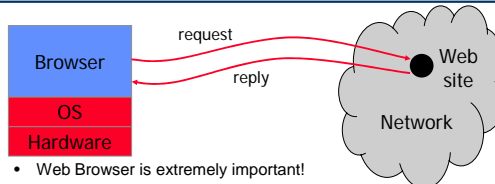


Lecture 5: Browser Security

ECE1776
David Lie

1

Web Browser



- Web Browser is extremely important!
 - The prime method for users to access remote hosts on the internet
 - A great deal of attacks and vulnerabilities involve web browsers



2

Browser and Network

- Browser sends requests
 - May reveal private information (in forms, cookies)
 - Also sends other information that may be damaging:
 - IP address
 - Referring address
 - Browser version/type, screen resolution
- Browser receives information, code
 - May corrupt state by running unsafe code
 - Information may exercise a bug in the browser allowing arbitrary remote code execution
- Susceptible to network attacks
 - Consider network security later in the course



3

How much information is revealed?

IP	User Agent	Referrer
24.188.118.53	Netcape 7	Linux 2
206.74.141.18	MSIE 6	Windows 2000
24.188.118.53	Netcape 7	Linux 2
192.168.1.1	MSIE 6	Windows XP
206.74.141.18	MSIE 6	Windows 2000
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP
192.168.1.1	MSIE 6	Windows XP



4

Browser could also have exploitable vulnerabilities

- A malicious web page could exploit them and cause a variety of problems. A quick search of the CERT vulnerability database:
 - MS Internet Explorer: 4 documented vulnerabilities in 2005
 - One was a buffer overflow in JPEG rendering library
 - Firefox: 9 vulnerabilities:
 - 1 buffer overflow and 1 heap overflow
- Other vulnerabilities include:
 - Execution of Javascript of applets with elevated privileges
 - Failure to restrict access for remotely supplied commands or scripts
 - Insecure object handling, incorrectly displaying information



5

Browser Security Check

Ensure Your Browser Is Secure

The information-like credit card numbers- you share with Web sites is only as safe as your Web browser. Use the Free Browser Check to ensure you've got the latest, most secure Web browser.

With one click, Browser Check instantly tells you:

- What browser and version you're using
- Your browser's encryption strength-standard 40-bit SSL, or 128-bit SSL: the strongest encryption available
- Upgrade recommendations

Current Browser Version:
Microsoft Internet Explorer MSIE 6.0

Recommendation: No Upgrade Required
Your browser supports strong encryption and contains the recommended level of security.

- ✓ **Secure Browsing Support:** Your browser is capable of securely communicating with web site certificates.
- ✓ **Strong Encryption Support:** Your domestic browser currently supports strong encryption: 128-bit SSL sessions.
- ✓ **Digital Certificate Support:** Your browser can utilize personal Digital IDs for secure access control and email.

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

What kind of security are they checking?



6

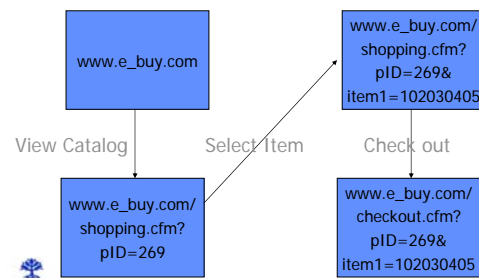
This Lecture: Browser Security

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



7

Browser Session Example: Purchasing Online



http is stateless:
Accumulate state information about session in URL

8

HTTP Protocol

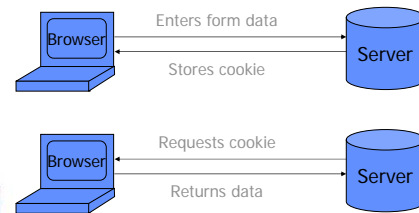
- HTTP is stateless. This causes problems in a lot of transactions that need a concept of a "session":
 - A customer wants to purchase an item online.
 - A customer logs onto their bank to pay bills
 - Sites like Yahoo allow users to customize their view of the portal
- As the user jumps from web page to web page, the server can't keep track of whether it's the same user, or another user requesting the same page



9

Store info across sessions?

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



Cookies add state as well

10

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



11

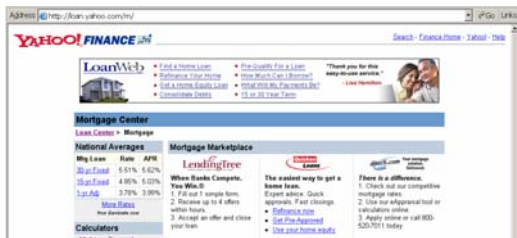
Third-Party Cookies

- Taken directly from Yahoo's Privacy Policy:
 - "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)."



12

Example: Mortgage Center



```
<html><title>
Mortgage Center
</title><body>
... http://www.loanweb.com/ad.asp?RLID=0b70at1ep0k9
```



13

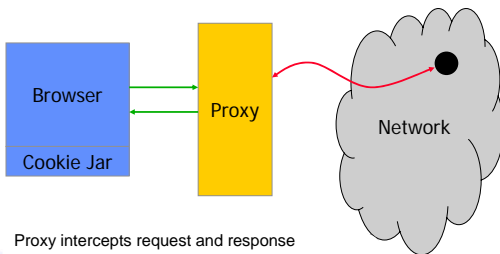
Cookie issues

- Problems
 - Cookies maintain record of your browsing habits
 - May include *any* information a web site knows about you
 - 3rd party cookies can be used to track your habits across *different* web sites
 - Browser 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.
- Not just a privacy issue!
 - Stealing someone’s cookies may allow attacker to impersonate the victim:
 - Cross-site Scripting attacks and session high jacking



14

Solution: 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.



15

Sample Proxy: Privoxy

- There are many privacy enhancing tools out there such as Norton, ZoneLabs, Google and even Yahoo themselves.
- An open source and user configurable one is Privoxy
 - Allows you to specify rules:
 - Rules based on some loose pattern matching, similar to regular expressions
 - Specify actions to either block, pass, or send back a vanilla wafer (empty value) for cookies
 - Can also filter out ads, web bugs
 - web bugs hidden parts of a web page that cause your browser to access a 3rd party web page
 - An example would be a 1 pixel by 1 pixel image
 - Privoxy is very slow, but is a good way to learn



16

Privoxy Example

```
<script language="JavaScript" type="text/javascript">
document.write(<a
href="http://rd.yahoo.com/M=276022.4302192.5600194.17/D=fin/S=38996708:N
/A=1941716/R=1/http://click.atdmt.com/OGI/go/yhfnca600200014ogi/direct/01/
&time=1075013844491207" target="_blank"></a>);
</script><noscript><a
href="http://rd.yahoo.com/M=276022.4302192.5600194.17/D=fin/S=38996708:N
/A=1941716/R=2/http://click.atdmt.com/OGI/go/yhfnca600200014ogi/direct/01/
&time=1075013844491207" target="_blank"></a></noscript></iframe>
Becomes
<p><a
href="http://rd.yahoo.com/M=39122.1678112.3208917.121/D=fin/S=38996708:N
/A=666785/2/http://ca.insurance.yahoo.com/" target="_top"></a>
```



17


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

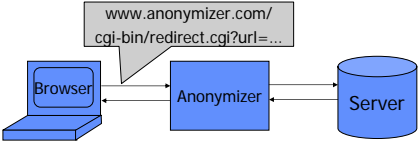


18


Browsing Anonymizers



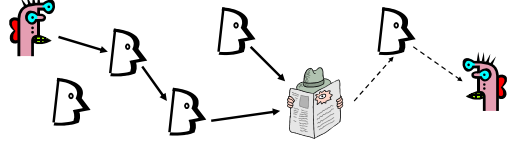
- Web Anonymizer hides your IP address




- But of course you have to trust anonymizer
There is a general solution called crowds...


19

Related approach to anonymity

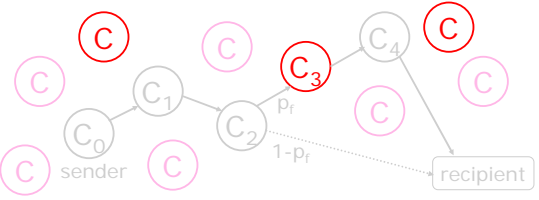


- Hide source of messages by routing them randomly
- Routers don't know for sure if the apparent source of the message is the actual sender or simply another router
- Existing systems: Freenet, Crowds, etc.



20

Crowds

[Reiter, Rubin '98]




- Sender randomly chooses a path through the crowd
- After receiving a message, honest router flips a coin
 - With probability P_r routes to the next member on the path
 - With probability $1 - P_r$ sends directly to the recipient
- Some routers can be honest, some corrupt


21

What Does Anonymity Mean?

- Beyond suspicion
 - The observed source of the message is no more likely to be the actual sender than anybody else
- Probable innocence
 - Probability $< 50\%$ that the observed source of the message is the actual sender
- Possible innocence
 - Non-trivial probability that the observed source of the message is not the actual sender

Guaranteed by Crowds if there are sufficiently few corrupt routers


22


Something you can try at home

(or someone else's machine)

- Find out what sites know about you
 - Anonymizer.com, other sites will tell you what they can find about your IP address
 - Many other sites offer this too ...


www.anonymizer.com

Try **Private Surfing** FREE!
Make your online activities invisible and untrackable to online snoops.
Just type a URL & click "GO."


23

Controlling information from web

- Data is harmless (?)
 - Remember that on van Neumann architectures, data and code are the same
- Risks come from code received from web
 - Scripts in web pages
 - Interpreted by the browser
 - Applets
 - Mobile code that is temporary
 - Interpreted by some other application (JVM)
 - Plug-ins (realplayer, flash, etc....)
 - Usually installed as applications and are called by browser
 - Run with full permissions of user


24

JavaScript

- Language executed by browser
- Used in many attacks (to exploit other vulnerabilities)
 - Cookie attack (08 Nov 2001):
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 ...
- JavaScript runs
 - Before the HTML is loaded, before the document is viewed
 - While the document is viewed, or as the browser is leaving



25

ActiveX

- ActiveX controls reside on client's machine, activated by HTML object tag on the page
 - ActiveX controls are not interpreted by browser
 - Compiled binaries executed by client OS
 - Can be downloaded and installed
- Security model relies on three components
 - Digital signatures to verify source of binary
 - IE policy can reject controls from network zones
 - Controls marked by author as *safe for initialization*, *safe for scripting* which affects the way control used

Once accepted, installed and started, no control over execution !



26

Installing Controls



If you install and run, no further control over the code.

In principle, browser/OS could apply sandboxing, other techniques for containing risks in native code.



27

Risks associated with controls

- MSDN Warning
 - An ActiveX control can be an extremely insecure way to provide a feature.
- Why?
 - A COM object, control can do any user action
 - read and write Windows registry
 - access the local file system
 - Other web pages can attack a control
 - Once installed, control can be accessed by any page
 - Page only needs to know class identifier (CLSID)
- Recommendation: use other means if possible

<http://msdn.microsoft.com/library/default.asp?url=/workshop/components/activex/security.asp?frame=true>



28

Browser Helper Objects (Plug-ins)

- COM components loaded when IE starts up
- Run in same memory context as the browser
- Perform any action on IE windows and modules
 - Detect browser events
 - GoBack, GoForward, and DocumentComplete
 - Access browser menu, toolbar and make changes
 - Create windows to display additional information
 - Install hooks to monitor messages and actions
- Firefox has a very similar plug-in facility
 - Summary: No protection from plug-ins

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebgen/html/bho.asp>



29

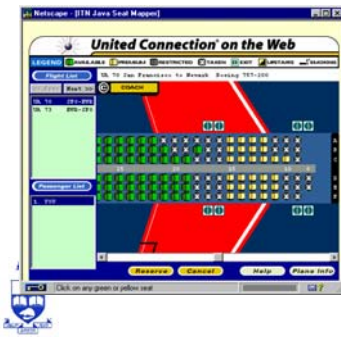
Java

- Java is general programming language
- Web pages may contain Java code
- Java executed by Java Virtual Machine
 - Special security measures associated with Java code from remote URLs
- Usually used to execute mobile code



30

Java Applet



- Local window
- Download
 - Seat map
 - Airline data
- Local data
 - User profile
 - Credit card
- Transmission
 - Select seat
 - Encrypted msg

31

Mobile code security mechanisms

- Examine code before executing
 - Java bytecode verifier performs critical tests
- Interpret code and trap risky operations
 - Java bytecode interpreter does run-time tests
 - Security manager applies local access policy
- Beyond the Browser: code modification
 - Replace standard calls by calls to "safe" versions
 - Check parameters to standard methods to make sure they are in appropriate ranges



- Because of type safety, attacks like buffer overflows are not possible in Java, you data and code are different "types"

32

How do we know verifier is correct?

- If there is an error in the verifier, an attacker could exploit that to run unsafe code
 - Many early attacks based on verifier errors
 - Adversary can coerce VM to do something unsafe
- Formal verification studies prove correctness
 - Abadi and Stata
 - Freund and Mitchell
 - Found error in initialize-before-use analysis



33

Java Security Mechanisms

- In addition to verifying byte code:
- Sandboxing
 - Run program in restricted environment
 - Analogy: child's sandbox with only safe toys
 - This term refers to
 - Features of loader, verifier, interpreter that restrict program
 - Java Security Manager, a special object that acts as access control "gatekeeper"
- Code signing
 - Use cryptography to determine who wrote class file
 - Info used by security manager



34

Java Sandbox

- Four complementary mechanisms
 - Class loader
 - Separate namespaces for separate class loaders
 - Associates *protection domain* with each class
 - Verifier and JVM run-time tests
 - NO unchecked casts or other type errors, NO array overflow
 - Preserves private, protected visibility levels
 - Security Manager
 - Called by library functions to decide if request is allowed
 - Uses protection domain associated with code, user policy
 - Enforcement uses stack inspection



35

Security Manager

- Java library functions call security manager
- Security manager object answers at run time
 - Decide if calling code is allowed to do operation
 - Examine protection domain of calling class
 - Signer: organization that signed code before loading
 - Location: URL where the Java classes came from
 - Uses the system policy to decide access permission
- The security manager is user configurable



36

Beyond JVM security

- JVM does not prevent
 - Denial of service attacks
 - Applet creates large windows and ignores mouse
 - Certain network behavior
 - Applet can send unauthorized e-mail or forge email (on some implementations)
 - URL spoofing
 - Applet can write false URL on browser status line
 - Annoying behavior
 - Applet can play loud sound, or display images
 - Applet can reload pages in new windows



37

Summary: Browser security

- Because Browser is often the primary point of contact with the Internet, it poses several security risks:
 - May damage user's privacy through cookies or web bugs
 - Mobile Code in the form of plug-ins, controls or scripts may allow unauthorized access to system resources
- Solutions usually involve using a sandbox or a proxy that filters content
 - The difficulty usually involves configuring a policy that is safe, but not too restrictive

We'll see many of these issues in other forms when we discuss OS security, network security



38