INTERHACK

Interhack
2599 E Main St #512
Columbus, OH 43209

VOX +1 614 545 HACK
FAX +1 614 545 0076
WEB http://web.interhack.com/

PCFriendly Enables DVD Backchannels

Matt Curtin

February 28, 2002

Abstract

Numerous DVD titles from major movie producers between 1996 and 2000 come enabled with "PCFriendly," an application developed by InterActual Technologies that tracks DVD usage. The system is designed to identify users persistently, without using an HTTP cookie, thus bypassing any privacy-enhancing technologies like cookie management software or browser configurations. The identifying token is persistent through product registration and PCFriendly use.

Normal use of popular DVD titles on computers will result in users being identified verinymously, along with the DVDs that were used on the machine. Privacy problems for the user are significantly exacerbated by the DVD titles' links to Web sites, some of which have nonexistent privacy policies and in at least one case, send the user's email address to a third party.

This behavior conflicts directly with the PCFriendly posted privacy policy of December 2000. Further discussion with InterActual showed that the policy was written to apply to the newer InterActual Player, released to replace the PCFriendly player, for which no privacy policy existed.

PCFriendly appears to offer users granular control over which parts of the backchannel to enable, but the controls are not obvious, and are all enabled by default. Further, the software has been deprecated in favor of the newer InterActual Player, which includes additional features for user control over backchannel behavior.

1 Executive Summary

Various movie producers, including Universal, Elektra, Dreamworks, and Paramount, add "advanced interactive features" to their DVD titles that allow for additional "content" to be served to the client from the Internet. As the "PCFriendly" application that enables this functionality is used, the user's activity is uniquely tagged and reported to the PCFriendly web site. Because each installation of PCFriendly is uniquely identified with a `USERID` token, it is also possible for InterActual Technologies to profile the PCFriendly system's users, which "advanced feature" DVD titles are in their collections. (Notably, this token is passed from PCFriendly to an advertising service at NetFlix.com.) Depending on which DVD title installs the software, this will happen with no notice whatsoever, or with an reminder to read the PCFriendly privacy policy that has no link or posted URI.

Additionally, many of the sites we investigated collect personal information like name, address, and email address, but have no stated privacy policy. Others have varying levels of disclosure about the data collection and privacy-related practices of the sites and their operators. It is important to note that PCFriendly is an enabling technology, connecting the DVD content to Web content provided by the DVD producers. It is the DVD producers and Web content developers involved responsible for privacy erosion taking place.

2 How PCFriendly Works

PCFriendly is a Microsoft Windows application created by InterActual Technologies, Inc. When a DVD title is put into a Windows machine, the system will recognize the PCFriendly application, which will be started, alerting the user that the DVD contains "advanced features" which may be now used. If the user proceeds, the PCFriendly application is installed on the machine. The application includes "channels" that will provide the user with buttons to identify various sites that can be visited. Users can then watch the content as they would any other DVD title, with the exception that there's the additional benefit of a banner ad at the bottom of the viewer and some extra navigation buttons in the "channels" frame on the screen. Additional content might be suggested to the user (presumably in the "channels" window, but we don't really know) based on what InterActual knows about the user, as collected through the use of PCFriendly.

2.1 Who Knows What, When

Registration data, including name, address, email address, and age are gathered from the user. A unique "user ID" is created—interestingly, the number seems to be created on the client. The client tests to see whether it's on the network with a "ping" (ICMP ECHO) to www.pcfriendly.com. After the return of the ping from the server, an HTTP connection is made to www.pcfriendly.com that will alert PCFriendly to the user's presence. The format of the connection is fairly consistent, created such that InterActual knows:

- The user's ID (represented as a long hexadecimal number). (This is effectively a cookie that never expires.)
- Some sort of version identifier (perhaps of the PCFriendly software).
- A number to identify the DVD title in the drive.
- `NONE`—we don't know what this field is.
- `1`—perhaps some kind of bit; we don't know how it's used.

2.2 Types of Connections Made to InterActual

Analysis of the connections to InterActual show that there are several, consistent types of connections in the backchannel.

- `RemoteAgentUpgrade.dll?RemoteAgentDownloadA`
  Initiating, just after the installation of PCFriendly, giving the user ID, DVD title, etc., as described above. Also appears when explicitly checking to see whether the installed PCFriendly player is the most recent.
- `RemoteAgentUpgrade.dll?LogfileUpload`
  Makes an HTTP `POST` that includes the user's unique ID, followed by an ASCII `NULL`, and a file compressed with the LZH algorithm. The decompressed file doesn't seem to make sense, but we can identify which file on the user's machine the file is. This requst always directly follows the `RemoteAgentDownloadA` request above, that is, every time the user puts in a new title while online. We do not know whether this includes offline activity.
- `RemoteAgentUpgrade.dll?RegistryUpload`
  Makes an HTTP `POST` that includes the user's unique ID, followed by an ASCII `NULL`, and a file that claims to be compressed with LZH, but apparently is not. If this includes data from the user's Windows registry, this will list all installed PCFriendly DVDs—both those watched while online and offline. It does get bigger as time goes on; data are accumulating there.
- `RemoteAgentUpgrade.dll?BroadcastEventA`
  Makes an HTTP `GET` request in the format of `RemoteAgentDownloadA`, described above.
- `RemoteAgentUpgrade.dll?UpdateUrlA`
  Makes an HTTP `GET` request in the format of `RemoteAgentDownloadA`, described above.
- `RemoteAgentUpgrade.dll?UpdateStateA`
  Makes an HTTP `GET` request in the format of `RemoteAgentDownloadA`, described above.
- `redirect.cgi`
  Makes an HTTP `GET` request that includes these data:

  - `LINK=WH00000002`
    Likely the specific link that was chosen on the interactive menu. Note that the format is always two letters followed by a long number. The first two letters appear to correspond to the publisher. This example is Warner Home Video.
  - `USERID=0x3d92ce40ee0711d4b3af00608c0e42a9`
    This is the hexidecimal user ID seen in other requests.
  - `DISCID=10000013000015000001`
    This corresponds to the DVD title in question.
  - `CHID=00000000000015000001`
    We don't know what this is.

  `redirect.cgi` is the means by which InterActual knows which users clicked which links on which titles in order to connect to the publishers' sites. The client is given an HTTP 302, described below.

- `banner.cgi`
  Makes an HTTP request to connect the user to a web page, in response to clicking a banner ad. The request contains the following data:

  - `BID=20000000000015000001`
    Likely the "banner ID".
  - `USERID=%s`
    This should be the user ID, but `%s` is literally being reported instead of the user's unique ID. This is almost certainly a bug.
  - `DISCID=%s`
    This should be the disc ID, but `%s` is literally being reported instead of the disc's unique ID. This is almost certainly a bug. On some DVDs it works as expected, i.e., the bug has been fixed.
  - `CHID=00000000000015000005`
    We don't know what this is. (Maybe a "chapter ID"—that could make sense in this context, but might not make sense in all contexts. We didn't really analyze this thing's behavior, so we don't know what affects its behavior. "Chapter ID" is a guess.)

  An HTTP 302 is returned, as described below.

- `RemoteAgentUpgrade.dll?BroadcastSuccededA`
  Makes an HTTP `GET` request in the format of `RemoteAgentDownloadA`, described above. It appears to be used to report that a "broadcast" message—an ad that pops up in a dialog box—results in a "More Info" click by the user. In the case we found, this resulted in the `USERID` token being passed to `NetFlix.com` as the `uid` parameter in the query string. Note that it is only the `USERID` (a pseudonym) that is being passed; no marriage of the PCFriendly and NetFlix profiles is possible without access to both sets of data.

Should InterActual and NetFlix merge, for example, it would be possible to link the profiles. The transaction headers follow:

```
GET /?uid=0x0eb2e180f46711d49ea000a0c975d4b1&
  did=1000001500000300006&bid=8 HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0;
  Windows 98; DigExt)
Host: www.netflix.com
Connection: Keep-Alive

HTTP/1.1 302 Object moved
Server: Microsoft-IIS/4.0
Date: Sat, 27 Jan 2001 22:19:55 GMT
Set-Cookie:
  SITESERVER=ID=b686d57ba5d34a4a4853ff3b54e4d009;
  expires=Monday, 01-Jan-2035 00:00:00 GMT;
  path=/; domain=.netflix.com
Location: /validReEntry.asp?sid=820&cookieLessUrl=
  %2FDefault%2Easp&cookieLessQuery=
Content-Length: 194
Content-Type: text/html
Set-Cookie: validReEntryCookie=yes;
  expires=Sat, 01-Jan-2011 08:00:00 GMT; path=/
Set-Cookie: nflx%5Fsid=820; domain=.netflix.com; path=/
Set-Cookie:
  ASPSESSIONIDQGQQQQLS=JPAPAEFBECIAFPKPNLAKJEAF; path=/
Cache-control: private
```

2.3 Types of Responses From PCFriendly/InterActual

Additionally, responses from the PCFriendly site are highly standardized.

- `_INTERACTUAL_OK_`—acknowledges recript of the data and ends the connection.
- `_INTERACTUAL_ERROR_`—causes the client to send the data in a slightly different format, perhaps to resolve some ambiguity.
- `www.pcfriendly.com\update\default.htm`—always given in response to the `UpdateUrlA` request.
- `[English]`—always given in response to "UpdateStateA" request.
- HTTP 302 (redirect)—always given in response to the redirect.cgi requests; these instruct the client to connect to the given URI to complete the request.

3 Other Sites Involved in Investigation

In addition to PCFriendly and InterActual sites, PCFriendly-enabled DVDs we examined linked to other sites.

- `www.warnervideo.com`
  Linked to from *You've Got Mail*. Sets a user-unique domain cookie that expires in 2010:

  ```
  WBWTID=38.194.92.86-3A689F8B0DA000001B4678C-www-terra
  path=/
  expires=Friday, 01-Jan-10 12:00:00 GMT
  domain=.warnervideo.com
  ```

- `www.warnerbros.com`
  From *You've Got Mail*. Ads coming from `ads.entertaindom.com`, `adfarm.mediaplex.com`, and `ng3.ads.warnerbros.com`.

- `www.americangreetings.com`
  Used to send *You've Got Mail* greeting cards. The handoff happens such that `www.warnerbros.com` (the site serving the link) registers the handoff:
  `/event.ng/Type=click&ProfileID=4567&`
  `RunID=21351&AdID=9000&`
  `TagValues=199.1844.3073.3075.3087.3108`
  `&FamilyID=1329&GroupID=380&`
  `Redirect=http:%2F%2Fwww.americangreetings.com`
  `%2Findex.pd%3Fsource%3Dwb101"`

- `www.netflix.com`
  Serves ads. A request is made up of these parts:

  - `uid=0x0eb2e180f46711d49ea000a0c975d4b1`
    This is the *same* `USERID` that is used by PCFriendly. That number is then stored in a .netflix.com domain cookie that expires in 2035.
  - `did=10000015000003000006`
    This is the DVD's `DISCID` used by PCFriendly.
  - `bid=8`
    This seems to be the "banner ID", indicating which ad generated the reqeust to netflix.

  NetFlix doesn't appear to have any connection to PCFriendly; it seems to be just a "partner" of some type, a third party to the transaction. Some registration data:

  ```
  Kibble (NETFLIX2-DOM)
  750 University Avenue
  Los Gatos, CA 95032  US
  Domain Name: NETFLIX.COM
  ```

There has to be some money behind them, though, because they're using Akamai to serve up some parts of the site.

- `activex.microsoft.com`
  Something decided that it needed to `POST` something to `http://activex.microsoft.com/objects/ocget.dll`. What it sent was this: `CLSID={20666967-0000-0010-8000-00AA00389B71}`.

  The server returned a 404 (not found), but that doesn't necessarily mean that Microsoft didn't get the data, and they definitely got the log entry. It isn't clear whether Windows originated this request or PCFriendly.

- DoubleClick
  Some of these things link back to `imdb.com`, which uses DoubleClick advertising; the links are constructed such that it feeds the search terms to their search engine, which in turn pulls the terms out and sticks them in the kw= part of the DoubleClick banner ad URI.

  DoubleClick is also active on the MacroMedia site, which we ended up on because we needed to download some content from their site to make the *Mission: Impossible 2* content work. (We clicked on something, bringing up a dialogue box, to which we answered "yes" and wound up there.)

- *Mission: Impossible 2* has links to Shockwave content, which if downloaded also seems to watch. Note that the `paramount.interactual.com` site sends the user's name, email address, age, language, and page viewed to MacroMedia.

  ```
  http://www.shockwave.com/bin/shockwave/
  visitor/welcome.jsp?first=Ferris&last=Beuler&
  email=ferris_fb%40hotmail.com&pref=y&lang=en&
  age=0&url=http://paramount.interactual.com/mi2/
  training/moto/moto.dcr
  ```

4 Conclusions

InterActual developed PCFriendly to provide additional interactive content to DVD titles. Thus, Internet connectivity is a necessity for the title to work as advertised. Analysis of the system's operation shows that little attention was given to user privacy in the system's original design. In particular:

- Data gathering happened by default.
- A privacy policy did not exist originally. Later software mentions a privacy policy only by name (rather than by link).
- PCFriendly's privacy policy falsely states that data collected are anonymous. Data are collected with a pseudonymous token (`USERID`) that can be linked back to information supplied during product registration, which is quite likely verinymous.

- Commendably, options did exist for turning off various parts of the backchannel, but unless users went looking for them, they were unlikely to be found.

Significantly, the newer version of the software—the InterActual Player—was designed to address privacy concerns. According to InterActual:

> InterActual proactively redesigned its second-generation software to take consumer privacy into account. The InterActual Player software now works in a completely anonymous mode (no personally identifying information), gives complete disclosure of all anonymous information that is tracked, provides controls within the software to limit any data tracking, and provides links directly to the InterActual Player privacy policy for additional information.

We disagree with InterActual's use of the term "anonymous". To be anonymous is to have no name, but as long as users are identified uniquely, they are pseudonymous, which is to have a persistent name, but one separate from one's real life identity. Risks endured by pseudonymous users are significantly different from risks borne by anonymous users [12, 10, 1, 4].

There are two main privacy-related failures here.

Lack of fail-safe default. A privacy-aware system would not assign user IDs or have any profiling of user behavior by default. A safer approach would be to have the software do nothing in the backchannel by default, allowing users to enable the pieces they want [5, 13].

Misunderstanding nymity. Problems resulting from the backchannel are incorrectly understood because InterActual believes that its token is anonymous (no name), when it is in fact pseudonymous (a name, not necessarily connected to the user in other contexts), and if the user registers the product, verinymous (a real name).

These are significant shortcomings, not because InterActual intends to harm users, but because unintended side-effects with significant consequences can arise even in systems designed by competent professionals with the best of intentions [6, 9, 8, 7, 3, 11, 2].

5 Defenses

There are several avenues of defense available to privacy-conscious consumers.

- Do not watch DVD titles on a computer. Backchannels are easy to implement on systems with Internet connectivity.
- Upgrade to the latest InterActual Player. Privacy problems with Web-based content provided by the DVD producers (as opposed to InterActual Technologies) will not be addressed in this case, making this solution incomplete.
- Block all access to `pcfriendly.com` and `interactual.com` domains.

In any case, functionality will be inhibited.

6 Caveat

This report originally compiled on January 31, 2001, and amended in May 2001. PCFriendly's privacy policy, however, has not been updated between December 2000 and February 2002. Additionally, since PCFriendly clients are installed from DVD media, new versions of the software might or might not be in use. Thus, our findings are as relevant in February 2002 as they were in January 2001.

7 Acknowledgment

Paul Graves and Lawrence Williams provided valuable assistance on this project.

InterActual Technologies has been clear, forthright, and prompt in its response to a draft of this article.

A Titles Used in Investigation

- *You've Got Mail*, Warner Brothers
- *The Perfect Storm*, Warner Brothers
- *Chicken Run*, Dreamworks
- *Jurassic Park* (Collector's Edition), Universal Pictures
- *U-571*, Universal Pictures
- *The Emperor's New Groove*, Walt Disney Pictures
- *Blast From the Past*, New Line Cinema
- *Mission: Impossible 2*, Paramount

References

[1] Daniel Bleichenbacher, Eran Gabber, Phillip B. Gibbons, Yossi Matias, and Alain Mayer. On secure and pseudonymous client-relationships with multiple servers. In *3rd USENIX Workshop on Electronic Commerce*, page 99, Boston, Massachusetts, August 31-September 3 1998. USENIX.

[2] Fernando J. Corbató. On building systems that will fail. *Communications of the ACM*, 34(9):72–81, 1991.

[3] Matt Curtin. A failure to communicate: When a privacy seal doesn't help. Technical report, Interhack Corporation, August 2000.

[4] Matt Curtin. Shibboleth: Private mailing list manager. In *Proceedings of the 9th USENIX Security Symposium*. USENIX Association, August 2000.

[5] Matt Curtin. *Developing Trust: Online Privacy and Security*. Apress, November 2001.

[6] Matt Curtin, Gary Ellison, and Doug Monroe. "What's Related?" Everything But Your Privacy. Technical report, The Ohio State University, Department of Computer and Information Science, October 1998.

[7] Matt Curtin, Paul Graves, and Shaun Rowland. Getting to know you (intimately): Surreptitious privacy invasion on the e-commerce web. Technical report, Interhack Corporation, July 2000.

[8] Gary Ellison, Matt Curtin, and Doug Monroe. DoubleClick Opt Out Protocol Failure == Opt In. Technical report, Interhack Corporation, May 2000.

[9] Gary Ellison, Matt Curtin, and Doug Monroe. Opting In, By Accident. Technical report, Interhack Corporation, May 2000.

[10] Ian Avrum Goldberg. *A Pseudonymous Communications Infrastructure for the Internet*. PhD thesis, UNIVERSITY of CALIFORNIA at BERKELEY, 2000. [online] http://www.isaac.cs.berkeley.edu/ iang/thesis-final.pdf.

[11] Paul Graves and Matt Curtin. Bank one online puts customer account information at risk. Technical report, Interhack Corporation, October 2000.

[12] Josyula R. Rao and Pankaj Rohatgi. Can pseudonymity really guarantee privacy? In *Proceedings of the 9th USENIX Security Symposium*, pages 85–96. IBM T.J. Watson Research Center, USENIX Association, August 2000. [online] http://www.usenix.org/publications/library/proceedings/sec2000/rao.html.

[13] Jerome H. Saltzer and Michael D. Schroeder. The protection of information in computer systems. In *Proceedings of the IEEE*, volume 63, pages 1278–1308, September 1975.