Browser Security

John Mitchell

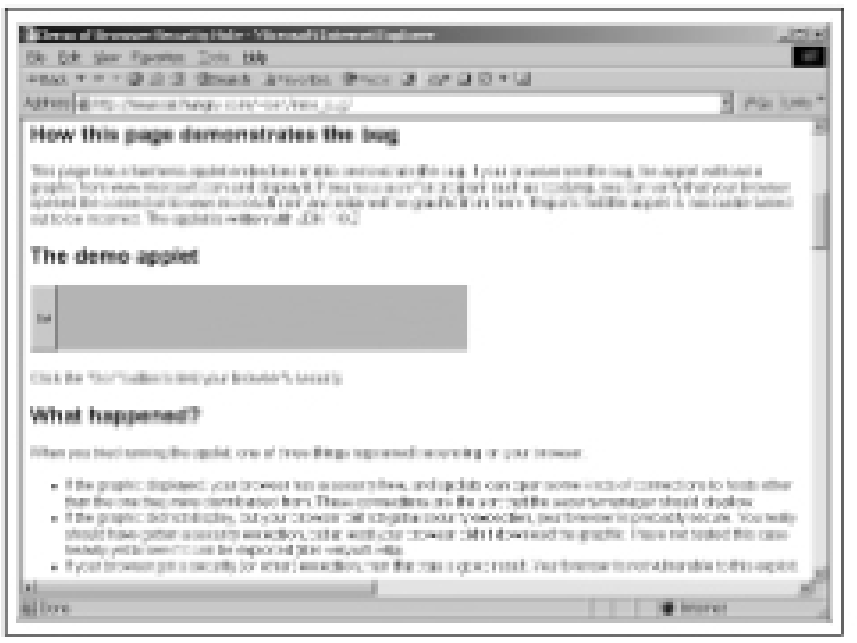
Question from last time: Purify

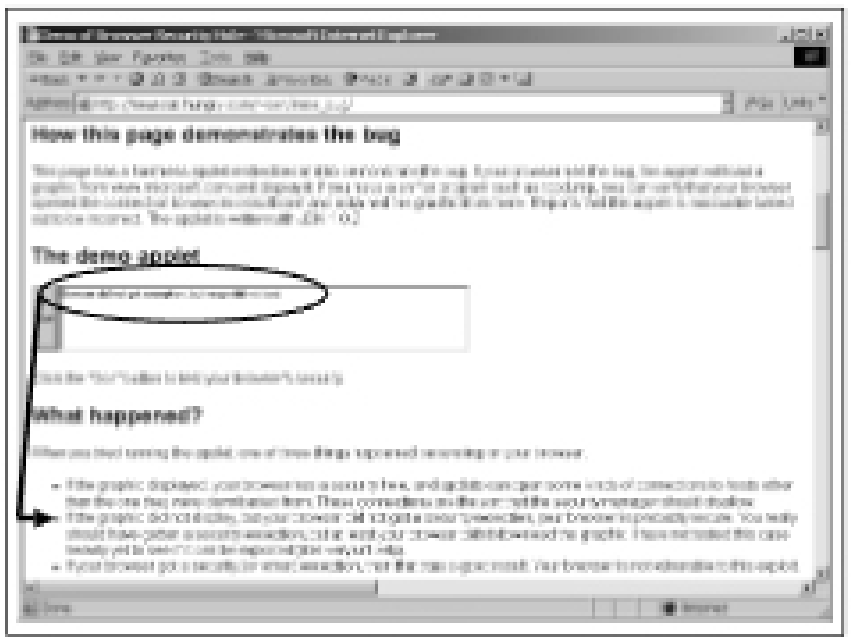
- Goal
  - Instrument a program to detect run-time memory errors (out-of-bounds, use-before-init) and memory leaks
- Technique
  - Works on relocatable object code
    - Link to modified malloc that provides tracking tables
  - Memory access errors: insert instruction sequence before each load and store instruction
  - Memory leaks: GC algorithm

Browser security

- Browser uses network and local disk
  - Potential for outside access to local data
- Brower interprets code from network
  - HTML, JavaScript, ActiveX, Java
- Browser installs, executes plug-ins
  - Acrobat, Shockwave, …
- Malicious code can pose risks
  - Consume resources
  - Steal information
  - Compromise system

A browser is an operating system





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."

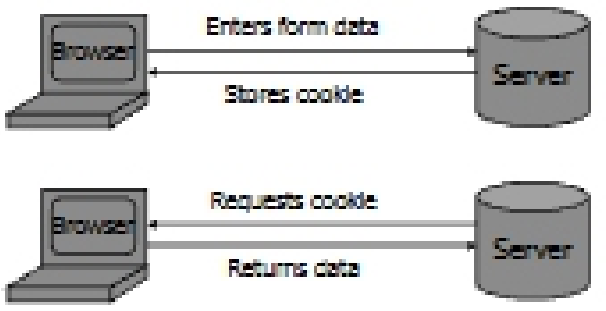
Latest patch addresses:

- 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 ...

Tour of security issues

- Cookies
- JavaScript
- ActiveX
- Java
  - Most of lecture devoted to Java
    - Representative case, more developed security model
- Using a network proxy to increase security
- Plug-ins ?

Cookies



- Http is stateless protocol; cookies add state
  - Other method: modify URL

Cookie issues

- Policy
  - Cookie from site S can be returned to site S *only*
- Problems
  - Cookies maintain record of your browsing habits
  - Sites can share this information (e.g., doubleclick)
  - Attacks could invade your "privacy"

    08 Nov 2001

    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.

JavaScript

- Language executed by browser
- Used in many attacks
  - Cookie attack from last slide:

    With the assistance of some JavaScript code, an attacker could construct a Web page or HTML-based e-mail that could access any cookie in the browser's memory or those stored on disk ...