

Practical Web Privacy with Firefox

Chuck Willis
chuck.willis@mandiant.com

Live-OWASP DC 2007
September 6, 2007



About Me

- Principal Consultant with MANDIANT in Alexandria, VA
 - Full spectrum information security company:
 - Professional Services
 - Government Services
 - Education
 - Software
 - Services include Application Security, Network Security, Incident Response, and Computer Forensics
 - Offices in Alexandria, VA, NYC, and other locations
- Member of OWASP-DC / Maryland Chapter
- See more on my web site www.securityfoundry.com

Privacy on the Web

- Web sites use a variety of techniques to gather data on users
- These techniques can be thwarted with the proper configuration of your web browser
- This presentation will describe information gathering techniques and ways to prevent them using the Firefox web browser
- Emphasis will be on techniques with minimal impact on the web surfing experience

Agenda

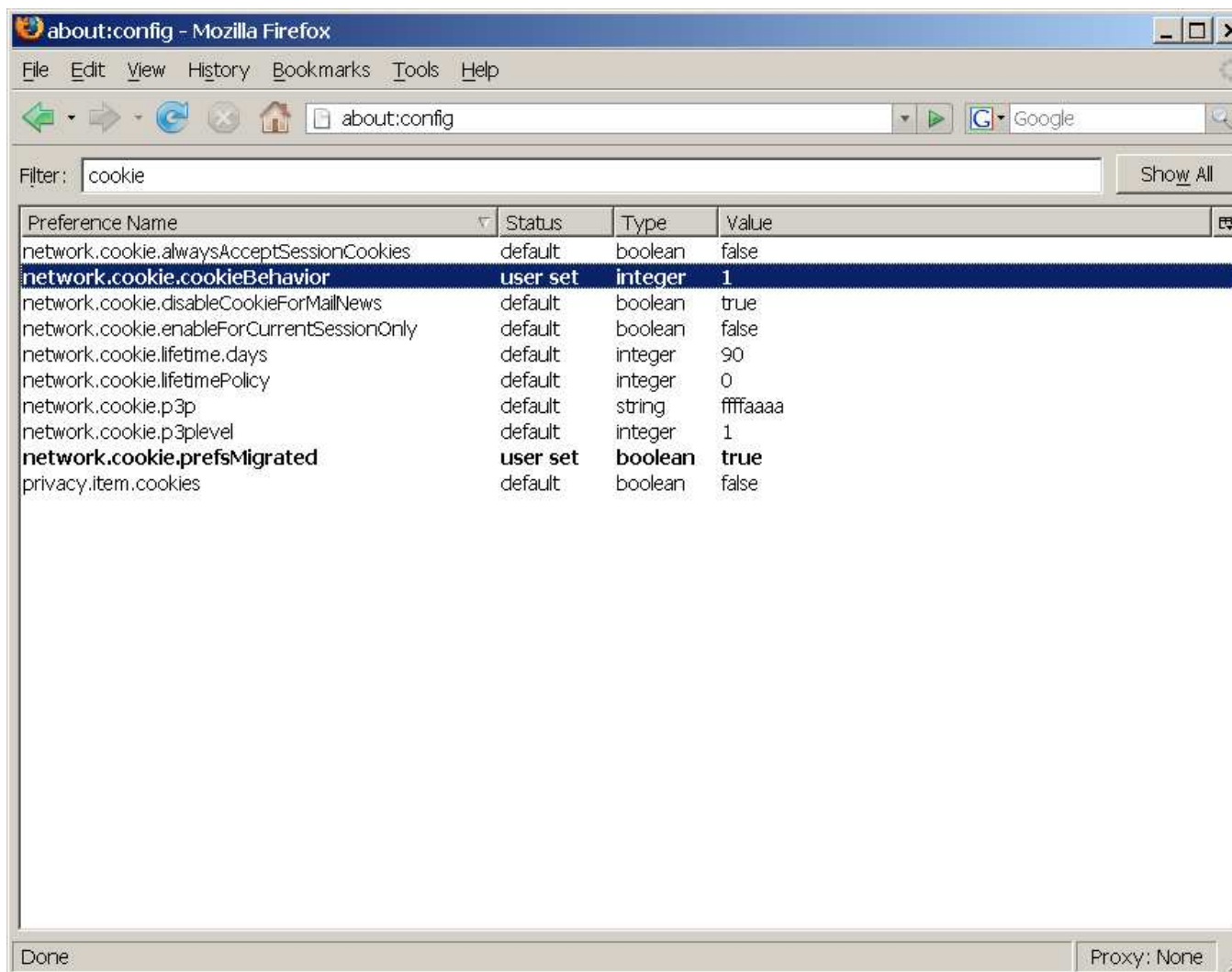
- Cookies
- Scripts and other Active Content
- Referrer Header
- Google
- IP Address Tracking and Geolocation
- History and Cache Snooping
- Site Registrations
- Privacy at a Public Hotspot

Cookies

Third Party Cookies

- Issue: When visiting a web site that imports content from another site, the third party site can set and receive cookies to track users
- Solution:
 - Disable third party cookies
 - This is set by changing Network.cookie.cookieBehavior to 1 in about:config
 - Only the site appearing in the URL will be sent cookies
 - This is the same setting that used to appear in the UI for Firefox 1.5 and below as allowing cookies "for the originating site only"

Firefox about:config



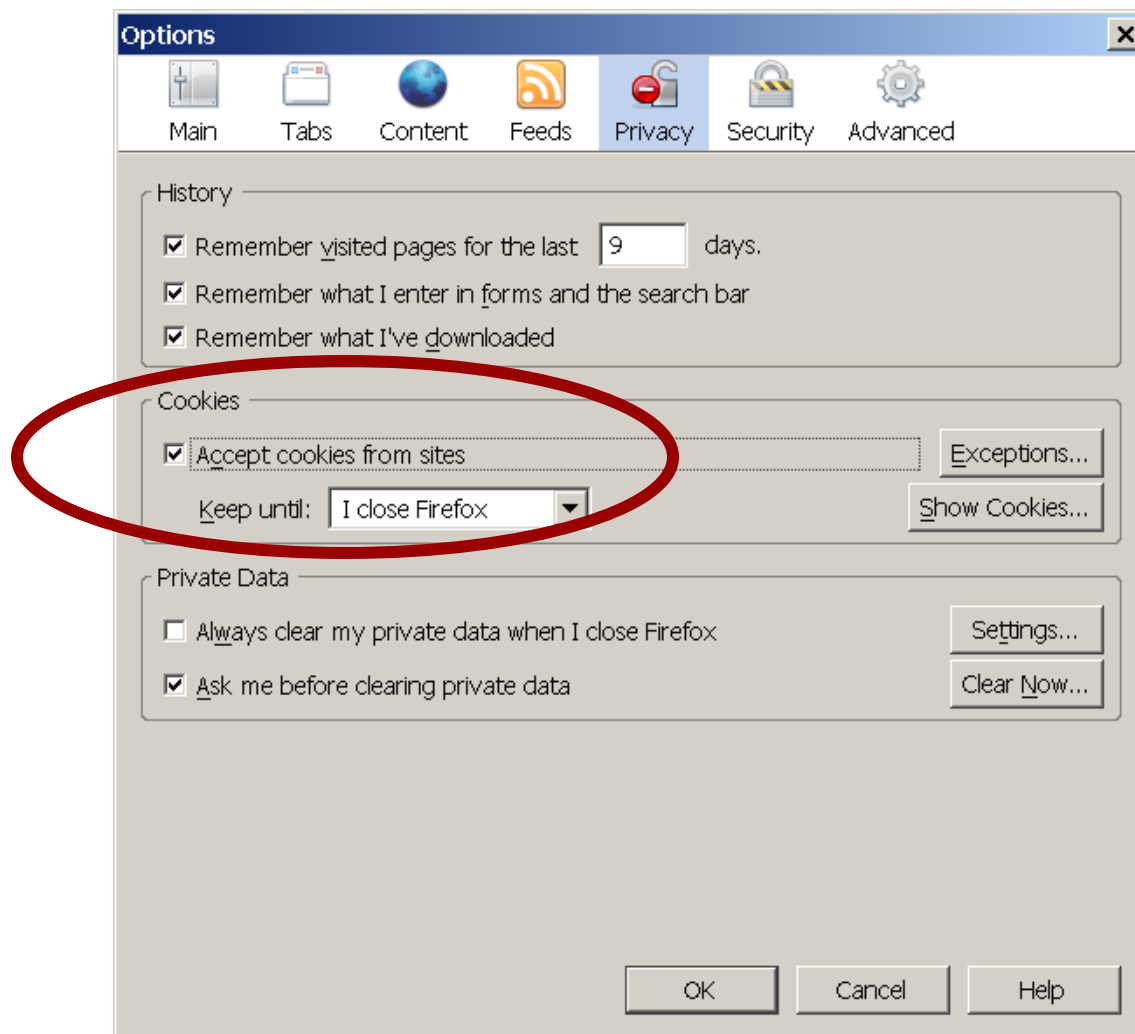
The screenshot shows the Firefox about:config page with the filter set to "cookie". The table below lists the relevant preferences:

Preference Name	Status	Type	Value
network.cookie.alwaysAcceptSessionCookies	default	boolean	false
network.cookie.cookieBehavior	user set	integer	1
network.cookie.disableCookieForMailNews	default	boolean	true
network.cookie.enableForCurrentSessionOnly	default	boolean	false
network.cookie.lifetime.days	default	integer	90
network.cookie.lifetimePolicy	default	integer	0
network.cookie.p3p	default	string	ffffaaa
network.cookie.p3plevel	default	integer	1
network.cookie.prefsMigrated	user set	boolean	true
privacy.item.cookies	default	boolean	false

Cookie expiration

- Issue: Web sites can set persistent cookies that last for years
- Solution:
 - Set cookies to expire at the end of the session by default (in Tools → Options → Privacy)
 - Use an extension to enable persistent cookies on sites you trust:
 - PermitCookies (addons.mozilla.org/firefox/44/)
 - CookieSafe (addons.mozilla.org/firefox/2497/)

Disabling Persistent Cookies



Scripts and other Active Content

Web Bugs

- Issue: Sites use "web bugs" (third party graphics, scripts, iframes, etc) to track visitors
- Solution:
 - Use the Adblock Plus (adblockplus.org) extension to block requests for tracking items
 - This can be done with or without blocking web advertisements
 - Subscribe to the EasyList ABP Tracking Filter (easylis.adblockplus.org) to block web tracking items

Tracking with Active Content

- Issue: Sites use active content such as Java, Flash, or JavaScript to track visitors and gain additional configuration information from them
- Solution:
 - Block active content on untrusted sites
 - Firefox has built in options to globally enable or disable JavaScript and Java (in Tools → Options → Content)
 - Several extensions allow for finer control:
 - FlashBlock (flashblock.mozdev.org)
 - QuickJava (quickjavaplugin.blogspot.com)
 - NoScript (noscript.net)

Referer Header

Referer Header

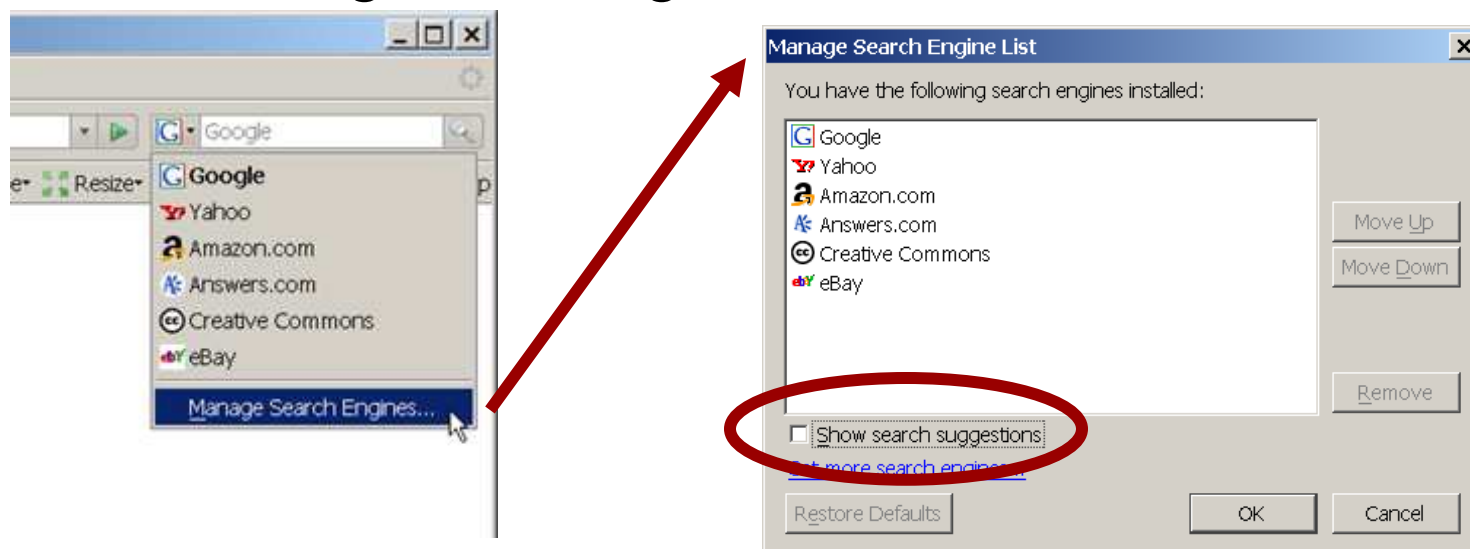
- Issue: Sites use the referer header or the `document.referrer` object to know where a visitor arrived from
- Solution:
 - Disable the referer header and `document.referrer`
 - Do this by setting `Network.http.sendRefererHeader` to 0 in `about:config` (kb.mozillazine.org/Network.http.sendRefererHeader)
 - Some sites don't like the lack of referer... there are several extensions available to selectively enable or disable referers

Google



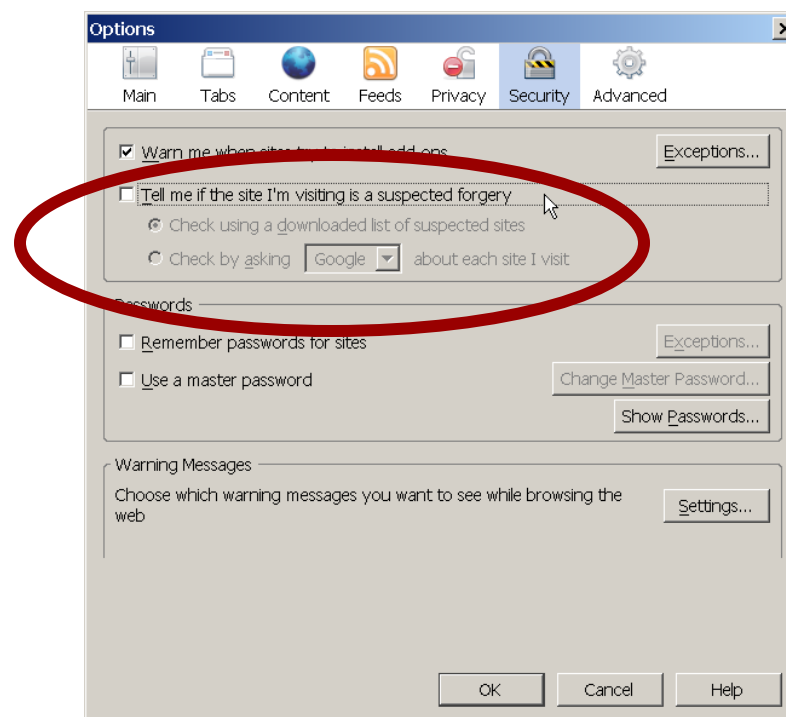
Search Suggestions

- Issue: Firefox sends partial search queries before they are submitted by default
- Solution:
 - Disable "Show search suggestions" in the Manage Search Engine dialog box



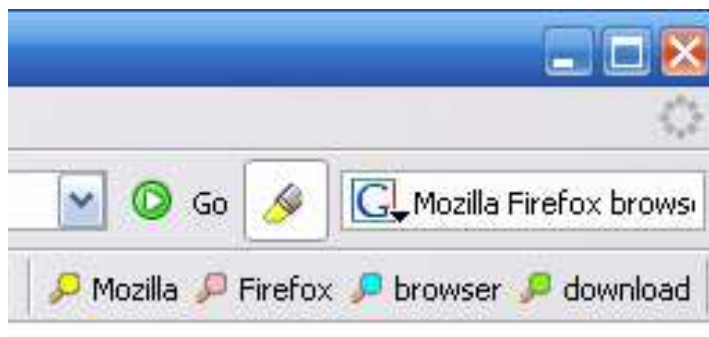
Google Forgery Detection

- Issue: Google site forgery detection will send every site you visit to Google
- Solution: Don't use Google to check if sites are a suspected forgery



Search Term Highlighting

- Issue: The Google Toolbar provides useful features, but it has privacy issues
- Solution:
 - Find alternatives for the desired features
 - The only feature I wanted was search term highlighting and in-page searching
 - I found these features in the SearchWP extension (legege.com/en/mozilla/searchwp)



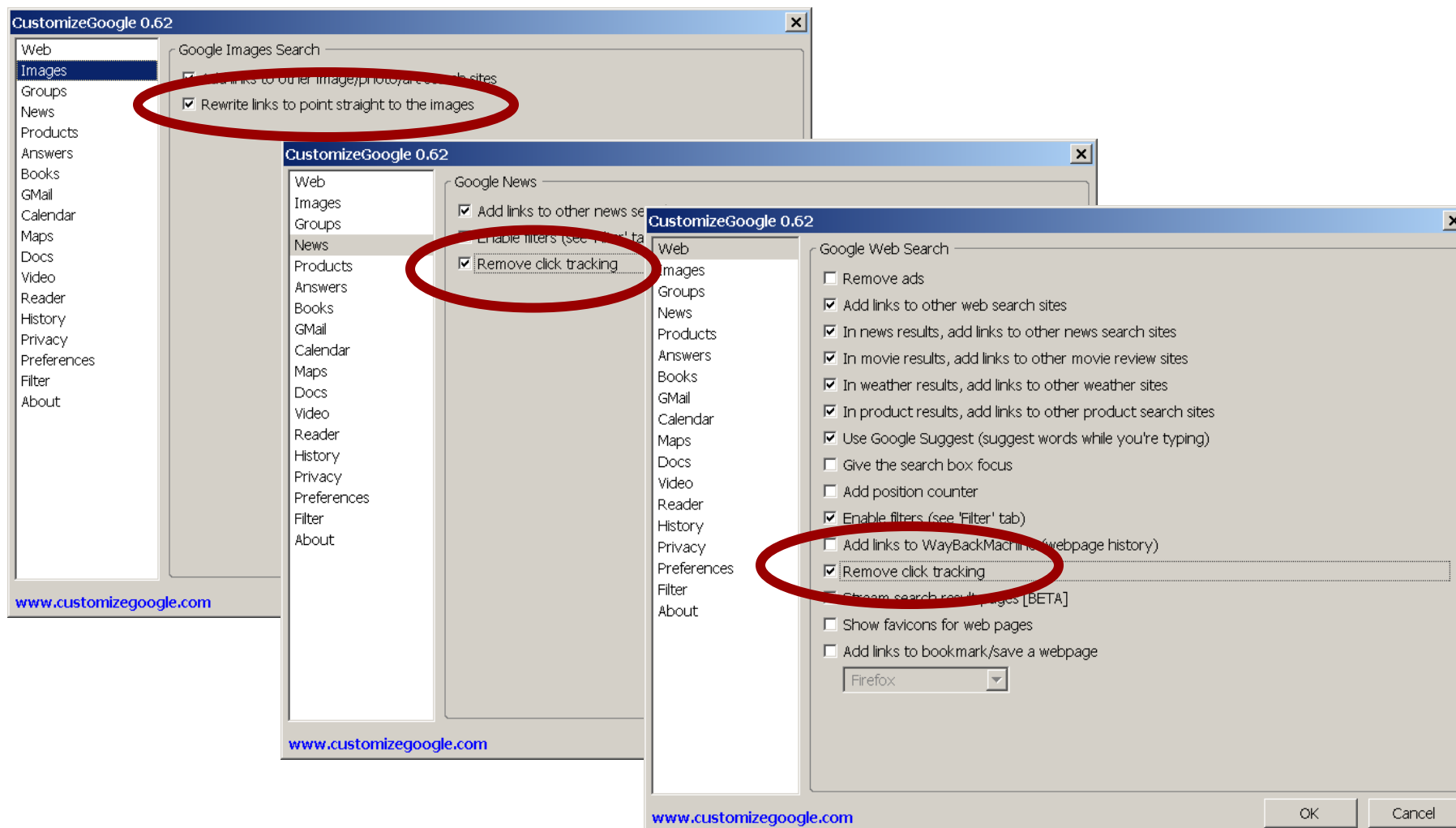
Firefox Profiles

- Issue: You want to be able to be signed in to Google services such as GMail without associating all your searches with you
- Solution:
 - Set up several Firefox profiles
 - Use one for signing in to Google services, use another for Google searches
 - Create a new profile in the Firefox profile manager:
`firefox -profilemanager`
 - Start the new profile with a shortcut that runs:
`"c:\program files\mozilla firefox\firefox.exe"
-p "profilename" -no-remote`

Click Tracking

- Issue: Google tracks which search result you visit after every search
- Solution:
 - Use the CustomizeGoogle extension (www.customizegoogle.com) to remove click tracking
 - Enable "Remove click tracking" option in the Web and News sections of the CustomizeGoogle Options
 - Enable "Rewrite links to point straight to the images" in the Images section of the CustomizeGoogle Options

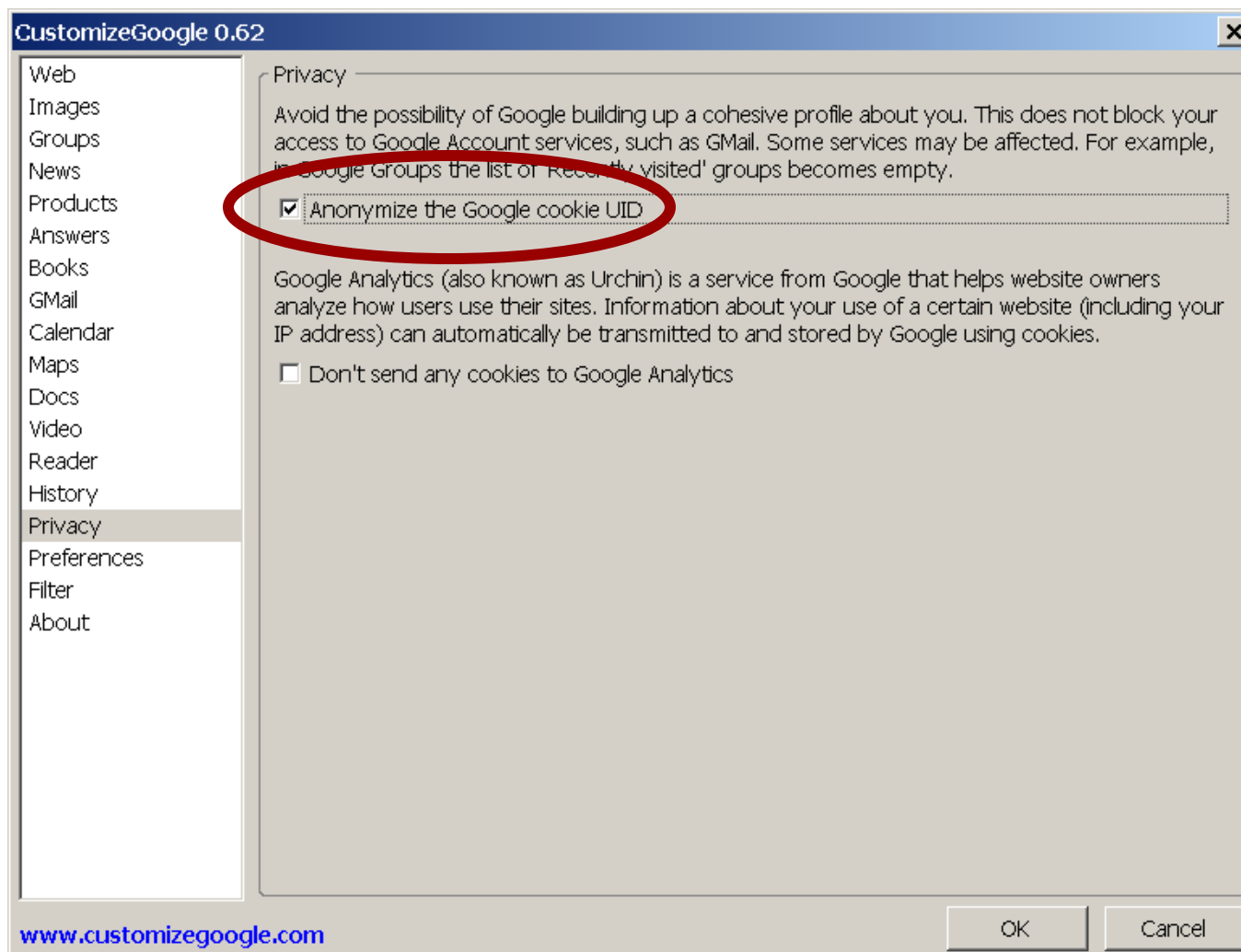
CustomizeGoogle Options



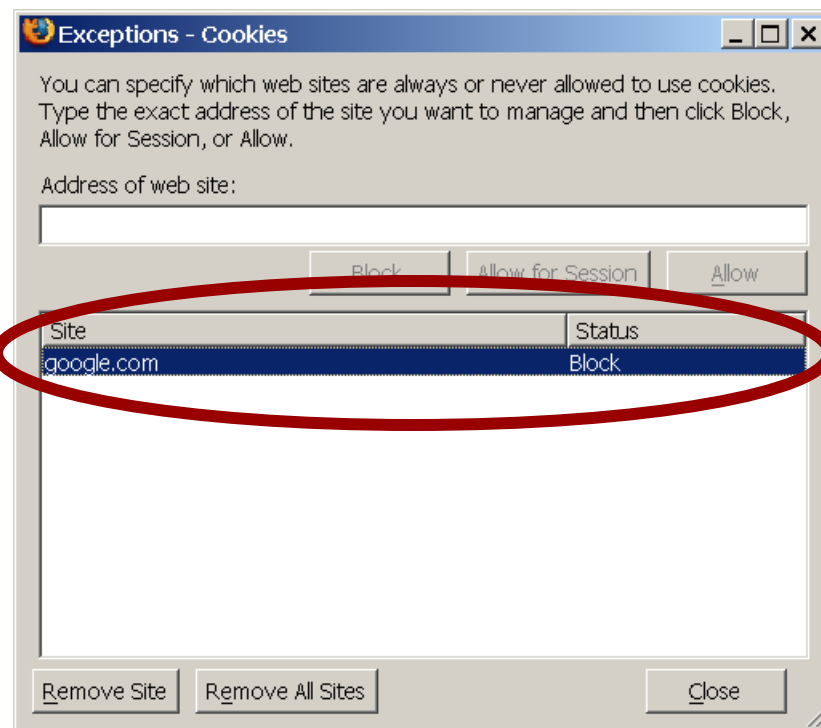
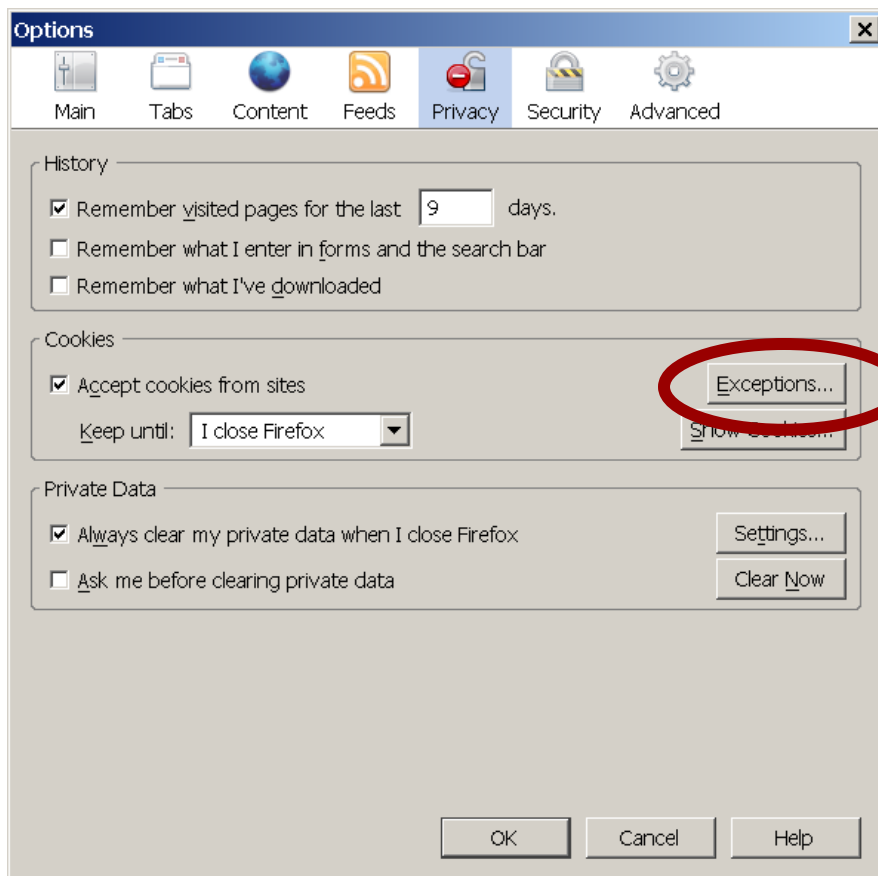
The Google Cookie

- Issue: The Google cookie will tie different search results together
- Solution:
 - In theory, you can "anonymize" the Google cookie (setting it to all zeros), but this doesn't appear to work any longer:
 - Use the CustomizeGoogle extension (www.customizegoogle.com) to anonymize the Google cookie
 - Enable "Anonymize the Google cookie UID" option in the Privacy section of the CustomizeGoogle Options
 - See www.imilly.com/google-cookie.htm for details on the cookie and a bookmarklet to anonymize it
 - Better option: Block google.com from setting any cookies at all (Tools → Options → Privacy → Exceptions)

Anonymizing the Google UID



Blocking Google Cookies



Search Query Data Mining

- Issue: Search queries may reveal personal information
- Solution:
 - Send fake search queries to search engines
 - TrackMeNot extension (mrl.nyu.edu/~dhowe/trackmenot/) sends random search queries to Google, AOL, Yahoo!, and MSN

IP Address Tracking and Geolocation



IP Address Tracking and Geolocation

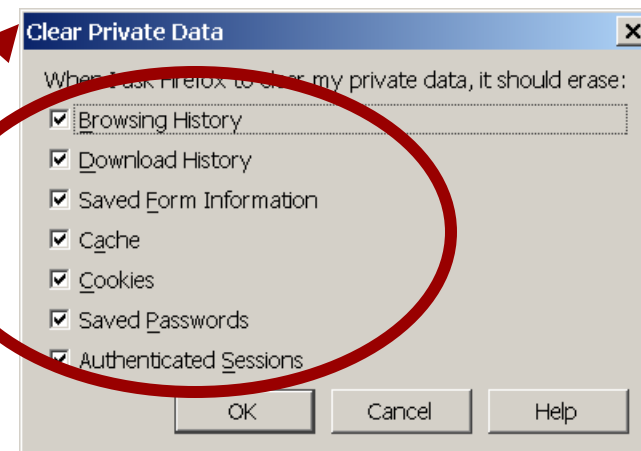
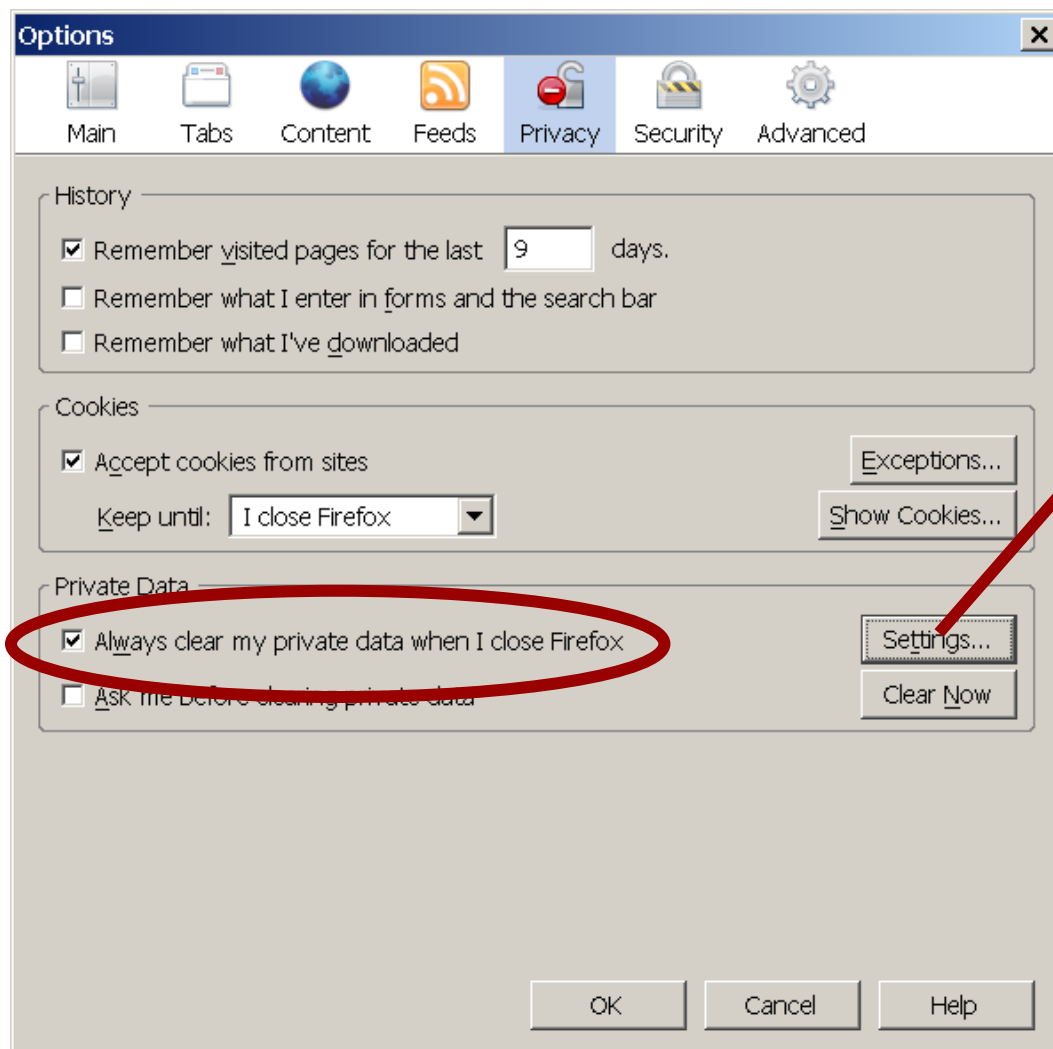
- Issue: Sites can associate multiple sessions from the same IP with one another, especially if the origin is a residential Internet connection
- Solution:
 - Can try to get a new IP address from your ISP periodically (doesn't address Geolocation)
 - Configure the SwitchProxy (mozmonkey.com/switchproxy/) or FoxyProxy (foxyproxy.mozdev.org) extension to use anonymous proxies
 - See foxyproxy.mozdev.org/proxylists.html for lists of anonymous proxies
 - For greater privacy, use Tor (tor.eff.org)
 - Be careful with either option - a malicious proxy or Tor exit node may be monitoring / manipulating your traffic

History and Cache Snooping

History and Cache Snooping

- Issue: Web sites can use JavaScript determine which sites you have visited and/or Style Sheets to customize their site based on your history
- Solution:
 - Clear your history and cache at the end of each session with "Clear Private Data" (in Tools → Options → Privacy)
 - Use the SafeHistory and SafeCache extensions (crypto.stanford.edu/sameorigin/)
 - These partition your history and cache according to the "same origin" policy

Clear Private Data



Site Registrations

Site Registrations

- Issue: Sites require registration to view content
- Solution:
 - See if content is available via the Google cache
 - Try using the User Agent Switcher extension (chrispederick.com/work/user-agent-switcher/) to pretend to be the Googlebot
 - Check with BugMeNot to see if they have a working login (or create one with their disposable email service)
 - If you use BugMeNot often, there is a Firefox extension to automate its use (roachfiend.com/archives/2005/02/07/bugmenot/)

Privacy at a Public Hotspot



Privacy at a Public Hotspot

- Issue: You want to surf the Internet on a public wireless connection without everyone reading your webmail
- Solution:
 - Use an SSH tunnel to a trusted network
 - I use Putty (www.chiark.greenend.org.uk/~sgtatham/putty/) on Windows as a Socks proxy
 - Firefox does not route DNS requests through the proxy by default
 - Set `Network.proxy.socks_remote_dns` to true in `about:config` to change this (see kb.mozillazine.org/Network.proxy.socks_remote_dns)

Questions or Suggestions?

Chuck Willis - chuck.willis@mandiant.com



Practical Web Privacy with Firefox

Chuck Willis
chuck.willis@mandiant.com

Live-OWASP DC 2007
September 6, 2007

