Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Personal Proxy - Online Privacy Protection for Home Users

Although online security has drawn increasing attention, online privacy issues have not been well addressed and communicated, especially for home users. Personal information collection is a common business practice for most web sites and this information can be collected without users' knowledge. There are few resources to educate home users effectively on how online privacy can be invaded and what they can do to protect against it. This paper describes certain online information collection methods and related privacy ...

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

Personal Proxy – Online Privacy Protection for Home Users

Tony Yao
10 September 2002
GSEC V1.4

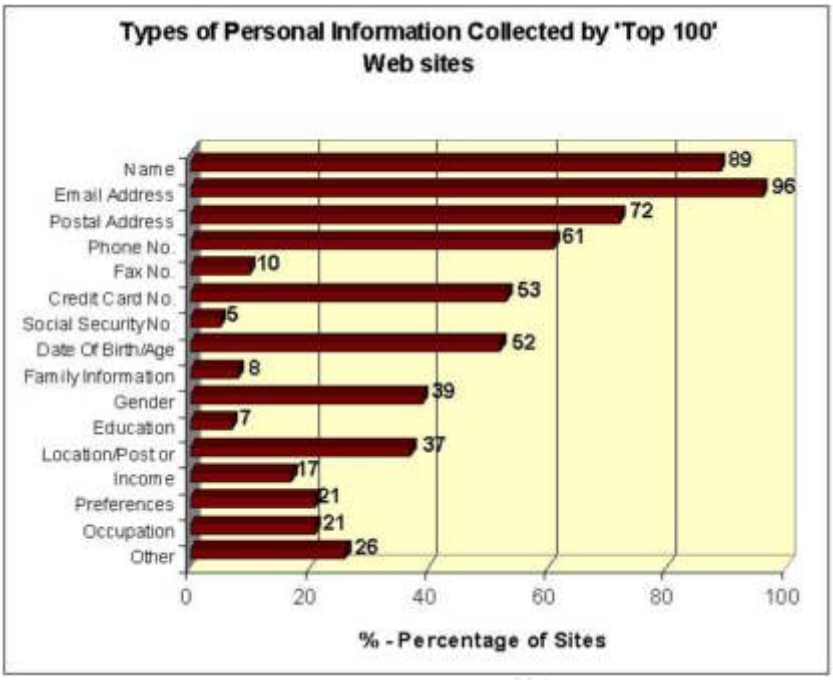
Summary

Although online security has drawn increasing attention, online privacy issues have not been well addressed and communicated, especially for home users. Personal information collection is a common business practice for most web sites and this information can be collected without users' knowledge. There are few resources to educate home users effectively on how online privacy can be invaded and what they can do to protect against it. This paper describes certain online information collection methods and related privacy issues and introduces several personal proxy tools, particularly WebWasher in detail, to secure home users' online privacy. It concludes that better and comprehensive home computer security can be achieved when three types of critical security products: personal proxy, personal firewall and anti-virus, all work together.

Introduction

Online security has been a very hot topic. A search on the Google site using the keywords "online security" returns more than four million results. As part of online security, online privacy is probably the most controversial and, in particular for home users, the least addressed computer security issue. Online privacy can be defined as "the right to determine when, how and to what extent information about ourselves is communicated to others." (1) However, while personal information collection is a common practice for most web sites as shown in the following diagram, (2) many of them do so without the user's consent. In many cases, online users are not made aware of personal information collection and do not have control of their own personal data. "You have zero privacy anyway, get over it", said Scott McNealy of Sun. (3)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



On the other hand, some effort has been made to increase public awareness of the online privacy risk. Searching "online privacy" on Google returns more than six million results. There are certain web sites that serve this purpose such as Privacy Foundation, Privacy Net, Electronic Frontier Foundation, Electronic Privacy Information Center and Online Privacy Alliance. Every year since 1998, Big Brother awards have been given by Privacy International to celebrate the invaders of personal privacy, including online privacy. Progress has been made, although it has been slow. For example, Microsoft recently reached a privacy settlement with the Federal Trade Commission in the U.S.A. because Microsoft's Passport authentication system collects too much information and fails to protect the privacy of personal information. As a result of this settlement, Microsoft is testing one of its products to allow users to control how much information they want to share. On 26 August 2002, the largest net advertising company DoubleClick agreed to change its policies on how personal information is shared and stored after a 30-month multi-state investigation.

However, most of these sites deal with the sharing of collected personal information rather than how personal information gets collected in the first place and how information collection can be either stopped or done in an informed way.

For the vast majority of home users, this online privacy issue has not been understood to the same extent as other computer security issues like viruses and hacking. Even experienced IT professionals hardly think about privacy when surfing the Internet at home. When people talk about home computer security and risks, attention is focused on viruses, Trojans, back door programs, chat clients, spam emails, spyware, hackings, etc. There is hardly anything about online privacy, although it is an important and essential part of

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

computer security. There are many online resources for educating home users on how to enhance computer security with anti-virus software and personal firewalls, but few of them cover how personal information is collected and how to protect against online privacy invasion. For instance, Microsoft published on its web site their seven steps to secure home computers; the US Federal Trade Commission released the guide to online safety for computers with high speed Internet access; and the CERT Coordination Center published a document on home network security on its web site. None of these documents deals with the online privacy issue. Even the online privacy document released by the Electronic Frontier Foundation does not give a simple and effective way to secure online privacy. This paper aims to address this neglected yet important computer security issue by educating home users about the ways personal information can be collected online without user's knowledge and therefore how online privacy can be invaded. It also introduces certain personal proxy tools, particularly WebWasher, to help protect online privacy for home users. Let's start from how personal information gets collected.

Online Information Collection

Spam email is a big problem for many of us today, accounting for 36% of email traffic. Everyday more than 30 spam messages are delivered to my Hotmail mailbox. Some of the spam messages that arrive may contain advertisements about the information you are interested in or be related to sites that were visited days ago. You have to wonder how these people can obtain my email address and know what I was interested in?

When you are using the Internet, your personal information will be collected by most of the web sites you visit. Quite often you are asked to enter your personal information into all sorts of forms, such as your name, gender, date of birth, email address, company, occupation, phone number, etc. But what you may not be aware of is that your personal information can also be collected without your knowledge. You may be surprised at how easily the latter one can be done. Privacy Net has set up a demonstration page. As simple as a mouse click on the link http://privacy.net/analyze/ will send the following information to this site's web server: (12)

- Date of last visit if user has been to the same site before
- Last page from which user was linked to this one
- Browser type and Operating System
- Time zone and local date/time
- Any browser plug-ins installed
- User's IP address
- Trace route information
- Who registered the user's domain
- How the user's domain is configured
- Who owns the user's network

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

How does this happen?

There are a number of ways to do this while users are surfing the Internet, including scripts, applets, ActiveX controls, cookies, web bugs, web referrers, advertising, etc. Web sites may use one or more of these. Scripts, applets and ActiveX controls are relatively easy to block (can be done by web browsers), and are mentioned by most home computer security articles like the ones published by Microsoft and CERT. Therefore this paper will only cover the other methods used to collect information online without users' consent. Let's start with cookies.

Cookies

A cookie is a small text file that a web server places on a user's computer to store data. This file contains a unique number that identifies that user, and a variety of data determined by the server. Most browsers can store at least 300 cookies ranging in size from a few hundred bytes to over 4KB.

There are two types of cookies, session or non-persistent cookies, and persistent cookies. A session cookie exists just for the current browsing session. The cookie is stored in the browser's cache and gets deleted as soon as the browser is closed. One the other hand, a persistent cookie is stored on the local hard drive and may last for years, depending on the expiration date.

If cookies are received from or sent to the web site that is being viewed, they are called first-party cookies. If they are received from or sent to different sites from what is being viewed, they are called third-party cookies. Many web sites allow third-party cookie placement while the majority of those cookies are from net advertising companies.

Cookie files can contain any data you enter into a browser, typically with following information: (14)

- Domain of server that created the cookie
- Whether access to the cookie requires a secure HTTP connection
- Pathname of URL(s) capable of accessing the cookie
- Expiration date and time of the cookie
- Name of the cookie entry
- String data associated with the cookie entry

If you are using Internet Explorer, the IECookiesView utility displays the details of all cookies on your computer.

Cookies are supposedly domain-specific. That is, if one domain creates a cookie, another domain cannot access it.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The cookie is wonderful and powerful, helping to provide a personalized surfing experience, as the web site remembers you, such as your name, other information you entered or the content of your shopping cart.

However, the power of a cookie that can store any data you enter into a browser can be abused and vulnerabilities exist in cookie implementation:

1. Advertising companies use cookies to profile user online activities and surfing habits without users' knowledge.
2. The storage and retrieval of cookies usually goes unnoticed by users. Banner advertisements can have their own cookies and because of their popularity on almost every web page, users may get many cookies in their system by visiting a single web site.
3. The "Open Cookie Jar" exploit makes it possible for a web site to read Internet Explorer cookies set by any other domains.
4. A vulnerability exists which allows a site to set cookies in a way that these cookies can be shared between other domains.
5. Another cookie exploit called "Cookie Monster" allows cookies that are set by a domain other than the American registrant (com, net, org, etc), to be returned to all servers in the same domain. For example, a cookie set by "mycompany.co.nz" might be returned to all servers below the domain "co.nz".
6. Hotmail.com cookies stored on a user's computer can be stolen.

As a result, privacy violation may occur as personal information can be collected without the user's knowledge.

Web bugs

Web bugs appears as graphics on a web page, email message or other web-aware documents used to track various statistics. Web bugs are often invisible because they are typically only 1x1 pixel in size (common resolutions for computer screens are 1024x768, 800x600 or 640x480 pixels), and usually match the background colour of the page. Banner ad companies often use web bugs to monitor who is looking at the document. Common names for web bugs include "clear GIF", "1-by-1 GIF", "invisible GIF", "beacon GIF", and "tracker GIF".

When they are used in web pages, HTML code can be hidden behind web bugs, and that HTML code can be used to collect information. When a web page is viewed, the web bug in this page can collect: (18)

- TCP/IP address of the machine used to view the page
- The URL of the page where the web bug is located
- The URL of the web bug image
- The date and time the web bug was viewed
- The browser type
- Monitor resolution, JavaScript settings, etc.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- The value of a cookie from the domain of the image which was previously set
- Information about the site you are surfing from
- Your windows registry information

Web bugs are widely used on web sites. In addition to the information above, companies use web bugs to: (19, 22)

- Count the number of times a particular web page has been viewed
- Track the pages a visitor views within a web site
- Track what pages an individual visits across many different web sites
- Measure the effectiveness of a banner ad campaign
- Record and report search strings from a search engine to an Internet marketing company - typically used to profile users.
- Transfer previously input demographic data (gender, age, zip code, etc) about visitors of a web site to an Internet marketing company
- Transfer previously input personally identifiable information (name, address, phone number, email address, etc) about visitors of a web site to an Internet marketing company
- Synchronize cookies. This allows two companies to exchange data in the background about Web site visitors.

The following is an example from a popular technical web site:

<img src="http://ad.doubleclick.net/ad/msft.sponsorlinks.dfp5/windows2000;kw=;abr=!ie;sz=1x1;ptile=10;ord=59319938?" border=0 height="1" width="1">

Not all 1x1 pixel GIF graphics are web bugs. To be a web bug, the graphic normally gets loaded from a different web server than the rest of the page.

Web bugs can also be hidden within email messages. The usage of this fashion includes: (19)

- To validate if a recipient's email address is real and working
- To find out if a particular message has been read by the recipient and when
- To obtain the IP address of the recipient. With this information, the recipient's ISP, domain and lots of other information can be obtained as well.
- To obtain the information about how often this message has been read and forwarded

The following is an example of web bug in one of the spam emails I received:

<img border="0" src="http://www.homesavingsplace.com/workathome4/creatives/form_np/images/spacer.gif" width="1" height="1">

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Web-aware documents can also contain web bugs, such as Microsoft Word, Excel, and PowerPoint, even Star Office from Sun. This is because these documents have the ability to load images located on a web server. Every time the document is opened, the web bug image is automatically downloaded from the web server. Similar information can be collected as in other methods.

Web bugs work best in conjunction with cookies and because they are images they can be used to set a cookie on your machine if there is not one there already. For example, it can be used to synchronize a web browser cookie to a particular email address.

Web Referrer

Every time online users go from one web page to another, the browser sends information (called "header information") to the web server hosting the new page, typically including: (20)

- The requested page
- A status code indicating success or error
- Browser type
- Screen resolution
- Local date and time
- TCP/IP address
- URL of previous page

The last item above is called the "web referrer". Referrer data gets sent for every click, even when the pages are within the same site and can be used to profile a user's surfing habits. There are two kinds of referrers, static and dynamic.

Static referrers are pages on other web sites that permanently maintain a link to a particular site. Being "static" means these referrers will continue to exist for a relatively long time. For example, on the www.microsoft.com site, if you click on "MSN Home", you will be taken to the www.msn.com site. For this site, www.microsoft.com is a static referrer as it is going to exist for a long time (isn't it?).

Dynamic referrers are web pages that change frequently or only exist for a relatively short period of time, for instance one day. Examples include news story pages and search engine listings. Homepages for news sites get updated all the time, search engine indexes get changed regularly and the searching logic is modified as well, in each case, the referrer may not be there for more than one day.

Because of this, some people may think dynamic referrers do not reveal as much information as static ones. However, web sites still collect information, and sometimes more, from dynamic referrers. Modern web sites analytical

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

applications can quickly recognize news sites and search engines, and can view and even save the page when dynamic referrer information is received. Even worse, in case of search engines, almost all search engines include the search phrase in the referrer information, so the next site not only knows which search engine you came from, but also what you were searching for.

In some cases, referrer information is not available. For example, if a user selected a link from a bookmark or their favorites, typed the URL directly, or clicked on the link included in an email message, no referrer information gets sent. In these cases, cookies and web bugs may be used instead.

Online Advertising

Online advertising allows companies placing ads on web pages to track user movements across many web sites. It is so popular today that you see ads on almost every web site you visit. Online advertising spending in the U.S.A. is estimated to increase 11% this year, and 14% next year to reach US$9.2 billion by 2003. (21)

Internet advertising can take many forms. The most common one is banner ads. Pop-up windows, Flash, RealMedia, Shockwave, or animated GIFs are frequently used to increase interactivity. CGI scripts, Java scripts and dynamic HTML can also be used to add variety. Another online advertising method is to place ads in online newsletters. If you subscribe to an online newsletter, for example, the chances are you will have emails with ads arriving in your Inbox and web bugs could be contained in those emails.

While closing all of those pop-up windows can be annoying when browsing a particular web site, the real issue is whether the user's privacy is being compromised. Online ads make use of all the above-mentioned methods: cookies, web bugs and referrers to collect user information without the user's knowledge. You don't even have to click on a single ad and your personal information is still gathered. Information collection is totally invisible to the users. If the collected information is combined with other information gathered by third parties, an extremely detailed and comprehensive user profile can be created, which may contain as many as 800 categories. (25) In this way, DoubleClick created about 100 million profiles early in 2000. (26) Another net advertising company Engage created 88 million profiles by the 2nd quarter of fiscal year 2001. (27) In addition, ad-tracking programs are also used to analyze the collected data in order to measure the performance and effectiveness of Internet marketing campaigns.

Reviewing the picture

Now you have the picture: cookies, web bugs, referrers and online ads can all be used to collect personal information without our knowledge. But can they be stopped? Basically yes, but it is very difficult to do so without impacting on normal usage of the Internet. Internet Explorer version 6.0, for example, gives users the ability to control cookies, but disabling cookies is difficult because so many sites need cookies to function. Besides, disabling cookies does not

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

stop the other three. Stopping web bugs is difficult too because they are basically images and the only way to stop them is to turn off all graphics from all web sites. Web bugs can be detected by installing the Bugnosis Web Bug Detector that currently only works with Internet Explorer version 5.0 or greater for Windows users.

Personal firewalls can provide certain degrees of protection, such as stopping hackers coming in, and stopping scripts, spyware or applets reporting back to Internet, but there are scenarios where firewalls cannot help. For example, if you want to visit a site but you don't want them to collect your information or pass your information onto a third party site, the firewall cannot do anything about it. This is where a personal proxy fits in.

Personal Proxy

A Personal Proxy sits between the web browser and the Internet and filters the conversation between browsers and the web sites by examining all the packets coming in to the user's web browser. It gives the user the ability to block cookies, web bugs, web referrers, ads, and scripts and stop them collecting online information. In addition, with web bugs, ads, etc. being filtered out, web page loading will be faster as less files are loaded and bandwidth will be saved. The most important is, without web bugs, ads, cookies, etc., a user's online activity is protected, but conversely it can impact on the how the user interacts with the web site.

There are quite a few personal proxy products in the market, including free and commercial ones. Some of the major players in this field are:

- **WebWasher**: Supports Internet Explorer, Netscape and Opera on Mac (OS 8.1 or above, 9 is recommended), Linux (all current distributions) and Windows 9x/ME/NT/2000 platforms; version 3.2 supports Windows XP as well. Both English and German versions are available. Based on different filters, ads, cookies, web bugs and referrers can be blocked respectively. It has logging function and a simple statistic summary pane. It is easy to configure and customize with its graphic interface, and works with an existing HTTP proxy. This product is discussed in more detail when used in a Windows 2000 Professional environment later in this paper.

  WebWasher is free for home users and schools.

- **Internet Junkbuster Proxy (or Privoxy)**: Runs on a wide range of UNIX platforms, RedHat Linux, Debian, Free BSD, OS/2, and Windows 9x/ME/NT/2000 platforms and supports all popular browsers, such as Netscape, Internet Explorer, Mosaic and Opera. Running in a console window, Internet Junkbuster Proxy blocks requests for Internet files based on blocking rules defined in text-based customizable block files. It also blocks unauthorized cookies and unwanted browser header information and referrer information. Other Internet Junkbuster users post their block files to the Web for use. Logging is extensive - basically, you can log everything into a log file. While you have total control of what you want to

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

block, it requires certain knowledge to create or edit block files, which makes it hard to maintain, especially for the majority of home users. It works with an existing HTTP proxy server.

Junkbuster is free to download, install and distribute according to the GNU General Public License.

Privoxy is essentially Junkbuster developed by other people. Junkbuster version 2.02, published in 1998, was the last official release from Junkbuster Corporation. Because it had been released under GNU GPL, further development by other people was allowed. The result is a product called Privoxy and the latest version is 3.0.0. At present, Privoxy supports Windows 9x/ME/NT/2000/XP, RedHat Linux, Debian, Mac OSX, OS/2, FreeBSD, Solaris, and many more flavors of Unix.

- **Guidescope**: While similar to Internet Junkbuster Proxy or Privoxy, Guidescope is much simpler and easier to install and maintain (of course less powerful). Current version (version 0.994) supports Netscape and Internet Explorer on Windows 9x/ME/NT/2K, and Netscape on X86 Linux and X86 Solaris, with plans to support Mac and Free BSD in future. It blocks ads, cookies, web bugs and referrers. An anonymous email function (User Mail) is provided for users to communicate with Guidescope such as asking for help. It does not have any logging function. It works with an existing HTTP proxy server.

  Guidescope is essentially a web service, which means when blocking is turned on, the URLs of the pages you visit are sent to Guidescope central server which checks them against a central database and sends back a list of what to be blocked. You can customize the list of blocking ads by modifying the Ad List on Guidescope Menu. The modified ad list is submitted to Guidescope for inclusion in their central ad-blocking database. Personally, I dislike this kind of central monitoring and control method because online privacy is exactly what we intend to protect. A similar Cookie List on Guidescope Menu can be used to allow a site to set and read cookies on your machine. Another thing I am not comfortable with is that all of the customization work is done via the Guidescope Menu, and if the Menu is not already open on your desktop, you have to go to Guidescope homepage to open it.

  Guidescope is free for individual use at home.

- **Proxomitron**: Supports all browsers and runs on Windows 9x/ME/NT/2000/XP platforms. Running on other platforms has not been tested although running on Linux has been reported. It may be the most powerful proxy filtering product I have come across because it is not really designed to filter anything specific, instead it just gives users the ability to filter whatever they want. It can re-write web pages on the fly. However, this means customization requires a fair amount of knowledge in areas like Java scripts, text-matching language and Meta characters, which is often beyond the scope of average home users.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Out of the box, Proxomitron blocks cookies, referrers, web bugs and ads based on the rule sets defined in different filters. It also does other things like stopping pop-up windows and banner ads, freezing animated ads, stopping web pages from auto-refreshing, stopping background MIDI songs from playing unless you choose to, removing dynamic HTML tags, etc. You can download and merge filters contributed by other Proxomitron users from Internet. It also has the most comprehensive help documents among other personal proxy products, possibly due to the fact that it is difficult to customize. On the Proxomitron web site, there are links to Proxomitron information sites in other languages.

A log window can be used to display information about ongoing activity, including HTTP requests and response header messages, and the filters that matched a particular web page. Logging is only active when the log window is open. When the window is closed, logging is off and previous logged information is gone. However, log windows information can be copied to Windows clipboard. Proxomitron works with an existing HTTP proxy server.

Proxomitron is free for use. It was released as ShonenWare – users can support the program's future development by purchasing any album by Japanese female power-trio Shonen Knife whose music is dearly loved by the author of Proxomitron.

- **Naviscope**: Supports all browsers and runs on Windows 9x/ME/NT/2000 platforms. Porting options are being explored to support Linux and Mac in future. It blocks advertisements, cookies, Java scripts, sounds, etc. Customization is done via the Naviscope toolbar that shows on top of browser screen (this can be annoying sometimes though) and automatically shrinks and grows. Limited logging function is provided, and you can specify the log file size.

  Filtering can be done globally or on a site-by-site basis. Images can be identified as ads by Ad Keywords and get blocked. It works with an existing HTTP proxy server.

  Naviscope comes with some handy tools, such as DNS resolution caching, persistent connection, MTU/RWIN (Maximum Transfer Unit/Receive Windows) optimization, etc. One of them worth mentioning is “pre-fetching” which can be used to speed up web browsing. Naviscope can, based on your request, use keywords to download web pages it thinks you are likely to visit next. For example, you search for “Online Privacy” on Google; Naviscope will download the next search result page while you’re viewing the first one. Perfecting is triggered by keywords that can be customized.

  Status Windows on toolbar can display information about the number of ads blocked, number of pages pre-fetched, physical memory load, browser cache hits, number of hops, etc.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Naviscope is free of charge as a limited time offer (still free as of today, 10 September 2002). Prior to this, it was shareware with 30-day trial period and US$19.95 for registration.

- **AdSubtract**: Being the #1 rated ad-blocking program on the market, AdSubtract Pro (Professional) supports all versions of Netscape and Internet Explorer on Windows 9x/ME/NT/2000/XP platforms. It blocks all kinds of ads such as banner ads, pop-up ads, flash ads, etc. It can also block animated GIFs, cookies, referrers, Java scripts, etc. Customization is done via a graphic control panel. Blocking can be done globally or on a site-by-site basis. Custom sites and tokens can be defined to recognize advertisements on these sites. It works with an existing HTTP proxy server.

  Log pane lists each filtering action and/or each HTTP request. Stats pane shows a summary of everything AdSubtract has filtered, such as the number of ads filtered, number of pop-ups filtered, etc.

  AdSubtract Pro is a commercial product costing US$29.95 with one year of regular ad database updates. A 30-day trial is available for download.

  AdSubtract SE (Standard Edition) is free for personal use at home for 6 months. Supporting any browsers on Windows 9x/ME/NT/2000/XP platforms, it only blocks banner ads and cookies.

- **Filtergate**: Works with all popular browsers on Windows 9x/ME/NT/2000/XP platforms. Based on filters, it can block pop-up windows, banner and tower ads, cookies, web bugs, referrers; it can also block access to adult sites. No browser configuration is required. It works with an existing HTTP proxy server.

  Simple customization is done via a graphic interface, where you can define an exception list to prevent a site or URL from being filtered. It doesn't have a logging function, just a statistical summary showing how many items have been filtered out.

  There's an Auto Update option. If it's on, Filtergate automatically updates the filter database while online.

  Filtergate is a commercial product costing US$19.95 (normally US$34.95) with free unlimited upgrades.

There are some other products like Ad Muncher, AdKiller, Banner Blind, Block Adverts, and Norton Internet Security etc., though many of them only focus on advertisement blocking.

Ultimately, home users need one product with comprehensive security features. Norton's Internet Security is a step in the right direction, by

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

combining anti-virus, firewall, privacy control and parental control components into one product suite, but its privacy control is limited to ad blocking.

WebWasher on a Windows 2000 Professional Machine

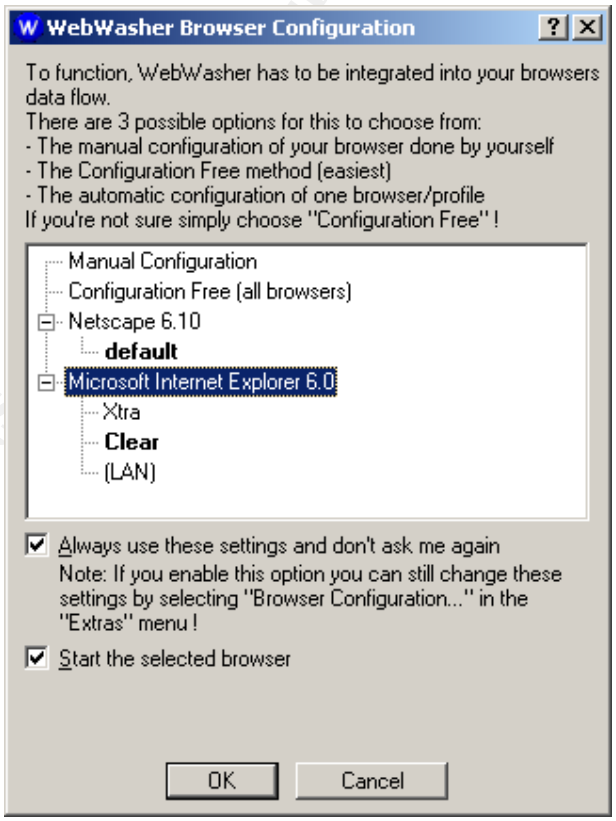
For the majority of home users, the most suitable option at present is WebWasher because it supports popular browsers and runs on multiple platforms. It is easy to install and configure with a nice graphic interface, and it's free.

The following description is based on WebWasher version 3.2 BETA 4 running on a Windows 2000 Professional machine.

Installation

Installation of WebWasher for Windows is simple and straightforward. Download the latest version for the Windows platform from WebWasher Windows download site and run the executable to kick off installation process.

After installation, the browser has to be reconfigured to work with WebWasher. WebWasher may need to be reconfigured as well if you are already using an HTTP proxy server for Internet access. The first time when WebWasher is run, following configuration screen is displayed:



There are three options to reconfigure the browser:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

1. ***Manual configuration***: Browser will be configured manually. If you're already using an HTTP proxy server, WebWasher has to be manually reconfigured too. The online help contains detailed steps to manually do this.
2. ***Configuration Free***: This is new to version 3.2. Previous versions including 3.0 don't have this option. Network settings for browser and WebWasher won't be changed, and WebWasher still works. This is mainly used in an environment where multiple browsers are used in the same time.
3. ***Automatic configuration***: Specified browser and WebWasher will be configured automatically based on your current network settings. You can choose browser and user if the computer supports multiple users and more than one browser. This is the recommended option.

Checking the ***Start the selected browser*** option means loading WebWasher will start the selected browser at the same time.

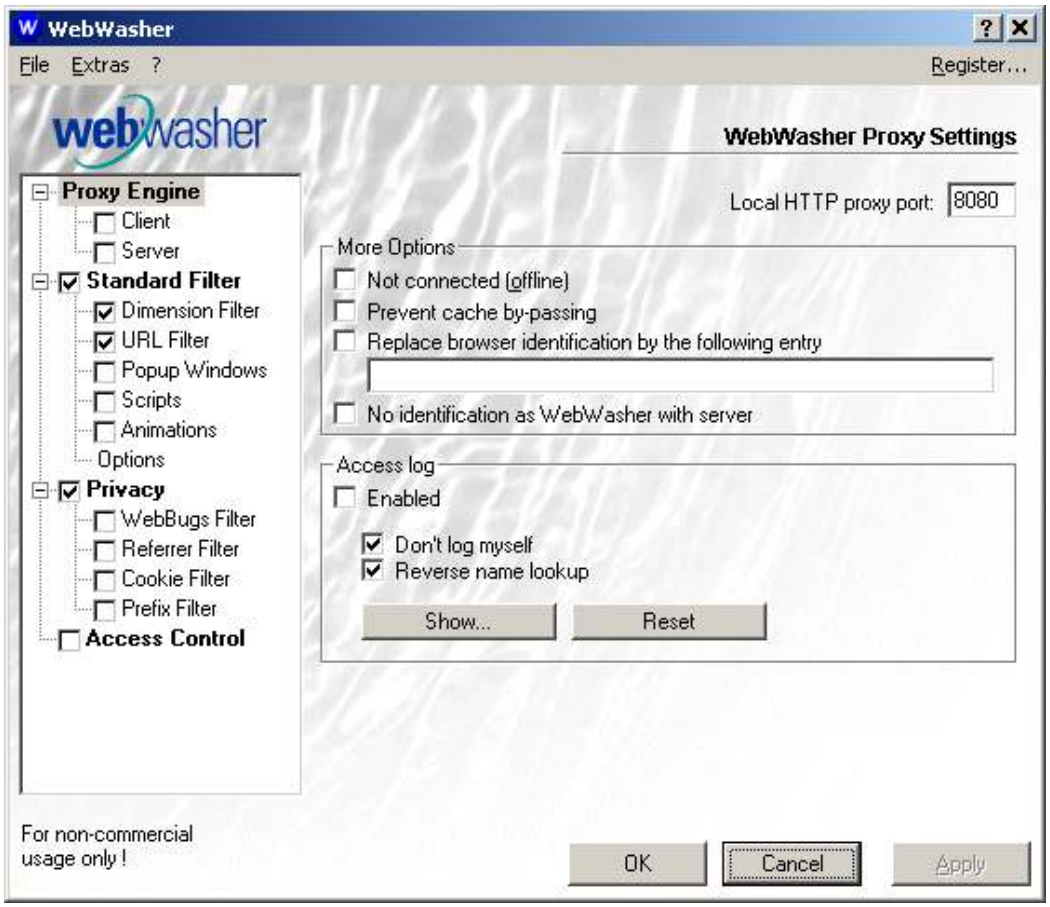
When WebWasher is running on your machine, an icon shows in the system tray: . A right click on it brings up the context menu, a double click on it brings up the configuration panel, one click disables WebWasher on the fly, and the tray icon changes to (same as selecting ***Deactivate standard filter*** in the context menu). One click on it again re-enables it.

You can change the browser and WebWasher settings anytime in the configuration panel, ***Extras***, ***Browser Configuration…*** or by selecting ***Browser Configuration…*** in the context menu.

Configuration

Double click on the WebWasher system tray icon or right click on the tray icon then select ***Preferences…*** to bring up the following configuration panel:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



Proxy Engine

As discussed previously, web bugs can come in email messages. The obvious way to stop this is to disconnect from the Internet after downloading and prior to reading email messages. This is sometimes inconvenient and this is where the ***Not connected (offline)*** option becomes handy. This option, when enabled, disconnects your browser from the Internet temporarily, so web pages are read from cache instead of Internet web sites.

Browser cache is normally used to accelerate web surfing when the same page is requested next time. However, some web pages contain special codes bypassing the browser cache to force all data to be transmitted again from the Internet. This behavior can be stopped by checking the ***Prevent cache by-passing*** option.

When you visit a web site, your browser normally sends identification information about itself to the site, such as browser type and operating system, etc. This identification information is called the "user-agent string". More information on this can be found in References. You can change the identification information or choose not to give the information. If you choose not to give any information, just check ***Replace browser identification by the following entry*** option and leave the entry blank.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

With WebWasher running, an additional WebWasher ID is included in the information the browser sends to the web site. Some sites (those that need banner ads, for example) may block your access if the WebWasher ID is detected. You can also choose not to send WebWasher ID information by checking ***No identification as WebWasher with server*** option.

Accesses via WebWasher can be logged into the access log file in WebWasher's program directory. This function works pretty well in version 3.0, but not in version 3.2 BETA 4, (this might be because this is just a BETA version). The following information is logged:

- Date and time
- Connection method such as GET, POST, etc
- URL
- Redirect strings
- Error code
- Bytes transferred
- HTTP type
- User agent (browser identification information)

Client setting is required if an HTTP proxy server existed before WebWasher installation. However, if ***Automatic configuration*** option is chosen the first time WebWasher starts, this configuration work is done automatically, which is a copy of previous network settings for Internet access.

Server setting is used to configure WebWasher as a proxy for other users to access the Internet.

Standard Filter
This is where you can block ads, pop-up windows, scripts and animations on web pages.

Dimension Filter is used to block advertising images. The Internet Advertising Bureau defined certain standards on banner ad size. Based on this, WebWasher comes with a built-in internal blocking list with all the sizes for ads. New dimensions (sizes) can be defined and you can choose to activate or deactivate specific dimensions. You can also enable or disable filtering for images, plugins and applets.

Image size information can be defined in HTML code or in the header of the image file itself. If it is not in HTML code, by default, WebWasher checks image file header to get the information. Checking ***Ignore images without specified dimensions*** option disables this behavior.

URL Filter is where filtering is defined based on URL and object types. On a web page, right click on the image you don't want to see, select ***Add to filterlist (WebWasher)***, and the URL will be placed in URL filter list

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

automatically. The filter list doesn't require full URL, partial ones with wildcards is fine. WebWasher online help explains in detail about the syntax.

WebWasher comes with a built-in filter list, in which most of the ads are automatically filtered.

There are two options for each URL. ***do not filter*** takes precedence over the built-in filter list and user-defined list. Taking an example, for whatever reason, if domain yahoo.com is filtered, you cannot do anything even if you can get to the www.yahoo.com site. If you want to get to Yahoo! Photos site, just put photos.yahoo.com under ***User defined filterlist***, and check ***do not filter*** option. ***inactive*** means the line is disabled, WebWasher will ignore the line in the list.

Popup Windows, ***Scripts*** and ***Animations*** settings are self-explanatory and online help provides a good description for each one of them.

Privacy
This is the place where cookies, web bugs, referrers, etc. can be blocked.

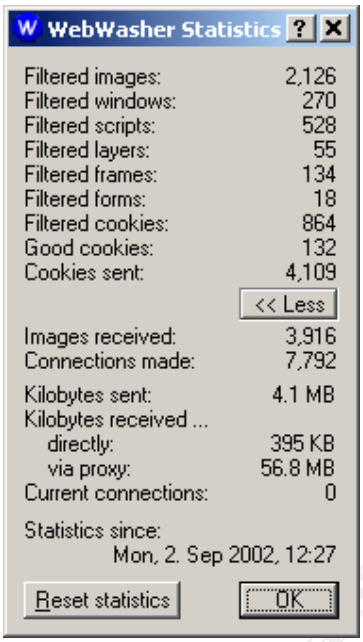
Web bug filter and referrer filter are pretty straightforward. Like the URL filter, WebWasher comes with a built-in cookie filter that automatically filters bad cookies.

You can list the domains from which you want to accept cookies (Good), or mark them as neutral (?) and specify a timeframe when these neutral cookies should expire, or you want to reject cookies (Bad). Again, WebWasher comes with a built-in cookie filerlist that contains many known ad sites.

Access Control
If you want to block all access to web pages or web sites no matter what exceptions such as ***do not filter*** may have been defined in **URL Filter** section, or if you want to redirect you browser for blocked URLs to another page, you can use ***Access Control*** setting to do so. By putting a URL here, you can't get to that URL at all.

Extras
In **Extras** menu, ***Statistics*** shows the number of each item that has been filtered out since WebWasher was first run, as follows:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



You can password protect the configuration menu by selecting ***Password protection*** from the **Extras** menu. By doing so, you must supply a password before you can access the configuration panel.

With all of these filters in place, not only can WebWasher protect user's online privacy, but Internet browsing will also speed up. If web sites require scripts or pop-up windows to be functioning, such as Windows Update site, or users may want to support ads on some web sites, WebWasher can be disabled temporarily. Alternatively, these sites can be added into user defined filter list.

Conclusion

Personal proxy enables online users to regain control over their personal information. With a personal proxy, online users can control how much information they want to share and with whom they want to share. Personal proxies are complementary to personal firewalls, and are indispensable software for comprehensive home computer security. Working together with anti-virus software and personal firewall software, a personal proxy provides home users with a more secure, faster and personalized surfing experience; thereby achieving far better computer security.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References:

1. Gutter, Richard. "A Survey of Recent Threats to Privacy Rights." 23 January 2002
   URL: http://rr.sans.org/privacy/survey.php (14 August 2002)

2. Halstean, Dave and Ashman, Helen. "Electronic Profiling." 2000
   URL: http://ausweb.scu.edu.au/aw2k/papers/halstead/paper.html (14 August 2002)

3. Sprenger, Polly. "Sun on Privacy: Get Over It." 16 January 1999
   URL: http://www.wired.com/news/politics/0,1283,17538,00.html (14 August 2002)

4. Wilcox, Joe. "Microsoft, FTC reach privacy settlement." 8 August 2002
   URL: http://news.com.com/2100-1001-948922.html?tag=fd_lede (14 August 2002)

5. Wilcox, Joe. "Microsoft adds privacy control." 27 August 2002
   URL: http://zdnet.com.com/2100-1104-955514.html (30 August 2002)

6. Reuters. "DoubleClick pays to end privacy probe." 26 August 2002
   URL: http://news.com.com/2100-1023-955356.html?tag=fd_top (27 August 2002)

7. CERT Coordination Center. "Computer security risks to home users." Home Network Security. 5 December 2001
   URL: http://www.cert.org/tech_tips/home_networks.html (16 August 2002)

8. Microsoft. "Assess your risk: Step 1 to personal computer security." 2 April 2002
   URL: http://www.microsoft.com/security/articles/assess.asp (16 August 2002)

9. Federal Trade Commission. "Safe at Any Speed: How to Stay Safe Online If You Use High Speed Internet Access." 27 August 2002
   URL: http://www.ftc.gov/bcp/conline/edcams/infosecurity/ (29 August 2002)

10. McCandlish, Stanton. "EFF's Top 12 ways to Protect Your Online Privacy." 10 April 2002
    URL: http://www.eff.org/Privacy/eff_privacy_top_12.html (20 August 2002)

11. Lemos, Robert. "Spam hits 36% of email traffic." 29 August 2002
    URL: http://zdnet.com.com/2100-1106-955842.html (30 August 2002)

12. Privacy.Net. "Privacy Analysis of Your Internet Connection – How It works"
    URL: http://privacy.net/analyze/analyzehow.asp (15 August 2002)

13. Kristol, D and Montulli. L. "HTTP State Management Mechanism." February 1997
    URL: http://www.ietf.org/rfc/rfc2109.txt (30 August 2002)

14. Goodman, Danny. "Cookie Recipes." December 1996
    URL: http://developer.netscape.com/viewsource/archive/goodman_cookies.html (16 August 2002)

15. Beciragic, Jasmir. "Cookies and Exploits." 27 April 2000
    URL: http://rr.sans.org/covertchannels/cookies.php (16 August 2002)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

16. Miller, Randall S. "Cookies – Exploitations and Invasion of Privacy." 19 April 2001
URL: http://rr.sans.org/privacy/invasion.php (16 August 2002)

17. Shalev, Dror. "Stealing Hotmail.com Cookie and User Login." 17 July 2002
URL: http://www.securiteam.com/exploits/5OP0D207PK.html (16 August 2002)

18. Lowe, Richard and Arevalo-Lowe, Claudia. "Web Bugs."
URL: http://internet-tips.net/Security/webbugs.htm (15 August 2002)

19. Smith, Richard M. "FAQ: Web Bugs."
URL: http://www.privacyfoundation.org/resources/webbug.asp (19 August 2002)

20. Lowe, Richard and Arevalo-Lowe, Claudia. "Referrer."
URL: http://internet-tips.net/Security/referrer.htm (15 August 2002)

21. Gaffney, John. "The Online Advertising Comeback." June 2002 Issue, Business 2.0
URL: http://www.business2.com/articles/mag/0,1640,40430,FF.html (19 August 2002)

22. BAGNOSIS. "Web Bug FAQ"
URL: http://www.bugnosis.org/faq.html (20 August 2002)

23. Laitt, Adam. "Online Advertising 101." 6 April 2001
URL: http://hotwired.lycos.com/webmonkey/01/14/index4a.html (22 August 2002)

24. Mozilla. "User-agent strings." 30 July 2001
URL: http://www.mozilla.org/build/revised-user-agent-strings.html (22 August 2002)

25. Press Release. "Engage Media's Profiles Maximize Online Marketing Campaign for StudentUniverse.com." 16 August 2002
URL:
http://www.engage.com/press_room/viewpress.cfm?urlcode=081600student (03 September 2002)

26. Heather Green. "Privacy: Outrage on the Web." 8 February 2000
URL: http://www.businessweek.com/smallbiz/content/feb2000/mk3668065.htm (03 September 2002)

27. Press Release. "Engage Announces Fiscal 2001 Second Quarter Results." 12 March 2001
URL: http://www.engage.com/press_room/2001q2.cfm (04 September 2002)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced