



Computer Security

Web Privacy and Security for Users

March 30, 2004

©2004, Bryan J. Higgs

1

Privacy

priva·cy

- 1 **a** : the quality or state of being apart from company or observation : seclusion
- b** : freedom from unauthorized intrusion
<one's right to *privacy*>
- 2 *archaic* : a place of seclusion
- 3 **a** : secrecy¹ **b** : a private matter : secret

¹However, note that current definitions of privacy do *not* consider *private* and *secret* to be synonyms, especially in the context of the Internet.

2

What is Private Information?

- Garfinkel¹ suggests the following categories of personal information:
 - Personal Information
 - Your name, date of birth, parents' names, etc.
 - Private Information
 - Personal information that is not generally known.
 - Sometimes protected by law (e.g. educational records, bank records)
 - Lots of other information is not protected
 - Social Security Numbers (although they are available in many databases)
 - Personally Identifiable Information
 - Information from which a person's identity can be derived
 - Example: a person's account number
 - Anonymized Information
 - The reverse of personally identifiable information.
 - Aggregate Information
 - Statistical information combined from several individuals -- e.g. [Census tract information](#)

¹*Web Security, Privacy & Commerce*, Simson Garfinkel, O'Reilly

3

Triangulation

- You might be surprised at how much information may be gained from so little. For example, assume you entered information into a web site that was merely your **ZIP code** and your **date of birth**. How likely is it that you could be identified from that amount of information?
 - There are (as of March 28th, 2004) ~ [292,897,151](#) people in the US.
 - The number of distinct birthdays is **365.25** (taking into account leap years)
 - The number of people in the US with each birthday = **292,897,151 / 365.25** or nearly **802,000** people
 - The total number of ZIP codes in the US = approximately **100,000**
 - So, the number of people in each ZIP code with the same birthday = **802,000 / 100,000 = about 8 people.**

This assumes an even distribution of birthdays throughout the year, and that people are evenly distributed throughout ZIP code areas, but it's still a reasonable approximation.

4

Web Privacy

- It is, in fact, very difficult to maintain your privacy when you go onto the Web. Do you realize:
 - When you log into a web site using an account id and password your account id and your password may or may not be securely passed?
 - What information is passed to each web server you visit?
 - What information is passed between your browser and that web server?
 - What cookies are being set/passed, what they contain, and for what purpose they are being used?
 - Every web server will log information about your visit?
 - Each web site has its own, different, privacy policy?
 - Many of your browser activities are being captured by web sites that are looking to determine your patterns, likes and dislikes?
 - That your browser caches information from your web browsing sessions?

5

HTTP is a Request/Response Protocol

- Here's a request from a browser (Microsoft Internet Explorer V6) for a very simple page:

```
GET http://www.rivier.edu/faculty/bhiggs/web/cs572aweb/Tools/VerySimplePage.htm HTTP/1.0
Accept: */*
Accept-Language: en-us
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; YComp 5.0.2.4)
Host: www.rivier.edu
Proxy-Connection: Keep-Alive
```

6

HTTP is a Request/Response Protocol

- And here is the server's response:

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Content-Location: http://www.rivier.edu/
X-Powered-By: ASP.NET
Date: Tue, 30 Mar 2004 03:21:41 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Tue, 30 Mar 2004 03:10:42 GMT
ETag: "065ac95416c41:999"
Content-Length: 263
```

```
<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>Simple Web Page</title>
</head>
<body>
<p>This is a very simple web page.</p>
</body>
</html>
```

[Try it!](#)

7

A Single Web Page Involves Many Requests/Responses

- That was a simple page. But in more realistic web pages, there are many components to request:
 - The HTML page itself
 - Any images it contains
 - Any other components that it contains

8

A Multi-Element Web Page

- Here's an HTTP request to obtain a slightly more complex web page:

```
GET
  http://www.rivier.edu/faculty/bhiggs/web/cs572aweb/Tools/SimplePageWithImage.htm HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg,
  image/pjpeg, application/vnd.ms-excel,
  application/vnd.ms-powerpoint, application/msword,
  application/x-shockwave-flash, */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
  Windows NT 5.0; YComp 5.0.2.4)
Host: www.rivier.edu
Proxy-Connection: Keep-Alive
```

9

A Multi-Element Web Page

- Here's the response to this request (notice that it contains an `` tag):

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Content Location: http://www.rivier.edu/
X-Powered-By: ASP.NET Date: Tue, 30 Mar 2004 20:28:52 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Tue, 30 Mar 2004 20:26:56 GMT
ETag: "0e843589516c41:999"
Content-Length: 478

<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>A simple page with an image</title>
</head>
<body>
<h1>A simple page <i>with an image</i></h1>
<p></p>
</body>
</html>
```

10

A Multi-Element Web Page

- Now, the browser has to obtain the image in order to display it, so it makes another HTTP request:

```
GET
  http://www.rivier.edu/faculty/bhiggs/web/cs572aweb/images/Ringmaster.gif HTTP/1.0
Accept: */*
Referer:
  http://www.rivier.edu/faculty/bhiggs/web/cs572aweb/Tools/SimplePageWithImage.htm
Accept-Language: en-us
Proxy-Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
  Windows NT 5.0; YComp 5.0.2.4)
Host: www.rivier.edu
```

11

A Multi-Element Web Page

- The response to this is:

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Content Location: http://www.rivier.edu/
X-Powered-By: ASP.NET
Date: Tue, 30 Mar 2004 20:28:53 GMT
Content-Type: image/gif
Accept-Ranges: bytes
Last-Modified: Tue, 30 Mar 2004 20:26:56 GMT
ETag: "0e843589516c41:999"
Content-Length: 7523
...
```

[Give it a try!](#)

12

One Web Page = Many Requests/Responses

- Did you notice how absolutely simple that web page was?
- Now compare that with the typical web page today – there's no comparison!
- Note also:
 - Elements in a web page do not all have to come from the same web site / domain.
 - In fact, most pages that contain advertising images (and other elements) contain elements that come from a potentially large number of web sites, all of which want to learn something about your browsing habits!

13

Web Bugs

- No, Web Bugs are not program bugs; they are tiny images (usually 1 pixel in size, and so visually undetectable) which are obtained from a third party web site.
- Here's an example:
 - <http://www.rivier.edu/faculty/bhiggs/web/cs572aweb/Tools/WebBugPage.htm>

14

Web Bugs

- When I visited that page, there were two requests:

```
GET http://www.rivier.edu/faculty/bhiggs/web/cs572aweb/Tools/WebBugPage.htm
HTTP/1.0
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg,
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword,
application/x-shockwave-flash, */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; YComp 5.0.2.4)
Host: www.rivier.edu
Proxy-Connection: Keep-Alive
```

and:

```
GET http://ad.doubleclick.net/ad/pixel.quicken/NEW HTTP/1.0
Accept: */*
Referer:
http://www.rivier.edu/faculty/bhiggs/web/cs572aweb/Tools/WebBugPage.htm
Accept-Language: en-us
Proxy-Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; YComp 5.0.2.4)
Host: ad.doubleclick.net
Cookie: id=800002b3d84368
```

15

Web Bugs

- Web Bugs can also be present in:
 - HTML-based email messages
 - Microsoft Word documents
 - Usenet messages
- For more information on Web Bugs, see:
 - http://www.eff.org/Privacy/Marketing/web_bug.html
 - <http://www.spywareinfo.com/articles/webbugs/>
 - <http://www.bugnosis.org/>
 - <http://www.leave-me-alone.com/webbugs.htm>

16

"Private Information" Passed via Your Browser

- Here's an example of how much information is passed when you browse to a web page – especially one which asks for your username and password:

<http://www.rivier.edu/faculty/bhiggs/web/cs572aweb/Tools/Login.htm>

17

Web Server Logs

- Every web server logs information about visitors to its web site(s) in a **web log file** (not to be confused with a WeBlog, aka "Blog"). Typical information recorded is:
 - The name and IP address of the computer that downloaded the web page
 - The time of the request
 - The URL that was passed
 - The time it took to download the file
 - If HTTP authentication was used, the username of the user who downloaded the file
 - Any errors that occurred
 - The previous web page that was downloaded by the web browser (called the *refer link*)
 - The kind of web browser that was used.

18

Web Server Logs

- A web log entry that uses **Common Log Format** will look like:

```
host/ip rfcname logname [DD/MMM/YYYY:HH:MM:SS -0000]
"METHOD /PATH HTTP/1.0" code bytes
```

where:

host/ip	The hostname or IP address of the client
RFC name	A name from the remote server for the user. If no value is present, a "-" is substituted.
logname	If you're using local authentication and registration, the user's log name will appear; otherwise, "-" is substituted.
timestamp	The timestamp of the request
retrieval	Method (GET, PUT, POST, or HEAD); path is the path and file retrieved; HTTP/1.0 defines the protocol.
code	HTTP completion code. 200 is successful, 304 is a reload from cache, 404 is file not found, etc.
bytes	number of bytes in file retrieved.

- For more information about Web Log Analysis, see:

http://www.webdeveloper.com/management/management_log_analysis.html

19

RADIUS Logs

- RADIUS (Remote Authentication Dial-In User Service) is used by many ISPs and large organizations to validate usernames/passwords for dial-up users and for accounting.
- Widely implemented by Cisco, Nortel, Lucent, etc.
- Here's an example of a RADIUS log file entry:

```
Sun Mar 18 04:35:24 2001
Acct-Session-Id = "06000004"
User-Name = "admin"
NAS-IP-Address = 192.168.1.5
Acct-Status-Type = Start
Acct-Authentic = Local
Service-Type = Administrative-User
Login-Service = Telnet
Login-IP-Host = 192.168.1.1
Acct-Delay-Time = 75
Timestamp = 984918924
Request-Authenticator = Verified
```

20

Mail Logs

- Mail messages are often logged on various email servers.
- Here's an extract from a sendmail log:

```
Nov 7 09:00:25 imrldmz1 sendmail[849]: [ID 801593 mail.info]
fa7800u00847: to=<je@orangemail.ch>, delay=00:00:01,
xdelay=00:00:00, mailer=esmtplib, pri=128178,
relay=smtp.orangemail.ch. [192.168.20.4], dsn=2.0.0,
stat=Sent (Message received: GMF6WR00.DUH)
Nov 7 09:00:41 imrldmz1 sendmail[864]: [ID 801593 mail.info]
fa780fu00864: from=<bidconfirm@ebay.de>, size=1975, class=0,
nrpts=1, msgid=<200111070804.fA7848u20675@damar.ebay.com>,
proto=SMTP, daemon=MTA, relay=miles.ebay.com [216.33.156.140]
Nov 7 09:00:42 imrldmz1 sendmail[866]: [ID 801593 mail.info]
fa780fu00864: to=<searles-daniel@orangemail.ch>,
delay=00:00:01,
xdelay=00:00:00, mailer=esmtplib, pri=121975,
relay=smtp.orangemail.ch.
[192.168.20.2], dsn=2.0.0, stat=Sent (Message received:
GMF7V600.IJK)
```

21

DNS

- The **Domain Name System (DNS)**, is a core feature of the Internet. It is a distributed database that handles the mapping between host names (**domain names**), which are more convenient for humans, and the numerical IP address, which a computer uses.
 - For example, the hostname **net.rivier.edu** maps to the IP address **[198.112.92.2]**
- A DNS name server can be configured to log every DNS query that it receives.

22

Cookies

- What is a cookie?
 - A piece of information sent by a Web server to a user's browser
 - The browser saves the information, and sends it back to the Web server every time the browser returns to that Web site.
 - Cookies were invented by Netscape, and introduced with Netscape Navigator 2.0
 - The preliminary cookie specification may be found at http://wp.netscape.com/newsref/std/cookie_spec.html
 - RFC 2965 may be found at <http://www.faqs.org/rfcs/rfc2965.html> but it is not clear that the RFC has been finalized/accepted.

23

Cookie Applications

- Why are cookies needed?
 - HTTP is a stateless protocol, but many web sites need to maintain state across many HTTP requests
 - Typical applications include:
 - To implement a "shopping cart" at sites such as amazon.com
 - To identify a user so that web sites can show user-specific information such as local news, weather, etc. This is often done at so-called **portals**.

24

Web Server Sending a Cookie

- A web server sends a cookie to a client's browser by including a **Set-Cookie** header in its HTTP response. For example:

```
set-cookie: RMID=c6705c8640699080;  
expires=Fri, 31-Dec-2010 23:59:59 GMT;  
path=/; domain=.internet.com
```

25

Contents of a Cookie

- The header contains a number of **name=value** pairs, including some special ones:
 - **expires=<time>**
 - Specifies when the cookie will expire.
 - If no expiration time is specified, the cookie is a *session cookie*
 - It is not written to disk, and lasts only as long as the current session
 - If an expiration time is specified, the cookie is a *persistent cookie*
 - It is written to disk, and will be passed on any subsequent request made to that web site.
 - **domain=<domain-name>**
 - Specifies which domain to send the cookie to (i.e. computers within that domain)
 - **path=<path>**
 - Specifies which path within the web site should be sent this cookie
 - **secure (no value)**
 - Specifies that this cookie should only be sent via SSL
 - It is still stored unencrypted in your browser's cookie storage

26

Browser Sending a Cookie

- The browser will send a cookie to a web site to which it is making a request, based on the attributes specified in the cookie. Here is a real example:

```
GET  
http://ad.doubleclick.net/adj/N3390.yahoo.com/B1311421.19;abr=!ie;sz=300x250;d  
copt=rcl;click=http://rd.yahoo.com/SIG=1287t229n/M=290987.4769227.5915455.135  
4091/D=mail/S=150500014:LREC/EXP=1080749117/A=2069371/R=1/*;ord=1080662717251  
677? HTTP/1.0  
Accept: */*  
Referer: http://us.f612.mail.yahoo.com/ym/login?.rand=419ck88julii0  
Accept-Language: en-us  
Proxy-Connection: Keep-Alive  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; YComp 5.0.2.4)  
Host: ad.doubleclick.net  
Cookie: id=8000002b3d84368
```

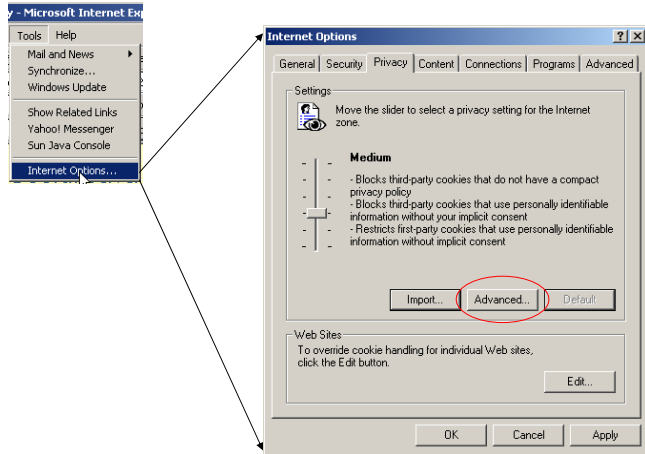
27

How Do You Control Cookies?

- Most browsers, by default, have far too lax control over cookies.
- Once you change the settings of your browser to ask when it should send a cookie to a site, you will be amazed at how many cookies are being exchanged, and with which web sites!
- Each browser has a different way to change cookie behavior...

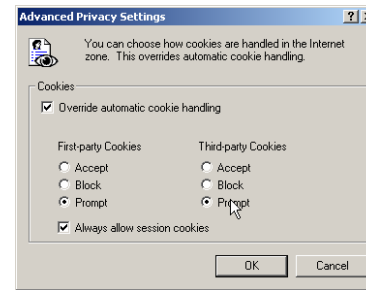
28

Microsoft Internet Explorer Cookie Control



29

Microsoft Internet Explorer Cookie Control



Specifies that you do not want Internet Explorer to use a Web site's P3P privacy policy to determine whether or not to allow the Web site to save a cookie on your computer. If you select this check box, you must specify below how you want Internet Explorer to handle first-party and third-party cookies.

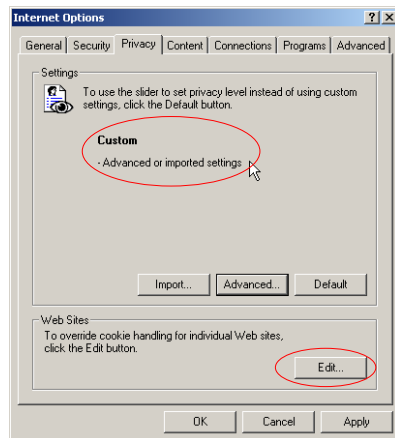
A cookie is a file created by a Web site that stores information on your computer, such as your preferences when visiting that site. A first-party cookie is one that either originates on or is sent to the Web site you are currently viewing. A third-party cookie is one that either originates on or is sent to a different Web site than the one you are currently viewing.

For more information about cookies, see Internet Explorer Help.

- P3P Privacy Policy:
 - <http://www.w3.org/P3P/>
 - <http://msdn.microsoft.com/library/default.asp?url=/workshop/security/privacy/overview/createprivacypolicy.asp>

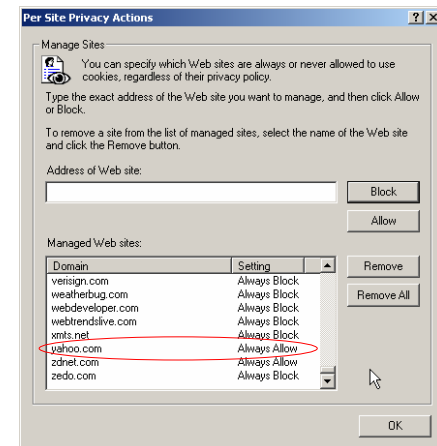
30

Microsoft Internet Explorer Cookie Control



31

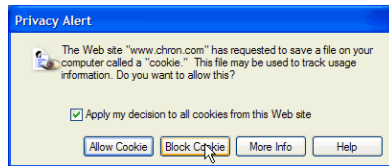
Microsoft Internet Explorer Cookie Control



32

Microsoft Internet Explorer Cookie Control

- Once you've changed the cookie behavior, you'll see lots of dialogs like:



- Initially, you'll see lots of them whenever you are in Microsoft Internet Explorer (and also some when you're in Microsoft Outlook [Express] !)
- If you check the "Apply my decision to all cookies from this Web site" checkbox, and click on the Block Cookie button, then gradually, you'll see fewer and fewer of them.
- I've found this to be a revelation in terms of how many cookies are set on my browser, and by whom!

33

Cookie Content Usage

- A cookie can be used in basically two ways:
 - A web site can use a cookie to contain the user's actual data
 - The cookie can contain a key into the web site's database
- Here's an example of a request that uses a session cookie (Yahoo! email). Which type do you think it is?

```
GET http://us.f612.mail.yahoo.com/lib_web/pulldowns.js HTTP/1.0
Accept: /*
Referer: http://us.f612.mail.yahoo.com/ym/ShowFolder?YY=74354&box=Inbox&YN=1
Accept-Language: en-us
Proxy-Connection: Keep-Alive
If-Modified-Since: Wed, 09 Jul 2003 22:28:35 GMT
If-None-Match: "bc40a1-3462-3f0c9711"
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; YComp 5.0.2.4)
Host: us.f612.mail.yahoo.com
Cookie: B=619m9j4v1cc8e&b=2; Q=q1=ACAAAAAAbw--6q2=P6aGog--; Cmg=1;
Umt= Nah02ZmHyt51q7jI9QLDR8bED16yVah6BA--4ux=OXIaBsun=0cf6mp6secto;
Fw=6nb4Vq6mVnL.HUEB10YFMme30LHxyogUKR4VwW92dAw=Jed8Wk7wy2AYOTib=saP1; CPv=500lbr=1;
Yw=1sn0cf6mp6secto1m41bo142kh4/csp=2602vk213000500&jb=241681&r=ck61gus&intl=us&np=1;
Tz=egZaB6vuaABh0geAXL51APMTY1BjY1NzExNk5PTzU-
&=YAEsk=DAOKd21uv5oU.sd=c2w8mpFeUFURX1NRfkyTVRrNE9ESS0BYQF2QUUbb2sBw1cwlQf0aXABR0IWEEDAXp6ATzxWmFb
QmXQ0--?
YM.Gen=i=vaJ46U81CyUC6SohqziJVP01rSKYKjdtidT31QJrzneEKKH5YDK7bS1g6hjhuyAbIj2os0H61ti2DfrzP_q3g39ys1lfr
JQhGeiB5pd_y1VMTCa7UDQw_2RMJ4wxkzKm8thdxEG7UDmnT87vMlctEchpQ8Cx9dRdtDgtLPzTr2L3kd2pB1ziz1_QV3H5lLr
2F8hVX5oW1hjyqsdcaJLEy8x7ur34veJHKWJ1Dy8m9vcp1eF1lbdz&_jsH1DeV8N90cmadF1Q3DoIfsJec1e84-cwK5
rcjxu0WbT0iY81K2cVHMW54ud6gc6oeAyOd10mh4FM_tMzm76BpgFk1S9bvp.VQ_U_yVrJ0s0asp23Ct75cxPFVM_sBngCbXb0inu
QWzrhhu44_bEca.haoEG.v.EcRpiF_mC5Xeb1EJevvV1DE41Xdjd0D6YvXkc.qaR5TLwJu07Bu1ByKX00Ghai0fzVtJ0mC8Eues
fy04DcLke66kxhdjfoaotd3Tfv1KlaEMg_Qc50uzShhNqnykyvzBbs6_gacV8gCdeH0Jm5-dm2b5WNB_baB111TWJGwNAT;
4I6C2x7Hgy_gcV46DeRe13dPc1e591Fmyou7e_FWRIZ8uTSXKreVosU2OQDOuXds61_CwYI30cxY4s201KP02Epp0Qfw3xhecAMa1.N
bYpFhn0KjyqgPzFKLr6nwuxd9tc9uherAtvJcTXEu47qjb.vUFH1dQrD84-&v=1
```

34

Cookie Content Usage

- What if the cookie looked like:
Cookie: USER=bryan PASSWORD=myfavoritepassword
?
- In general, cookies can:
 - keep data on the client's computer
- OR:
 - keep data on the web site's computer

35

Current Cookie Practices

- Today, one of the most popular uses for cookies is to give a permanent identification number to each user, to measure the number of visitors to a web site. Advertising!
- Many advertisers use cookies to build comprehensive *profiles* of web users, via banner ads.
 - A profile might show that a particular user is interested in sports, entertainment, camcorders, whatever.
 - Even though profiles are supposed to be anonymous, sufficient cross-indexing across multiple profiles and registration information can cause a user to be identified

36

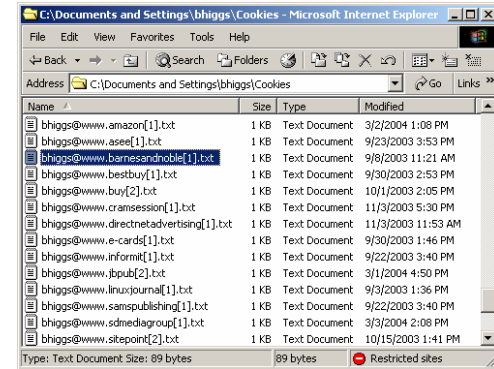
Finding Cookies in Microsoft Internet Explorer

- MS Explorer maintains its cookies in a directory, one file per cookie.
- The directory is found from the registry entry:

```
\HKEY_CURRENT_USER\Software\Microsoft\Windows\  
CurrentVersion\Explorer\User Shell Folders\Cookies
```

37

Finding Cookies in Microsoft Internet Explorer



38

Cookie Security

- Users can modify the contents of cookies
- Thus, it is unwise for a web site to trust the contents of a cookie
- Apparently, there was one real case where a web site used cookies to store information about items placed in the web site's "shopping cart".
 - The cookie's contents included the price charged for each item, which the web site trusted to be accurate.
 - A user modified the cookie, lowering the prices in the cookie, and thus managed to obtain goods very inexpensively.

39

Browser Cache

- Each browser maintains a **browser cache** which helps dramatically improve browsing performance.
- The browser cache contents can become a security issue, if they contain sensitive information (they are stored in plaintext format)

40

Browser History

- Browsers also keep track of recently visited URLs over a recent period.
- Often used to allow browsers to implement automatic *completion* of user-entered URLs
- Again, the history can become a sensitive area, especially when the URLs include search strings, account names, and the like.

41

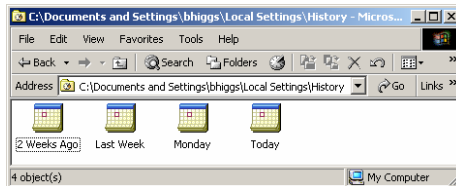
Microsoft Internet Explorer Browser History

- MS Explorer maintains its history in a directory
- The directory is found from the registry entry:

```
\HKEY_CURRENT_USER\Software\Microsoft\Windows\  
CurrentVersion\Explorer\User Shell Folders\History
```

42

Microsoft Internet Explorer Browser History



- It's wise to delete the browser history in a judicious way.

43

Blocking Ads and Spyware

- **Pop-up ads** have become one of the scourges of the Internet.
 - They are certainly annoyances during your browsing experience!
- **Spyware**, similarly, has become a real annoyance, close to virus proportions.

44

Pop-up Ad Blockers

- One problem MS Internet Explorer is that Microsoft actually has financial agreements with certain companies, which can mean that they are slow/unwilling to modify their browsers to prevent pop-up ads and similar scourges.
- Other browser producers have been more enlightened:
 - Netscape Navigator 7.1 has pop-up blocking built in
 - Mozilla 1.5 has pop-up blocking built in
 - Mozilla Firefox also has pop-up blocking
 - The Avant Browser does too.
 - To see how they compare, see:
 - <http://www.popup-killer-review.com/browser-popup-killer.htm>

45

Pop-up Ad Blockers

- Then there are other solutions to block pop-up ads:
 - Free toolbars from Google, Dogpile, MSN, and Yahoo
 - I've used Google's toolbar with good results: <http://toolbar.google.com/>
 - Many other utilities (do a Google search for "pop-up ad blockers")
 - Even Microsoft is apparently producing a built-in Internet Explorer pop-up blocker in Windows XP Service Pack 2, purported to be shipping in the first half of 2004

46

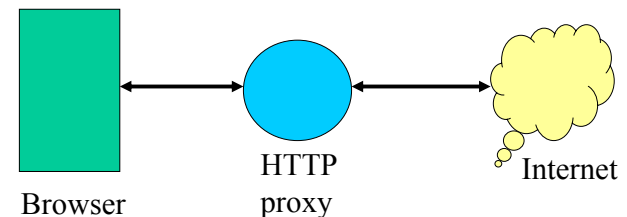
Spyware

- You may not realize how ubiquitous Spyware is.
- Really the only way to find out whether you have spyware on your machine is to get a spyware eliminator program, and run it.
- The best (at least I have had good luck with it) seems to be:
 - [Spybot - Search & Destroy](#)

47

HTTP Proxies

- An **HTTP proxy** acts as an intermediary between your browser and the Internet.



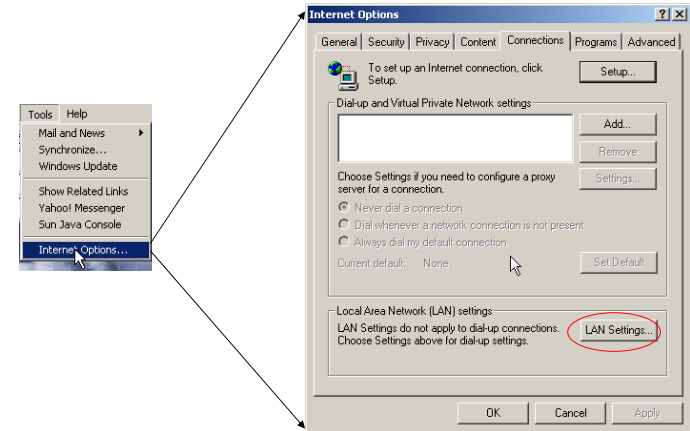
48

HTTP Proxies

- Here are some reasons for installing an HTTP proxy:
 - To **enhance security**, by only allowing a single machine true access to the Internet; all other machines have to use the HTTP proxy.
 - The HTTP proxy can hide information about the other machines.
 - To **enhance network bandwidth**:
 - By limiting which machines can access the Internet
 - By caching commonly-used pages in the HTTP proxy
 - To **control content**:
 - The HTTP proxy can be programmed to make certain sites (such as pornography sites, etc.) inaccessible.
 - Many pop-up ad blockers implement an HTTP proxy to control content in this way.
- Many commercial and free HTTP proxies are available

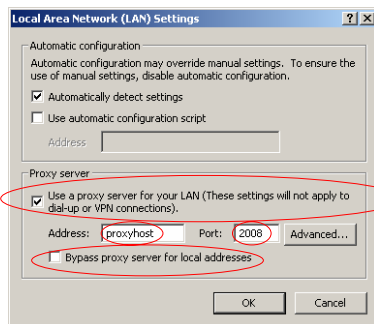
49

Setting up Internet Explorer to Use an HTTP Proxy



50

Setting up Internet Explorer to Use an HTTP Proxy



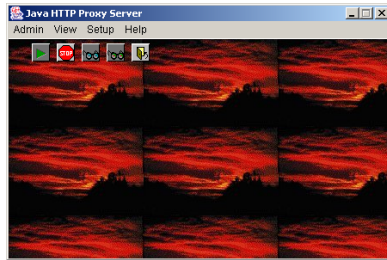
51

Local HTTP Proxies

- One other reason for installing an HTTP proxy is to monitor HTTP traffic and content for learning purposes.
- In this case, you would likely install a Local HTTP Proxy on your own machine.
- There are many available, often free.
 - One I've been using is the [Java HTTP Proxy Server](#) which I've used to capture requests and responses, and generally explore HTTP exchanges.

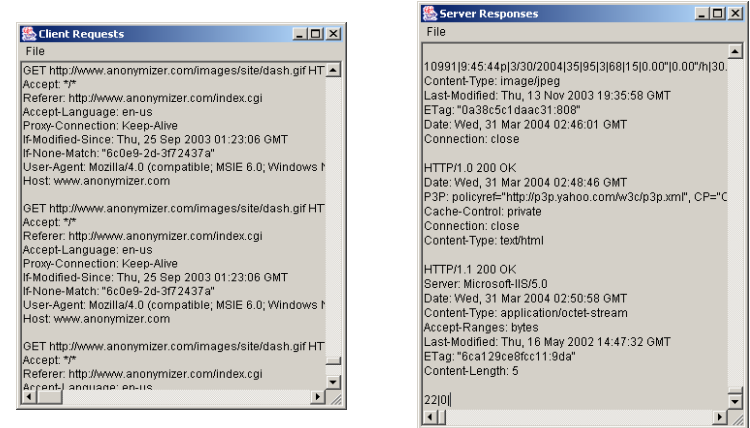
52

Java HTTP Proxy Server



53

Java HTTP Proxy Server



54

Java HTTP Proxy Server

[Let's try a demo!](#)

55

Anonymous Browsing

- When you browse the web normally, you leave tracks behind, and people are watching your every page visit.

"Just because you're not paranoid doesn't mean they're not after you!"

56

Anonymous Browsing

- You can remove some of the information that you would leave behind, by ***browsing anonymously***:
 - Browse from a public terminal at a library
 - But beware Net Nannies and the Patriot Act!
 - Use an ISP that uses a web cache or a proxy server
 - This may, or may not, hide your machine's information
 - Be sure to understand your ISP's privacy policy
 - Use an anonymous web browsing service:
 - Anonymizer.com
 - Freedom
 - Others – do a Google search for " anonymous web browsing "

57

Email Security

- The main email privacy issues are:
 - **–SPAM !**
 - Viruses, worms, Trojan horses, etc.
 - Confidentiality of email contents
- There are other issues, but we won't talk about them here...

58

SPAM

- As we all know, SPAM (with or without viruses) is the number one problem on the Internet, and it's getting worse.
 - You can defend yourself in a number of ways:
 - First, be very careful divulging your email address
 - Have one real, carefully controlled, email address, and other (potentially disposable) ones for entering into web pages, etc.
 - Use a web-based email system, such as Yahoo!, Hotmail, etc.
 - They all have some level of SPAM filtering
 - I use Yahoo!, and like their SPAM filtering
 - Use an anti-SPAM program on your machine
 - For example, Norton Anti-SPAM (<http://www.symantec.com/antispam/>)
 - Most seem to expect Microsoft Outlook or Outlook Express
 - I wasn't impressed with Microsoft Outlook's Junk mail filtering
 - Eudora 6.0 email client (paid-only) has SPAM filtering.

59

Viruses

- If you use a Web-based email service, they usually have anti-virus built in.
 - I use Yahoo! email, and have found their antivirus software to be very effective. Besides, most of the time, you leave messages on the server and never download them unless you need to.
- Regardless, you need to ***practice safe computing***:
 - You really need to run an anti-virus program on your own computer (PCs are the most subject to viruses), and:
 - You need to keep its virus data up to date on nearly a daily basis.
 - I have used Norton AntiVirus, with much success
 - There are even free antivirus programs available
 - I have used [AVG Anti-Virus](http://www.avg.com) with success
 - So there's no excuse for not running an anti-virus program!

60

Email Confidentiality

- When combined with anonymous browsing, web-based email can provide private and nearly untraceable email.
 - I wouldn't trust this against court orders, however...
- You could use PGP with your conventional email (freely downloadable PGP plugs into Microsoft Outlook)
- An interesting option is the use of [Hushmail](#), a web-based email service:
 - Unlike Yahoo!, Hotmail, etc., Hushmail encrypts all email messages passing through its system
 - Even Hushmail can't read your email, so court orders may be impossible to satisfy (although who knows what the Patriot Act might have done to that?)

61

Summary

- Again, we've covered a lot of ground on this topic.
- Web security and privacy is a large set of topics, and I can't claim completeness on the subject, but hopefully you've learned some useful facts and ideas.

62