interhack

interhack corporation 871 eastmoor blvd columbus, oh 43209 http://www.interhack.net/

Privacy Advisory

subject Opting In, By Accident
date May 15, 2000
authors Gary Ellison `<gfe@interhack.net>`
Matt Curtin `<cmcurtin@interhack.net>`
Doug Monroe `<monwel@interhack.net>`

1 Executive Summary

Netscape Communicator can inadvertently “OPT IN” to tracking sites after an explicit “OPT OUT” has taken place.

2 Overview

The recent consumer and government uproar over privacy concerns of surfing the net has pushed tracking agencies, such as DoubleClick and AdKnowledge (P.K.A. Focalink), to offer consumers an “OPT OUT” mechanism whereby they can choose to not be subjected to the advertisers’ tracking of their web surfing.

In general, the mechanism used by tracking agencies is to have you (voluntarily or involuntarily) “OPT IN” by setting the value of a tracking cookie to a *unique* value. Every time the browser requests a resource from the tracking domain, the request will include the cookie containing this unique value. Conversely, the mechanism used by tracking agencies to allow one to “OPT OUT” is to set the value of the tracking cookie to a *constant* value. That is, the value of the tracking cookie is the same for all browsers that opt out.

For example, DoubleClick sets the constant (opt out) value of their tracking cookie to `id=OPT_OUT`. The opt out cookies usually have a long expiration period (the year 2030 and 2010 for DoubleClick and AdKnowledge respectively) and thus is intended to persist in the browser cookie store, and to be issued in all resource requests made to tracking domains, until it expires [1, 3]. Presumably, this constant (opt out) value can not be tied to a individual as easily as a unique (opt in) value.

However, an apparently short-sighted implementation of a feature in Netscape Communicator can result in an inadvertent (and potentially unnoticed) opt-in to these tracking sites even after one has explicitly chosen to opt out. Netscape Communicator seems to assume that if you *ever* configure “Do not accept or send cookies” that you will *never* want to re-enable any previously stored cookies in the future.

It has been observed that whenever you choose `"Edit"->"Preferences"->"Advanced"` and select “Do not accept or send cookies”, communicator deletes the cookie store, including the opt out cookies. (Note that on the Windows platforms, versions 4.7x label this button “Disable cookies”.)

Thus, your next browser session will not send the constant “OPT OUT” cookie (since all cookies have been deleted), and will result in your being issued unique tracking cookies by these agencies once again. Note that as long as you retain the “Do not accept or send cookies” setting, both unique and constant tracking cookies will be discarded. If you do re-enable one of the other cookie control options “Accept all cookies” or “Only accept cookies originating from the same server as the page being viewed”, then the next time a tracking site is referenced you will once again receive a unique tracking cookie (i.e., “OPT IN”.)

3 Tested Systems

In all likelihood all versions of Communicator which give you the cookie managment options have this defect. We specifically tested Communicator versions 4.5, 4.7, and 4.72 on Solaris 2.7; 4.51, 4.6, 4.7, and 4.72 on RH Linux 6.1; and 4.5, 4.6, 4.72, and 4.73 on Windows 9x and NT.

4 Other Systems Tested

Netscape 6 Preview Release 1 implements a different cookie management scheme and does not exhibit the behavior described above. Also note that this release of Netscape exhibited odd behavior during the opt out sequence with DoubleClick. Refer to the DoubleClick Opt Out Advisory [2].

Internet Explorer 5.x stores each cookie in a separate file and does not delete them when cookies are disabled.

Opera 4.0 Beta 3 stores cookies in a single file but does not toss them when cookie acceptance is disabled.

5 Demonstration

Select `Edit->Preferences->Advanced` and "Do not accept or send cookies" as shown in Figure 1.

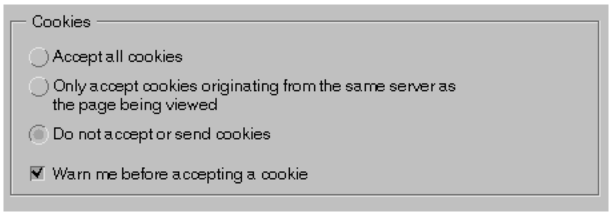

Figure 1: Turning off cookies

Exit the browser. All cookie data is now gone from disk and memory.

Start Communicator and select `Edit->Preferences->Advanced` and "Only accept cookies originating from the same server as the page being viewed" as shown in Figure 2.

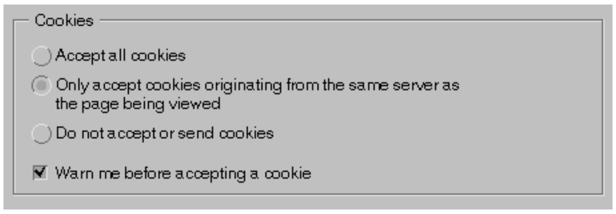

Figure 2: Turning on cookies

Now surf to the DoubleClick opt out page at
`http://www.doubleclick.net:8080/privacy_policy/privacy.htm`.

By setting the "Warn me before accepting a cookie" option you can see the tracking cookie coming to the browser. If you sniff the network traffic you should see the following in the HTTP header;

```
Set-cookie: id=A; path=/; domain=.doubleclick.net; expires=Wed,
            09-Nov-2030 23:59:00 GMT
```

6 Workarounds

If you frequently toggle the Cookie Accept/Deny setting there is no convenient workaround. There are several options, each of which carries some particular type of overhead.

The best that can be offered is always to leave the "Warn me before accepting a cookie" option set so that you have a chance to discard the tracking cookies as they come in. The problem with this option, of course, is that if you visit a site that has many independent graphics, you might see a high number of dialogue boxes, each asking whether to allow the cookie. Thus, you'll be required to answer them one-by-one until they've all been addressed. Some Web sites are unusable this way.

Another alternative is to use third party cookie handling software.

7 Deleting Cookies

Of course, you can delete your cookies file every time you quit Communicator. However, this carries with it the problem of being tracked for the duration that your browser is active (and that it's configured to allow cookies)—until the cookies are saved to disk and you manually delete them. The advantage provided here is that it is much more difficult for a third party (such as a banner advertising network) to track your activity over the long-term, which is how the most egregious privacy invasion typically happens.

References

[1] Netscape Communications Corporation. Persistent client state HTTP cookies. [online] http://www.netscape.com/newsref/std/cookie_spec.html.

[2] Gary Ellision, Matt Curtin, and Doug Monroe. Doubleclick opt out protocol failure == opt in. Interhack Privacy Advisory, May 2000. [online] http://www.interhack.net/pubs/dc-proto-fail/.

[3] D. Kristol and L. Montulli. HTTP state management mechanism. RFC 2109, February 1997. [online] http://www.ietf.org/rfc/rfc2109.txt.