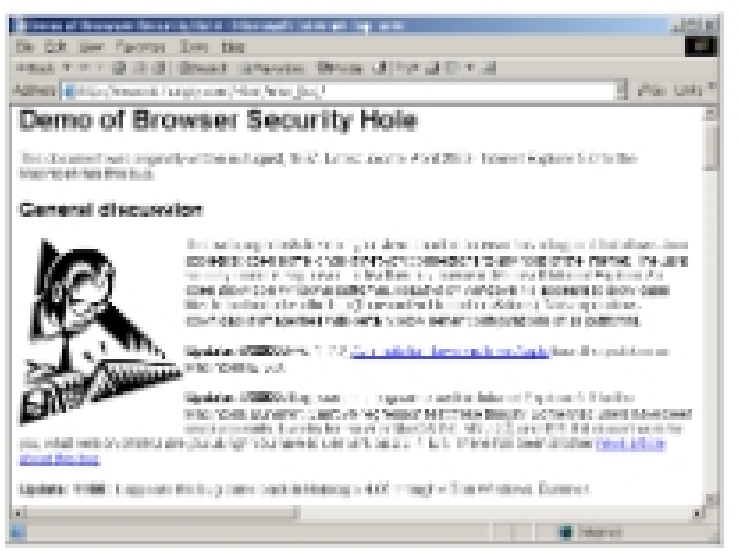
Browser Security

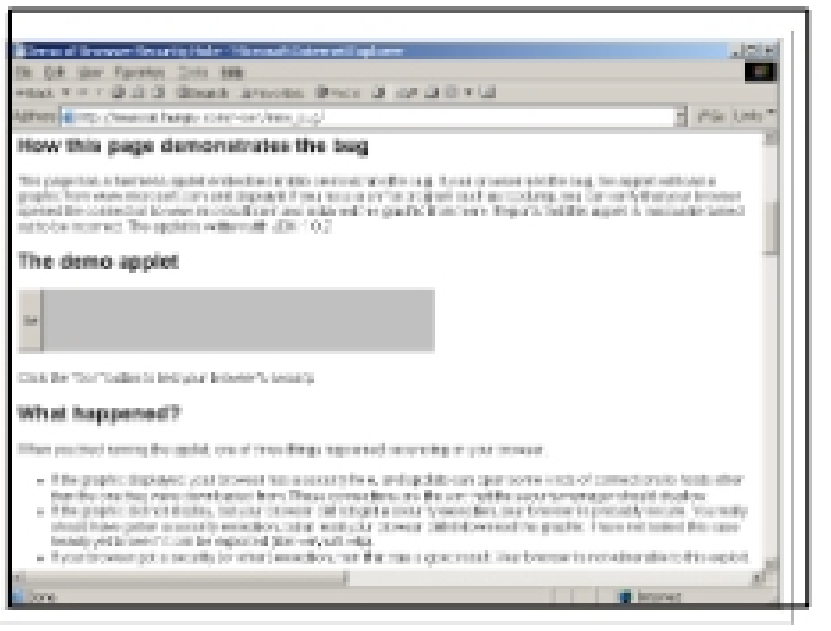
John Mitchell

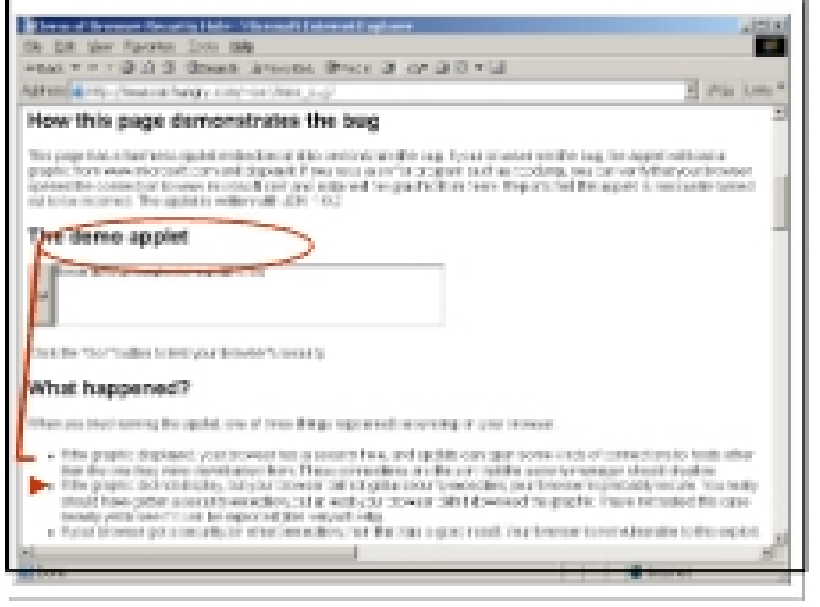
Browser and Network



- Browser sends requests
  - May reveal private information (in forms, cookies)
- Browser receives information, code
  - May corrupt state by running unsafe code
- Susceptible to network attacks
  - Consider network security later in the course







INTERNETWEEK.com Tuesday, February 12, 2002

Microsoft Issues New IE Browser Security Patch

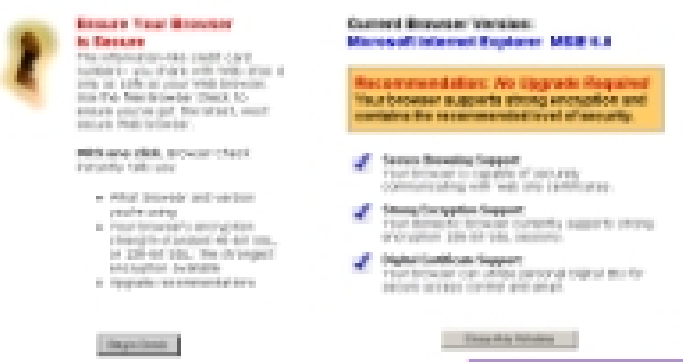
By Richard Karpinski

- Microsoft has released a security patch that closes some major holes in its Internet Explorer browser
- The so-called "cumulative patch" fixes six different IE problems ...
- Affected browsers include Internet Explorer 5.01, 5.5 and 6.0.
- Microsoft rated the potential security breaches as "critical."

Latest patch addresses:

- A buffer overrun associated with an HTML directive ... Hackers could use this breach to run malicious code on a user's system.
- A scripting vulnerability that would let an attacker read files on a user's systems.
- A vulnerability related to the display of file names ... Hackers could ... misrepresent the name of a file ... and trick a user into downloading an unsafe file.
- A vulnerability that would allow a Web page to improperly invoke an application installed on a user's system to open a file on a Web site.
- ... more ...

Browser Security Check



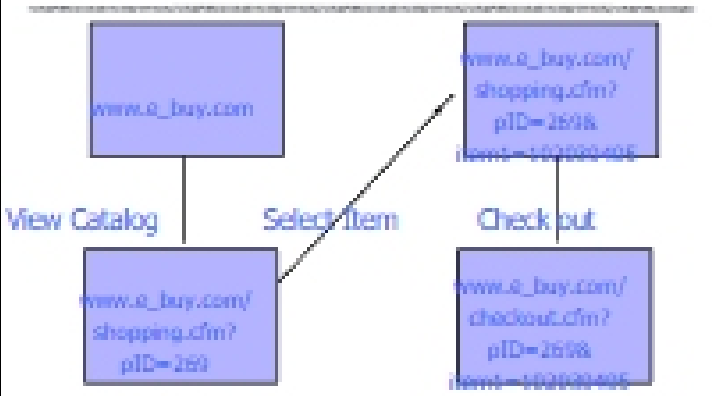
http://www.verisign.com/advisor/check.html

What kind of security are they checking?

Browser security topics

- Cookies
  - Cookie mechanism, JunkBuster, P3P
- Privacy
  - Anonymizer
- Mobile code
  - JavaScript
  - ActiveX
  - Plug-ins
  - Java
    - Interesting security model

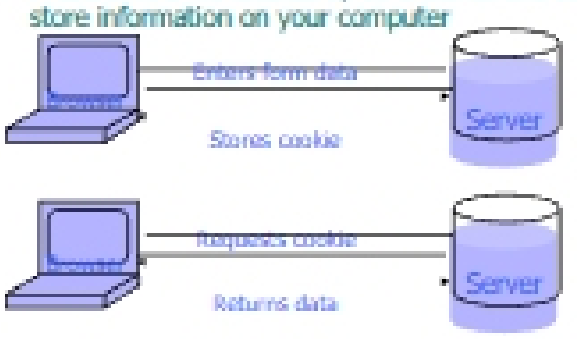
Basic Browser Session



Accumulate session information in URL

Store info across sessions?

- Cookies
  - A cookie is a file created by an Internet site to store information on your computer



HTTP is stateless protocol; cookies add state

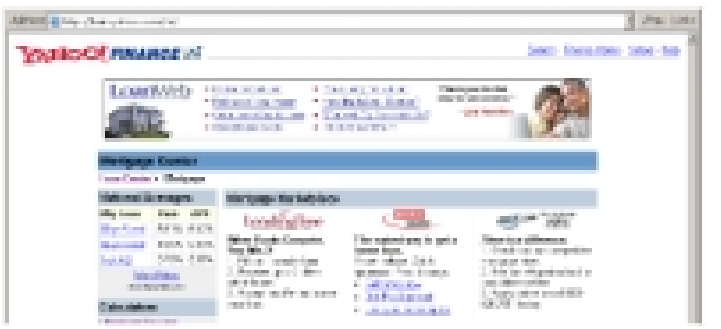
Cookie Management

- Cookie Ownership
  - Once a cookie is saved on your computer, only the Web site that created the cookie can read it.
- Variations
  - Temporary cookies
    - Stored until you quit your browser
  - Persistent cookies
    - Remain until deleted or expire
  - Third-party cookies
    - Originates on or sent to another Web site

Third-Party Cookies

- Yahoo! Privacy Center
  - Yahoo! sends most of the advertisements you see
  - However, we also allow ... third-party ad servers ... to serve advertisements
  - Because your web browser must request these ... from the ad network web site, these companies can send their own cookies to your cookie file ...
  - **Opting Out of Third-Party Ad Servers**
    - "If you want to prevent a third party ad server from sending and reading cookies on your computer, currently you must visit each ad network's web site individually and opt out (if they offer this capability)."

Example: Mortgage Center



```
<html><title>
Mortgage Center
</title><body>
... http://www.loanweb.com/ad.asp?ILID=db75at1ep0k9
```

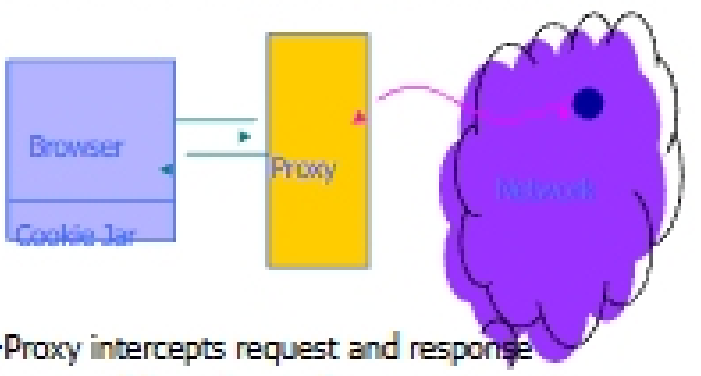
Cookie issues

- Problems
  - Cookies maintain record of your browsing habits
    - May include any information a web site knows about you
  - Sites can share this information (e.g., doubleclick)
  - Browser attacks could invade your "privacy"

    08 Nov 2000

    Users of Microsoft's browser and e-mail programs could be vulnerable to having their browser cookies stolen or modified due to a new security bug in Internet Explorer (IE), the company warned today.

Managing cookie policy via proxy



- Proxy intercepts request and response
- May modify cookies before sending to Browser
- Can do other checks: filter ads, block sites, etc.

Sample Proxy: JUNKBUSTERS

- Cookie management by policy in *cookiefile*
  - Default: all cookies are silently crunched
  - Options
    - Allow cookies only to/from certain sites
    - Block cookies to browser (but allow to server)
    - Send vanilla wafers instead
- Block URLs matching any pattern in *blockfile*
  - Example: pattern /*.*/ad matches http://nomatterwhere.com/images/advert/g3487.gif

Easy to write your own http proxy; you can try it at home

Preserving web privacy

- Your IP address may be visible to web sites
  - This may reveal your employer, ISP, etc.
  - Can link activities on different sites, different times
- Some mechanisms exist to keep sites from learning information about you
  - Anonymizer
    - Single site that hides origin of web request
  - Crowds
    - Distributed solution