UNIVERSITY OF MICHIGAN
INFORMATION TECHNOLOGY SECURITY SERVICES
http://safecomputing.umich.edu

Security considerations of Google Desktop

Desktop search represents an emerging (Q1 2006) market segment designed to make searching your desktop as easy as it is to search the Internet. This paper examines, from a security perspective, one entry in this product space: *Google Desktop*. The goal is to provide information that can be leveraged by the University community to perform a more thorough evaluation or a more secure deployment of Google Desktop.

The conclusions drawn by this paper do not apply to desktop search products in general. However, the methods used may provide a framework for evaluating such products (see **Appendix A** for a list of desktop search products). Based on the analysis presented herein, ITSS makes the following recommendations regarding Google Desktop:

1. Google Desktop should not be deployed
    a. As part of a "standard build" that is available to all users
    b. On workstations that process sensitive (per SPG 601.12) data
    c. In Terminal Server environments
    d. On workstations that do not follow common security best-practices such as automatic OS updates and automatic AV updates
    e. On workstations that leverage external (non-UM) email or IM services
2. Instead, Google Desktop should only be deployed to individual users on an "as-needed" basis in accordance with the following deployment guidelines:
    a. Disable Google Integration
    b. Disable Network Drive Indexing
    c. Disable Indexing of secure web pages
    d. Disable Indexing of Instant Messages
3. In managed Windows environments
    a. Use the *Enterprise* version of Google Desktop so that the recommended configuration settings (above) can be enforced via Group Policy.
    b. Be prepared for "zero-days" in the indexer by ensuring that you can centrally disable it.
4. Finally, make user's aware of
    a. Google Desktop's privacy policies and, in particular,
    b. Privacy concerns with Google Desktop Advanced Features

The remainder of this paper provides an architectural overview of Google Desktop along with the corresponding analysis that led to these recommendations.

January 31st, 2006

Product Description

Google Desktop (GD) is "freeware" that can be downloaded from http://desktop.google.com. Version 1.0 was released on February 27th, 2005 and Version 2.0 (which this paper evaluates) was released on November 1st, 2005. GD provides two primary features. First is the ability to index and, thus, quickly find local desktop content included in email, Office documents, visited web pages, chats, etc. Second is the ability to harness "real-time" information from the web such as news, weather, stock quotes, etc., and present it on, what Google calls, a "Sidebar". Both the desktop search feature and the sidebar feature support a plug-in architecture that allows different content to be indexed or new information to be downloaded as plug-ins become available. There is also a free "Enterprise" version of Google desktop for managed Windows environments that provides a deployable MSI install package and supports configuration management via Active Directory based Group Policy.

Installation

System-wide Setup

GD is initially installed by an administrator in order to copy files into the Program Files directory and to configure per-machine registry values (in HKLM). **Appendices B** and **C** list the per-machine files and registry keys that are created during setup.

GD does not install any user-mode services that start e.g. on system boot. Instead, GD modifies the "run" key (`HKLM\Software\Microsoft\Windows\CurrentVersion\Run`) so that `GoogleDesktop.exe` runs for any user that interactively logs on. `GoogleDesktop.exe`, in turn, spawns `GoogleDesktopIndex.exe` which, among other tasks, provides an HTTP service that listens on TCP port 4664. This HTTP service is not accessible over the network since it binds to the loopback address 127.0.0.1. Just like users connect to `http://www.google.com` to search the web, they can now connect to the web server on their local host (`http://127.0.0.1:4664`) to search their desktop with the same "look and feel" they are already familiar with on google.com.

Besides adding itself to the "run" key, setup also adds `GoogleDesktopNetwork3.dll` to the `AppInit_DLLs` registry value (`HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows`). According to Microsoft Knowledge base 197571, this causes `GoogleDesktopNetwork3.dll` *to be loaded by each Microsoft Windows-based application.* Our research shows, however, that `GoogleDesktopNetwork3.dll` is not ultimately loaded into every Windows GUI application. So either the MS KB article is incorrect, or the dll is getting loaded then unloading itself. One application where `GoogleDesktopNetwork3.dll` does remain loaded in is Internet Explorer (and presumably other browsers). This loading of GoogleDesktopNetwork3.dll into IE appears to be the primary mechanism GD uses to achieve its *web integration* feature discussed later.

Finally, the initial setup phase results in the creation of a Google Desktop icon that subsequently appears on every user's desktop and system tray so that each user can click on the icon to "enable" then subsequently use Google Desktop with their own preferences.

Note that `GoogleDesktop.exe`, `GoogleDesktopIndex.exe` (the HTTP listener), and `GoogleDesktopNetwork3.dll` (in IE) are automatically loaded and run for each user regardless of whether or not a specific user "enables" Google Desktop. Similarly, other dll's such as `GoogleDesktopOffice.dll, GoogleDesktopAPI2.dll` and `GoogleDesktopResources_en.dll` are registered on a per-machine basis and loaded in process for Word, Excel, Outlook, etc. whether or not a specific user ever “enables” GD.

Per-User Options

Normal (non-admin) users “enable” Google Desktop by clicking on the desktop or tray icon that was deposited during admin setup. This step obtains agreement with Google’s EULA and Privacy Policy then allows the user to specify the following options before kicking off the indexing process:

- □ Enable Advanced Features
- ☑ Show sidebar or searchbox
- □ Index and Search my Gmail messages
- ☑ Set Google as my default search engine

The “Advanced Features” option will be discussed further below. Other per-user settings that can be configured post setup include:

- ☑ Search Types (e.g. Email, Office Docs, Media Files, PDF’s etc.)
- □ Plug-ins (for indexing additional content types or extending the “Sidebar”)
- □ Search these locations (for indexing network drives)
- □ Don’t search these items (to exclude certain folders or web-sites from being indexed)
- □ Encrypt Index (to encrypt the search index using NT’s Encrypting File System)
- ☑ Enable Indexing
- ☑ Default Search Type (e.g. Web, Groups, News, Desktop etc.)
- ☑ Show desktop search results as I type
- ☑ Google Integration (for combining Web and Desktop search results)

Several of these options are interesting from a security perspective and will be discussed later.

Indexing

After a user “enables” Google Desktop, `GoogleDesktopCrawl.exe` and `GoogleDesktopIndex.exe` are launched in the user’s context to start “greping” files and building the initial search index. The resulting search database is stored in the user’s profile (under `\Documents and Settings\%USERNAME%\Local Settings\Application Data\Google\Google Desktop Search`). Thus, assuming default Windows XP file permissions, Non-admin *User1* cannot access an index of User2’s files. Of course, if end user’s are running as Administrators, User1 can access User2’s data (and vice versa) independent of Google Desktop.

Once the initial index has been built, it is clear that it is kept up to date by tracking changes – at least for file system objects (email was not tested). Using Filemon.exe from www.sysinternals.com, it is clear that whenever a change is made to a file it is immediately “re-crawled” by `GoogleDesktopCrawl.exe`. Presumably, this is accomplished using directory change notifications although a dependency walker (depends.exe) did not reveal any of the Google code leveraging the typical Win32 file system change notification API’s (`FindFirstChange(), FindNextChange(), ReadDirectoryChanges()`). Interestingly however, the dependency walker did reveal that `GoogleDesktopCrawl.exe` leverages the same DLL (query.dll) that Microsoft’s content indexing service uses to index Office documents!

Searching

Searches are performed by submitting an HTTP request to the local web server (`GoogleDesktopIndex.exe)` listening on TCP port 4664. As mentioned previously, such requests will fail to be heard over the network since the port is available only on the loopback address (127.0.0.1). Additionally, a "key" (i.e. a string of 27 alphanumeric characters and symbols) must be passed as part of the search request. This additional requirement appears to be a safeguard against cross-site scripting (XSS) attacks. In short, it is not enough for an evil script to search: `http://127.0.0.1:4664/search?q=password`, the script must pass a URL that looks like: `http://127.0.0.1:4664/search?q=password&s=LgRzfzxIdqnsg_ImkLZ5u8Nzn34` where the key (`s=LgR…`) changes with each request and is (somehow) shared between the local Google Desktop web server and, as noted above, an appropriately hooked local HTTP client such as IE. It should be recognized however that despite this safeguard, Google Desktop is still susceptible to cross-site scripting vulnerabilities in any of the google.com web sites when the web integration feature is enabled. This will be discussed in more detail later.

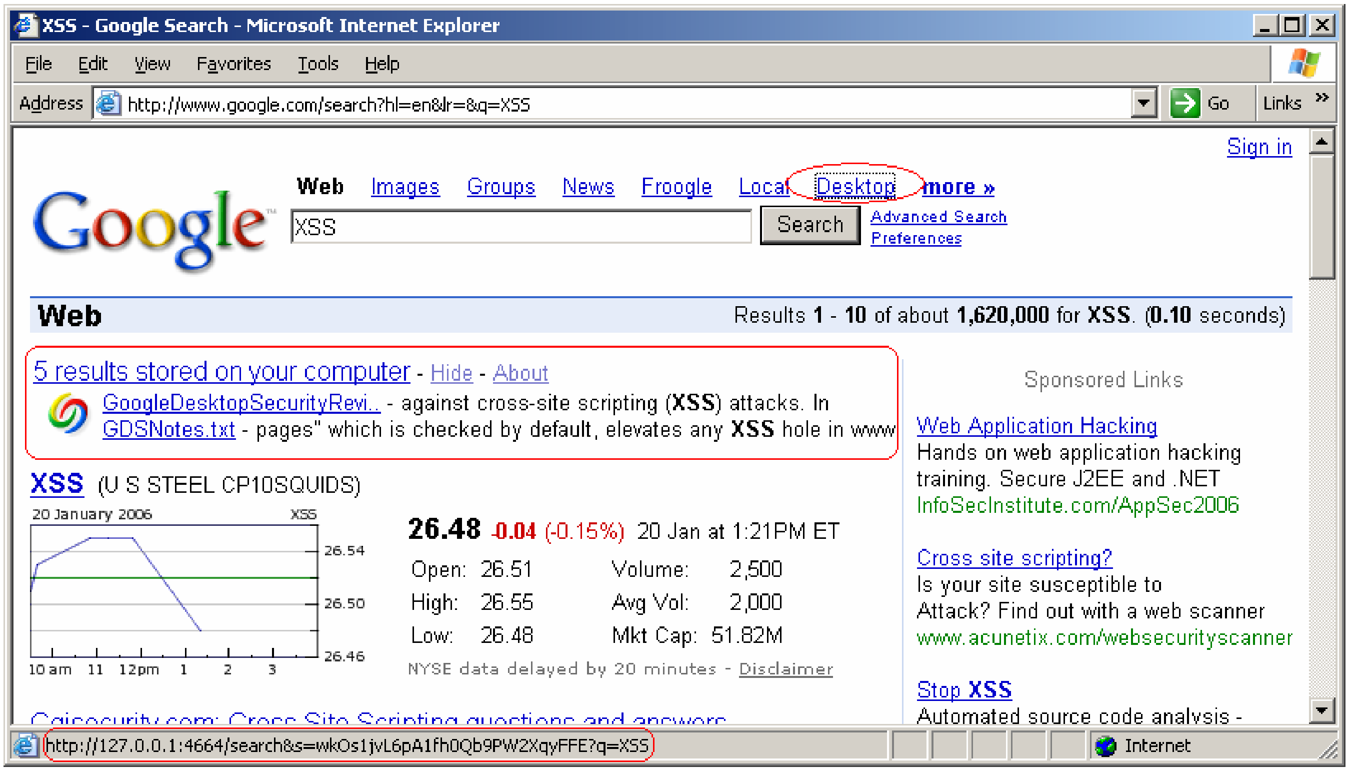
Security Considerations

The previous sections, which provide an overview of the Google Desktop application and some architectural insights, raise some security considerations which are analyzed below:

Google Integration

The most interesting feature of Google Desktop from a security perspective is the "Google Integration" option. There are two aspects of this feature. First, when "Google Integration" is enabled, you will notice that a "Desktop" link automatically appears when you connect to any of the web hosted Google sites (e.g. `www.google.com`, `news.google.com`, `groups.google.com` etc.). Second, the Google Integration feature causes your local desktop to be searched whenever you perform a web search then it displays the combined results from both searches together in one UI.

The following diagram shows the "Desktop" link that is presented when connected to `www.google.com` along with the URL to the local web server (including the secret key discussed previously) that this "Desktop" link references. Additionally, the screenshot illustrates how the desktop search results are combined with, and precede, the web search results.


XSS - Google Search - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.google.com/search?hl=en&lr=&q=XSS
Go
Links »
Sign in
Web Images Groups News Froogle Local Desktop more »
XSS
Search
Advanced Search
Preferences
20 January 2006
XSS
26.54
26.50
26.46
10 am 11 12pm 1 2 3
Internet

Web Results **1** - **10** of about **1,620,000** for **XSS**. (**0.10** seconds)

5 results stored on your computer - Hide - About
GoogleDesktopSecurityRevi... - against cross-site scripting (**XSS**) attacks. In
GDSNotes.txt - pages" which is checked by default, elevates any **XSS** hole in www

XSS (U S STEEL CP10SQUIDS)

26.48 -0.04 (-0.15%) 20 Jan at 1:21PM ET
Open: 26.51 Volume: 2,500
High: 26.55 Avg Vol: 2,000
Low: 26.48 Mkt Cap: 51.82M
NYSE data delayed by 20 minutes - Disclaimer

Cgisecurity.com: Cross Site Scripting questions and answers

Sponsored Links

Web Application Hacking
Hands on web application hacking training. Secure J2EE and .NET
InfoSecInstitute.com/AppSec2006

Cross site scripting?
Is your site susceptible to Attack? Find out with a web scanner
www.acunetix.com/websecurityscanner

Stop **XSS**
Automated source code analysis -

http://127.0.0.1:4664/search&s=wkOs1jvL6pA1fh0Qb9PW2XqyFFE?q=XSS

Our research indicates that the integration of local information into the web-based search is all occurring locally and not over the network. For example, the "Desktop" referral link is not being returned in the HTML from `www.google.com`. Neither are the local search results. Instead, these "local" items are "injected" into the HTML stream that is returned from google.com.

Opinions vary on exactly how this is accomplished. For example, in [1], a claim is made that *"Google Desktop must be observing all outgoing network connections"* and *"performing packet analysis to identify HTTP proxy connections in addition to looking for direct connections to Google"* then *"Integration … occurs after packets are received, but before they are given to the web browser or application"*. If true, this would be quite alarming (you wouldn't want Google Desktop looking at every packet that exits your machine and possibly altering data on the return path up the stack).

Fortunately, we do not believe this is how the "Google Integration" feature is being accomplished. To test this, `netcat.exe` and `telnet.exe` were used to issue HTTP requests to google.com from a machine that had Google Desktop installed. None of the data returned back to these applications had any hint of the Google integration features. Instead, we believe the integration is occurring at the browser level via the `GoogleDesktopNetwork3.dll` and the `GoogleDesktopIE.dll` browser helper object (BHO) that we know are loaded in IE (but not in other Windows applications).

To verify this conjecture, we first set the "kill bit" on the `GoogleDesktopIE.dll` BHO and observed that this prevented the local search results from being displayed with the web results – but the search against the local machine was still being triggered and performed. We also noticed that setting the kill bit only worked once. That is, failure to display the combined results occurred once, and only once, on the first query after the kill bit was set. From then on, it was as if the kill bit were never set (even though it was).

Next, `GoogleDesktopNetwork3.dll` was removed from the AppInit_DLLs registry value and the local desktop query ceased to function entirely when issuing a web-based Google query. Thus, it appears that `GoogleDesktopNetwork3.dll` is responsible for "intercepting" Google queries and triggering the same query locally while `GoogleDesktopIE.dll` is responsible for injecting the summary results in front of the web-based results.

While the Google Integration feature does not appear to be as invasive as some reports would indicate, there is at least one serious concern. First, enabling this feature means that your local data is susceptible to any cross-site scripting vulnerability on any of the google.com search sites. This is because a search of your local machine is being conducted (and results are being returned) as a byproduct of issuing a Google search. This completely bypasses the "secret key" safeguard used to prevent cross-site scripting vulnerabilities in non-Google sites.

Just as serious for some users, perhaps, is the "shoulder surfing" scenario. In this case, a user may inadvertently reveal private information while performing a Google search while someone else is present.

Indexing

Google Desktop mines data. In order to do this successfully it must open files and parse their content. This parsing activity is also where an increasing number of vulnerabilities are starting to surface. In the first quarter of 2006 (when this paper was written), vulnerability trends show a demonstrable increase (consistently 1 per week) in file and binary protocol parsing bugs. This trend is consistent with the development of file "fuzzers" that pick up where network fuzzers (used to discover buffer overflows) left off and is expected to continue in a similar vein. From a threat perspective, one should consider this confluence of increased file parsing bugs and expanding data mining capabilities as a landscape that will be ripe for exploitation and be prepared for inevitable zero-days.

Caching

Google Desktop creates cached copies of everything it indexes (your Office documents, your email, the web sites you've visited, your IM conversations, etc.). As a result, this information will likely still be available long after it has been deleted. This behavior may not be expected or desired. Additionally, this behavior may inadvertently violate any retention policies imposed by regulations such as HIPAA, GLBA, SOX, etc. Note that Google Desktop can search network drives in addition to local fixed disks.

Plugins

You do not need to be an administrator to install plug-ins that extend the indexing or sidebar capabilities of Google Desktop. Such plug-ins can be written by anyone. This is noted solely because, historically, security problems have been incorrectly associated with applications when, in reality, the problems originated in poorly written extensions.

Development Concerns

Many of the global system objects (Events, Mutexes, Shared Memory Sections) created by Google Desktop 2.0 are improperly ACL'd. For example, the following BaseNamedObjects are created with no security descriptor defined thus resulting in Everyone having full control:

- `\MUTEXkCaptureComponentStatDataNameId`
- `\_GD_Indexer_Started`
- `\_GD_shutdown_DG_`
- `\kWakeupCrawlNameId`
- `\MUTEXShortcutClicksFilterName`
- `\MUTEXkAlarmManagerNameId`
- `\SHARED_DATA_MEMBER_MUTEXkGMailEnabledIndicatorNameId`
- `\MUTEXkSystemSharedDataNameId`
- `\ShortcutClicksFilterName`
- `\_GD_ReportIds_DG_`
- `\_GD_local_shutdown_DG_1664`
- `\MUTEXkSystemPausedStateNameId`
- `\GD_ThrottlerId`
- `\MUTEXGD_ThrottlerId`
- `\_GD_Disp_Single`
- `\SHARED_DATA_MEMBER_MUTEXkMenuEnabledStateNameId`
- `\_GD_Index_Single_global`
- `\_GD_local_shutdown_DG_1684`
- `\GoogleDesktopIndex.eim`
- `\kCaptureComponentStatDataNameId`
- `\_GD_index_shutdown_DG_`
- `\kSystemSharedDataNameId`
- `\kAlarmManagerNameId`
- `... there may be more???`

In general, this vulnerability type leads to local DoS, privilege escalation, and/or information disclosure attacks. For example, during our testing, Cesar Cerrudo's DumpSS.exe tool was used to dump Google Desktop shared memory sections instantiated by one user from a different user account that was simultaneously logged onto an XP Pro machine via the Terminal Services based Fast User Switching technology.

Independent of the severity of this particular vulnerability (reported to Google on 1/18/06) the fact that global system objects were created with NULL security descriptors and that this made it through QA is not reassuring from a secure development perspective .

Privacy Considerations

Privacy Policy

Initial analysis of network traffic sniffed during the installation and usage of Google Desktop did not reveal any deviations from what Google already acknowledges that they collect. For example, from the privacy policy (included in **Appendix D**) as well as
http://desktop.google.com/support/bin/answer.py?answer=12531&topic=198

- Your copy of Google Desktop includes a unique application number. When you install Google Desktop, this number and a message indicating whether the installation succeeded are sent back to Google. Also, when Google Desktop automatically checks to see if a new version is available, the current version number and the unique application number are sent to Google. The unique application number is required for Google Desktop to work and cannot be disabled.
- If you choose to enable Advanced Features, Google Desktop may send information about the websites that you visit to provide enhanced Google Desktop functions, such as personalizing news displayed in Sidebar. Enabling Advanced Features also allows Google Desktop to collect a limited amount of non-personal information from your computer and send it to Google. This includes summary information, such as the number of searches you do and the time it takes for you to see your results, and application reports we'll use to make the program better.

- Google Desktop accesses the internet to retrieve "favicons" (icons associated with individual websites) for the websites included in your web history. Google Desktop displays these favicons next to your results, making it easier to find the page you're looking for.
- If you've chosen to integrate your Google Desktop and Google Web Search results, Google Desktop contacts Google to determine what Google site(s) to show the "Desktop" link on.
- So that we can improve Google Desktop, the program sends non-personal information about things like the application's performance and reliability to Google. You can turn this feature off at any time by visiting the Preferences page.
- Google Desktop will not send any personally identifying information, such as your name or address, to Google without your explicit permission.

Advanced Features

As recent news stories (http://www.nytimes.com/2006/01/20/technology/20google.html) highlight, there are already privacy concerns with Google's web-based search services. Specifically, Google keeps track of web searches in a way that could be linked back to individuals. The "Advanced Features" option of Google Desktop raises this concern another notch. With the client-side "Advanced Features" option, Google can now track the actual websites that you visit (not just the things you search for). To their credit, Google displays a prominent warning regarding "Advanced Features" during the per-user setup of Google Desktop:

> **Please read this carefully. It's not the usual yada yada.**
> When you use Advanced Features, you may be sending non-personal usage information and information about websites you visit to Google.
>
> For example, Google Desktop sends Google information about the news pages you visit in order to personalize the news you see in Sidebar. We use other non-personal usage data, including crash reports, to help improve Desktop's performance. Please note that none of this data actually tells us who you are; we use it merely to improve Desktop's ability to give you the information that's most relevant to you.

At this point, and anytime thereafter, the user can opt to use "Advanced Features" or not. If disabled, the tradeoff appears to be less "personalization" of the sidebar.

Private Web Pages

As noted earlier, Google Desktop indexes the web sites you visit and keeps a cached copy of those pages. By default however, this does not include pages viewed over HTTPS. However, this is a configurable preference and if this preference is set inadvertently by a user or by other malware, you could be indexing and caching (in the clear) sensitive information that is normally encrypted via SSL.

Conclusion

We reiterate here, the recommendations made at the beginning of this paper along with a short explanation derived from the detailed analysis presented above.

Recommendation 1: Google Desktop should not be deployed

a. As part of a “standard build” that is available to all users
b. On workstations that process sensitive (per SPG 601.12) data
c. In Terminal Server environments
d. On workstations that do not follow common security best-practices such as automatic OS updates and automatic AV updates
e. On workstations that leverage external (non-UM) email or IM services

Explanation 1: Not every user believes that finding information on their desktop is difficult. Since the proposed solution to this problem (i.e. desktop search) provides another attack vector for the convenient harvesting of personal and sensitive business data, the benefits should be weighed against the risk and the solution offered only to those that need it. For sensitive data, where the cost of disclosure is high, the benefit does not seem to outweigh the risk. Another way to look at this is that “all data is not created equal” – unless it is being mined by Google Desktop! While GD allows for the exclusion of certain directories (presumably, in part, to limit the indexing of sensitive data), this is not practically enforceable.

Regarding Terminal Server environments, the improperly ACL’d global system objects represents a significant threat. Note that the attacking user does not need to be running Google Desktop. In fact, testing revealed that multiple instances of Google Desktop running in different user sessions simply did not work anyway.

Finally, limiting deployment of Google Desktop to “managed” environments where systems are kept up to date and information services (e-mail, etc.) are known, allows local administrators or network administrators to respond to the projected incidents by “choking” off or recognizing (via signature) exploitable file formats or by deploying patches for parsing bugs in non-Google components that might be triggered “under the covers” as a result of Google indexing activity.

Recommendation 2: Instead, Google Desktop should only be deployed to individual users on an “as-needed” basis in accordance with the following deployment guidelines:

a. Disable Google Integration
b. Disable Network Drive Indexing
c. Disable Indexing of secure web pages
d. Disable Indexing of Instant Messages

Explanation 2: As explained above, the Google Integration feature essentially ties the confidentiality of your local data to the security of an external web site (*.google.com). This is an unacceptable security posture. Disabling the indexing of network drives, secure web pages, and chat sessions is a self-explanatory reduction in attack surface for University data, data that is otherwise encrypted, and data that has no other “choke point” for identifying and quarantining streams that might exploit parsing vulnerabilities.

Recommendation 3: In managed Windows environments

a. Use the *Enterprise* version of Google Desktop so that the recommended configuration settings (above) can be enforced via Group Policy.
b. Be prepared for “zero-days” in the indexer by ensuring that you can centrally disable it.

Explanation 3: Centralized management of a distributed environment is crucial. Use it if you can.

Recommendation 4: Finally, make user’s aware of

a. Google Desktop’s privacy policies and, in particular,
b. Privacy concerns with Google Desktop Advanced Features

Explanation 4: The University places a premium on the individual’s right to privacy. Google does a nice job trying to grab the attention of the user regarding the privacy implications of “Advanced Features”. If the previous recommendations are followed and Google Desktop is only deployed on an as-needed basis, you may want to reinforce and supplement this message as part of the request process.

Evaluation Process

The information provided in this paper was discovered via behavior analysis and not disassembly or reverse engineering. Specifically, Google Desktop 2.0 was installed on a virtual machine running Windows XP SP2. Common tools such as filemon, regmon, process explorer, and winobj (all available from http://www.sysinternals.com) and Ethereal (http://www.ethereal.com) were used to analyze the installation and runtime behavior of the product.

References

[1] S. Nielson, S. Fogarty, D. Wallach. *Attacks on Local Searching Tools*, Dec. 2004. http://seclab.cs.rice.edu/gdesktop-tr-dec04.pdf

[2] Google Corporation. *Why does Google Desktop Access the Internet?*, http://desktop.google.com/support/bin/answer.py?answer=12531&topic=198

[3] Matan Gillon, *Google Dekstop Exposed: Exploiting an Internet Explorer Vulnerability to Phish User Information*, Nov. 2005. http://www.hacker.co.il/security/ie/css_import.html

[4] Google Corporation. *Google Desktop Privacy Notice*, http://desktop.google.com/privacypolicy.html.

Appendix A: Desktop Search Products

- *Ask Jeeves Desktop Search*, Ask Jeeves Inc. (http://sp.ask.com/docs/desktop)
- *BeeText Find*, BeeText, (http://www.beetext.com/Find_series.htm)
- *blinkx*, Blinkx Inc. (http://blinkx.com)
- *Copernic Desktop Search*, Copernic Technologies Inc. (http://www.copernic.com)
- *dtSearch*, dtSearch Corp., (http://www.dtsearch.com/)
- *The File Seeker, (*http://sourceforge.net/projects/fileseeker)
- *Google Desktop Search*, Google Inc. (http://desktop.google.com)
- *IDOL Enterprise Desktop Search*, Autonomy Corporation. (http://www.autonomy.com/content/Products/IDOL_Desktop/)
- *ISYS:desktop*, ISYS Search Software. (http://www.isysusa.com/products/desktop/index.html)
- *Watson*, Intellext. (http://www.intellext.com/)
- *Windows Desktop Search*, Microsoft Corporation. (http://www.microsoft.com/windows/desktopsearch/default.mspx)
- *X1 Desktop Search*, X1 Technologies. (http://www.x1.com/)
- *Yahoo Desktop Search*, Yahoo Inc. (http://desktop.yahoo.com)

Appendix B: System-wide files installed during Google Desktop setup

By default, the following files are created in `%ProgramFiles%\Google\Google Desktop Search`:

- `aa ### WARNING - Do not`
- `ab ### move or delete these`
- `ac ### files - your system`
- `ad ### may stop working`
- `ae ###`
- `af ### To uninstall use`
- `ag ### Add-Remove programs`
- `ah ### in the control panel`
- `ai ### or run`
- `aj ###`
- `ak ### GoogleDesktopSetup.exe - uninstall`
- `al ###`
- `GoogleDesktop.exe`
- `GoogleDesktopActions.dll`
- `GoogleDesktopAPI2.dll`
- `GoogleDesktopCrawl.exe`
- `GoogleDesktopDeskbar2.dll`
- `GoogleDesktopDisplay.exe`
- `GoogleDesktopEncdet.dat`
- `GoogleDesktopHyper.dll`
- `GoogleDesktopIE.dll`
- `GoogleDesktopIndex.exe`
- `GoogleDesktopMail.exe`
- `GoogleDesktopMozilla.dll`
- `GoogleDesktopMozilla.png`
- `GoogleDesktopMozilla.src`
- `GoogleDesktopMozillaStub.js`
- `GoogleDesktopNetwork3.dll`
- `GoogleDesktopOE.exe`
- `GoogleDesktopOffice.dll`
- `GoogleDesktopPanels.dll`
- `GoogleDesktopResources_en.dll`
- `GoogleDesktopSetup.exe`
- `gzlib.dll`
- `pdftohtml.exe`
- `plugin_common.js`
- `plugin_common.vbs`
- `uninstall.ico`
- `\temp`

The following files are installed in
`\Documents and Settings\All Users\Start Menu\Programs\Google Desktop`:

- `Google Desktop Preferences.lnk`
- `Google Desktop.lnk`
- `Uninstall Google Desktop.lnk`

Other files created include:

- `\Documents and Settings\All Users\Desktop\Google Desktop.lnk`

Appendix C: Per-machine registry values created during Google Desktop setup

Note: For the sake of brevity, only the “root” keys that are created during setup are shown. If you are interested in the “unabridged” list, contact itss@umich.edu.

```
HKLM\SOFTWARE\Classes\AppID\actions.DLL
HKLM\SOFTWARE\Classes\AppID\gds_deskband.DLL
HKLM\SOFTWARE\Classes\AppID\{0F106145-25A5-4008-99E0-9C8FC1655906}
HKLM\SOFTWARE\Classes\AppID\{785C5BC4-9E0D-4CB3-A72D-32B2C4344FD9}
HKLM\SOFTWARE\Classes\CLSID\{0EE2B1C1-0357-4175-A2E1-8E8E1A033AE5}
HKLM\SOFTWARE\Classes\CLSID\{163BDD74-7164-4940-84B3-575898032CF9}
HKLM\SOFTWARE\Classes\CLSID\{1AB608BF-2E3F-4337-A0EA-FE6FD26F271F}
HKLM\SOFTWARE\Classes\CLSID\{1C7556A4-0B6C-46E8-846B-30F70177AA47}
HKLM\SOFTWARE\Classes\CLSID\{295E081E-1920-4D5C-802A-77D6B48C0856}
HKLM\SOFTWARE\Classes\CLSID\{2B62A832-2CA2-4843-86CA-45450D35EADA}
HKLM\SOFTWARE\Classes\CLSID\{2C6F11D4-CF22-4E1F-A271-2A4A0393ADAC}
HKLM\SOFTWARE\Classes\CLSID\{2F47A051-6AA3-4E7A-A5F5-2446708AFA18}
HKLM\SOFTWARE\Classes\CLSID\{33407F76-4054-4026-A9D2-DCC99FFBC18A}
HKLM\SOFTWARE\Classes\CLSID\{3872340B-239E-4C1C-A783-0E2A5E28383B}
HKLM\SOFTWARE\Classes\CLSID\{38F4C281-2396-424B-8B62-F236B44ADB02}
HKLM\SOFTWARE\Classes\CLSID\{3C66FE03-4FB7-497C-850F-60265842D043}
HKLM\SOFTWARE\Classes\CLSID\{40BC80C0-5B92-44F6-91CE-6D000C9AACF5}
HKLM\SOFTWARE\Classes\CLSID\{4516155C-B94E-4334-8D26-D4BF0932581C}
HKLM\SOFTWARE\Classes\CLSID\{50EDABE0-140C-406D-A8B9-32652145560A}
HKLM\SOFTWARE\Classes\CLSID\{579822B3-44CD-4786-83E0-AE32BCB9E6B1}
HKLM\SOFTWARE\Classes\CLSID\{5A734302-566D-4C1C-B805-4643F6A95565}
HKLM\SOFTWARE\Classes\CLSID\{6233543C-2323-456A-A169-2E9C5E6E977B}
HKLM\SOFTWARE\Classes\CLSID\{634E2122-6BB7-430F-B452-CF04C8722C47}
HKLM\SOFTWARE\Classes\CLSID\{640D184A-33D6-4FAB-B654-9EF19DB9F8FD}
HKLM\SOFTWARE\Classes\CLSID\{654AF3CA-DE94-4ABA-A4EE-9EB7E595BF6A}
HKLM\SOFTWARE\Classes\CLSID\{65E256AC-B335-4004-8C6A-5A7F986CD0A4}
HKLM\SOFTWARE\Classes\CLSID\{68E27672-0C2E-4F54-8B21-71DD68DFE343}
HKLM\SOFTWARE\Classes\CLSID\{6A515151-B135-458A-AE5C-985B5796B5FA}
HKLM\SOFTWARE\Classes\CLSID\{6B74AF68-3196-47E1-B3EE-FDFCEE692867}
HKLM\SOFTWARE\Classes\CLSID\{750E7D70-00AD-400A-96E3-78DD2B0431FC}
HKLM\SOFTWARE\Classes\CLSID\{75CCC48F-8C8A-4E21-896E-AB408D3592D0}
HKLM\SOFTWARE\Classes\CLSID\{81C68D76-253A-409F-9DFE-3A815655254D}
HKLM\SOFTWARE\Classes\CLSID\{8269ECFE-EC9A-44B3-906D-6CA873E7B1B6}
HKLM\SOFTWARE\Classes\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\TreatAs
HKLM\SOFTWARE\Classes\CLSID\{9130995A-B2F2-47C7-BD60-BC02E950A8A8}
HKLM\SOFTWARE\Classes\CLSID\{92177D99-F713-4CA2-B8E5-6537F5FC0571}
HKLM\SOFTWARE\Classes\CLSID\{94BB7FC1-B109-4628-9D15-6B4F8B9BF73C}
HKLM\SOFTWARE\Classes\CLSID\{9D763E7F-3EE1-4527-9AA2-CAA63091AF08}
HKLM\SOFTWARE\Classes\CLSID\{A05168CF-A880-4ED4-A17A-AE0AB04EC3EE}
HKLM\SOFTWARE\Classes\CLSID\{A1A81D4E-E268-4D5B-8D50-4E6720DECC2E}
HKLM\SOFTWARE\Classes\CLSID\{A1E23136-DA3C-49F3-9DF5-C209A89C03AA}
HKLM\SOFTWARE\Classes\CLSID\{A27060E0-6921-4C82-8C15-935620B73ED3}
HKLM\SOFTWARE\Classes\CLSID\{A5B8FE6A-E3E1-40F3-8189-630E37C2AA47}
HKLM\SOFTWARE\Classes\CLSID\{A5E46E3A-8849-11D1-9D8C-00C04FC99D61}\TreatAs
HKLM\SOFTWARE\Classes\CLSID\{A6C13C27-BA4F-43CE-B674-D6DA5321DC2A}
HKLM\SOFTWARE\Classes\CLSID\{AC129136-EB1C-4FFF-B0A2-6D6761BE4138}
HKLM\SOFTWARE\Classes\CLSID\{B334CA23-40EE-4556-A808-3EAA3E80517E}
HKLM\SOFTWARE\Classes\CLSID\{B583A8F7-33EC-4B7C-91F5-1B59D104309A}
HKLM\SOFTWARE\Classes\CLSID\{BB8B07A0-B8D1-44E0-A262-C9B7212AEC68}
HKLM\SOFTWARE\Classes\CLSID\{CCE15A15-75F9-4F05-AFF0-194FB588D26B}
HKLM\SOFTWARE\Classes\CLSID\{CCF3BB94-B83B-49C8-B6D8-27F6C3D93299}
HKLM\SOFTWARE\Classes\CLSID\{CFDAF37E-E5DA-475A-850D-74BAA1A9A8C5}
HKLM\SOFTWARE\Classes\CLSID\{D413C502-3FAA-11D0-B254-444553540000}
HKLM\SOFTWARE\Classes\CLSID\{D496FA5F-11C0-4EA8-A364-3A6BF8565EE6}
HKLM\SOFTWARE\Classes\CLSID\{D8F989E6-F339-4745-A952-DA0F1E57E426}
```

```
HKLM\SOFTWARE\Classes\CLSID\{E4FB3DDB-5CAD-42DA-8E22-DB9B04041350}
HKLM\SOFTWARE\Classes\CLSID\{ECCB4495-7F5B-4B4E-A887-7A66BE948AC1}
HKLM\SOFTWARE\Classes\CLSID\{F11D7457-2381-4337-977F-4090C75EBC23}
HKLM\SOFTWARE\Classes\CLSID\{F2CDFE24-8E06-4134-B588-61C90D51DD10}
HKLM\SOFTWARE\Classes\CLSID\{FBA13A6F-E595-48B7-AB73-2630042A4E93}
HKLM\SOFTWARE\Classes\CLSID\{FC4482E9-08FC-493A-BA7D-7ED5A6DD0938}
HKLM\SOFTWARE\Classes\CLSID\{FD7C32EA-3546-447A-8D4D-667FDB0F904A}
HKLM\SOFTWARE\Classes\CLSID\{FDD6F22F-18EA-4DA9-9AA7-FD2309ADF211}
HKLM\SOFTWARE\Classes\GoogleDesktop.ActionRegistration
HKLM\SOFTWARE\Classes\GoogleDesktop.ActionRegistration.1
HKLM\SOFTWARE\Classes\GoogleDesktop.ContentItemHelper
HKLM\SOFTWARE\Classes\GoogleDesktop.ContentItemHelper.1
HKLM\SOFTWARE\Classes\GoogleDesktop.DetailsViewHelper
HKLM\SOFTWARE\Classes\GoogleDesktop.DetailsViewHelper.1
HKLM\SOFTWARE\Classes\GoogleDesktop.DisplayPluginRegistration
HKLM\SOFTWARE\Classes\GoogleDesktop.DisplayPluginRegistration.1
HKLM\SOFTWARE\Classes\GoogleDesktop.EmailDefaultActions
HKLM\SOFTWARE\Classes\GoogleDesktop.EmailDefaultActions.1
HKLM\SOFTWARE\Classes\GoogleDesktop.EventPublisher
HKLM\SOFTWARE\Classes\GoogleDesktop.EventPublisher.1
HKLM\SOFTWARE\Classes\GoogleDesktop.EventRegistration
HKLM\SOFTWARE\Classes\GoogleDesktop.EventRegistration.1
HKLM\SOFTWARE\Classes\GoogleDesktop.FilterCollection
HKLM\SOFTWARE\Classes\GoogleDesktop.FilterCollection.1
HKLM\SOFTWARE\Classes\GoogleDesktop.IndexingRegistration
HKLM\SOFTWARE\Classes\GoogleDesktop.IndexingRegistration.1
HKLM\SOFTWARE\Classes\GoogleDesktop.OfficeAddin
HKLM\SOFTWARE\Classes\GoogleDesktop.OfficeAddin.1
HKLM\SOFTWARE\Classes\GoogleDesktop.Registrar
HKLM\SOFTWARE\Classes\GoogleDesktop.Registrar.1
HKLM\SOFTWARE\Classes\GoogleDesktop.SchemaFilter
HKLM\SOFTWARE\Classes\GoogleDesktop.SchemaFilter.1
HKLM\SOFTWARE\Classes\GoogleDesktop.SchemaPropertyFilter
HKLM\SOFTWARE\Classes\GoogleDesktop.SchemaPropertyFilter.1
HKLM\SOFTWARE\Classes\GoogleDesktopSearch.EventFactory
HKLM\SOFTWARE\Classes\GoogleDesktopSearch.EventFactory.1
HKLM\SOFTWARE\Classes\GoogleDesktopSearch.Register
HKLM\SOFTWARE\Classes\GoogleDesktopSearch.Register.1
HKLM\SOFTWARE\Classes\Interface\{00378CC2-78D4-45F8-A0D4-63836C675F58}
HKLM\SOFTWARE\Classes\Interface\{04D8CD86-CF9C-46C1-9BA0-BA069B3469E7}
HKLM\SOFTWARE\Classes\Interface\{06246CA4-B5E9-4B38-9462-F81CC3E01983}
HKLM\SOFTWARE\Classes\Interface\{07E881F2-7871-4CD4-BC6D-9D9BD6805CBE}
HKLM\SOFTWARE\Classes\Interface\{08A02699-A4BC-41A0-BFEE-A58395ED22A7}
HKLM\SOFTWARE\Classes\Interface\{0990D80E-EFF7-4119-9FC8-0C247AF43794}
HKLM\SOFTWARE\Classes\Interface\{0E74FEB9-CD68-4171-A3D5-4E1DCF7EB072}
HKLM\SOFTWARE\Classes\Interface\{0F561F9B-1706-43DE-A9BB-4DC5D047A100}
HKLM\SOFTWARE\Classes\Interface\{107A6055-EE5E-4454-BF50-79B6FBA4B85A}
HKLM\SOFTWARE\Classes\Interface\{151857B2-26E0-4F4D-ACED-4F7E4B2065EF}
HKLM\SOFTWARE\Classes\Interface\{1668C88E-4BBA-4569-AFCD-DB1015B6519C}
HKLM\SOFTWARE\Classes\Interface\{18F5CD0D-A205-47BE-AA55-FDEEEA85E730}
HKLM\SOFTWARE\Classes\Interface\{19CFBC40-9AF2-4F90-A5E3-1FEFC05403D7}
HKLM\SOFTWARE\Classes\Interface\{1C3CA604-EAFB-49C4-B47D-04799E577CB7}
HKLM\SOFTWARE\Classes\Interface\{1D15CE63-019C-4598-912A-3A50BF8EA735}
HKLM\SOFTWARE\Classes\Interface\{1EEE64A7-8BBC-4A7F-95FC-22470180E286}
HKLM\SOFTWARE\Classes\Interface\{225C3090-A83E-446A-A230-3E653D3F5837}
HKLM\SOFTWARE\Classes\Interface\{2BF1B7EE-DC5C-4F05-8DFA-273D6C199567}
HKLM\SOFTWARE\Classes\Interface\{2C4F95B0-EE5B-4D93-98ED-BBD0C2913976}
HKLM\SOFTWARE\Classes\Interface\{337D06C5-93E9-4F2B-A78C-9ED2234602F1}
HKLM\SOFTWARE\Classes\Interface\{35AD5708-ED56-494B-9866-374DFFDCFF5A}
HKLM\SOFTWARE\Classes\Interface\{36EDCC27-2F1D-4578-8F1E-714216F8CFF6}
HKLM\SOFTWARE\Classes\Interface\{3E467448-EC21-4A24-BFCD-2DF951214F00}
HKLM\SOFTWARE\Classes\Interface\{4052D303-74C5-49EA-BC6B-66099C8D4007}
HKLM\SOFTWARE\Classes\Interface\{43D89A8F-0440-409F-AD13-B5C9B18EE5BF}
HKLM\SOFTWARE\Classes\Interface\{4BDAEFD6-04C4-4A90-880C-F4670250AC01}
HKLM\SOFTWARE\Classes\Interface\{4E37FB82-3FC3-4464-A7AE-D3B9E90E11A7}
HKLM\SOFTWARE\Classes\Interface\{4F7B07A2-2D63-4520-899E-1F71B5957F3B}
```

```
HKLM\SOFTWARE\Classes\Interface\{51D91A41-1B56-4F69-AD80-1F4299A95DDC}
HKLM\SOFTWARE\Classes\Interface\{5E72293F-05C2-4C1A-8E4E-3158EC3D8574}
HKLM\SOFTWARE\Classes\Interface\{666677EB-2C7A-4393-ABB1-A5994E8D09CB}
HKLM\SOFTWARE\Classes\Interface\{66F9F427-03C9-462F-85AF-88F362620FB0}
HKLM\SOFTWARE\Classes\Interface\{77C5FC10-7876-4E3E-A499-276FD1796E23}
HKLM\SOFTWARE\Classes\Interface\{78C5468E-8074-414E-B16C-11979124FD1A}
HKLM\SOFTWARE\Classes\Interface\{79EDFDE2-6BC6-41BD-A54C-F8AFF2F3789A}
HKLM\SOFTWARE\Classes\Interface\{7B015F1A-B3C2-4C95-9186-A1ED218AB78F}
HKLM\SOFTWARE\Classes\Interface\{7DE4137F-B1DF-4786-AEA0-192EA48643C6}
HKLM\SOFTWARE\Classes\Interface\{81FA4BC2-E8B9-496D-B385-333369F28EC4}
HKLM\SOFTWARE\Classes\Interface\{8D230931-1C13-48D3-A73C-4EF5F1E4E576}
HKLM\SOFTWARE\Classes\Interface\{8EA92B6D-7D6C-436C-AF9F-2F508601BADF}
HKLM\SOFTWARE\Classes\Interface\{953EE805-9014-4B5D-8233-1DA9BCF1BC5B}
HKLM\SOFTWARE\Classes\Interface\{9575DED8-9BA4-4A3B-83AA-59B2CAD0CDEF}
HKLM\SOFTWARE\Classes\Interface\{96D278A0-92BF-450A-BFBC-26A5743EEB4D}
HKLM\SOFTWARE\Classes\Interface\{9B311E80-BC95-4518-A58C-446EC9A082B5}
HKLM\SOFTWARE\Classes\Interface\{9CBE5894-03B1-48C9-922A-CE5C886252F3}
HKLM\SOFTWARE\Classes\Interface\{A1DE6DB8-B20F-445C-BFDE-16C8D53A2FA1}
HKLM\SOFTWARE\Classes\Interface\{A4F5748B-DD06-4486-9AF8-6ACAFBED35DB}
HKLM\SOFTWARE\Classes\Interface\{A79E51C6-DB2D-4A44-848E-A8EBB22E5337}
HKLM\SOFTWARE\Classes\Interface\{B1ABA2A3-79A1-4D5E-B556-1C2F1B3EC7A7}
HKLM\SOFTWARE\Classes\Interface\{B41F373F-04FE-4D69-A972-DEB002444278}
HKLM\SOFTWARE\Classes\Interface\{B59107C8-55E2-4389-909E-B0ED8783CDC2}
HKLM\SOFTWARE\Classes\Interface\{B7734D6E-C899-4322-B811-B973071D6628}
HKLM\SOFTWARE\Classes\Interface\{B7BC8A9B-DC73-42D4-AB7D-17178619C8E4}
HKLM\SOFTWARE\Classes\Interface\{BBF09E2A-4E2A-4377-A4A7-980CC55F140B}
HKLM\SOFTWARE\Classes\Interface\{BC18CC8F-D1D6-485D-BF12-7C705BEAAF51}
HKLM\SOFTWARE\Classes\Interface\{BDAC0047-4759-43A1-BA04-B148E1679E87}
HKLM\SOFTWARE\Classes\Interface\{C3173C82-8B78-4F08-B19A-A65B7F48630A}
HKLM\SOFTWARE\Classes\Interface\{CB93C531-A7EE-4396-A026-17A44D384B65}
HKLM\SOFTWARE\Classes\Interface\{CCEE9332-AB1E-45BB-818A-9347E80721D4}
HKLM\SOFTWARE\Classes\Interface\{D7D23586-2724-4B05-AF2D-67B94703FEEA}
HKLM\SOFTWARE\Classes\Interface\{E1263168-954B-4359-B41F-9680CEECC94F}
HKLM\SOFTWARE\Classes\Interface\{E17F1A5B-5BEA-4713-A4E0-7315282E76E0}
HKLM\SOFTWARE\Classes\Interface\{E42581BB-17F1-4483-8C66-6066C9CF7686}
HKLM\SOFTWARE\Classes\Interface\{E5D57628-4068-42C8-94AC-8017A8AC8CBF}
HKLM\SOFTWARE\Classes\Interface\{E6442369-CB8C-4623-A9AD-C5A01AECA1ED}
HKLM\SOFTWARE\Classes\Interface\{E7C0BEB7-446B-43BF-83E3-5EC37A9DBCC8}
HKLM\SOFTWARE\Classes\Interface\{EB959B93-5C03-4267-9441-660A05DBB89F}
HKLM\SOFTWARE\Classes\Interface\{EEE5E27F-67A0-4CF3-A8B6-D0A5A9E22B85}
HKLM\SOFTWARE\Classes\Interface\{F3534261-9E76-435C-8AD7-C1406B5E1C83}
HKLM\SOFTWARE\Classes\Interface\{F38DFE0C-9C42-4DDC-970E-256A5DC5D5CD}
HKLM\SOFTWARE\Classes\Interface\{FAC60E5D-9D0E-42AB-ADBD-137373C5073E}
HKLM\SOFTWARE\Classes\Interface\{FC4F92BD-C3B6-44C6-A44B-DAFA5E528BD5}
HKLM\SOFTWARE\Classes\Interface\{FEF90C69-4A90-46BE-9B9E-C547AA10F170}
HKLM\SOFTWARE\Classes\TypeLib\{0265F4FC-85A3-4EA6-BD9A-74BC24F8682D}
HKLM\SOFTWARE\Classes\TypeLib\{26866851-46D4-4B25-ABFC-14FF93FB7C13}
HKLM\SOFTWARE\Classes\TypeLib\{3D056FE7-EA8E-481A-B18F-0B02EBF6B3C1}
HKLM\SOFTWARE\Classes\TypeLib\{A4CD2F29-6213-4301-8A95-4E414329FCB7}
HKLM\SOFTWARE\Classes\TypeLib\{ACD1A266-C77B-4691-B96A-AF712B83A364}
HKLM\SOFTWARE\Classes\TypeLib\{E3B60D50-19AB-4A32-A8B1-A09113AB2BA4}
HKLM\SOFTWARE\Google
HKLM\SOFTWARE\Google\Desktop
HKLM\SOFTWARE\Google\Google Desktop
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Google Desktop
```

Appendix D: Google Desktop Privacy Policy

From http://desktop.google.com/privacypolicy.html

October 14, 2005

The Google Privacy Policy describes how we treat personal information when you use Google's products and services, including information provided when you use Google Desktop. In addition, the following describes our privacy practices that are specific to Google Desktop.

Information we collect

- The Google Desktop application indexes and stores versions of your files and other computer activity, such as email, chats, and web history. These versions may also be mixed with your Web search results to produce results pages for you that integrate relevant content from your computer and information from the Web. Your computer's content is not made accessible through Google Desktop to Google without your explicit permission.

- Your copy of Google Desktop includes a unique application number. When you install Google Desktop, this number and a message indicating whether the installation succeeded are sent back to Google. Also, when Google Desktop automatically checks to see if a new version is available, the current version number and the unique application number are sent to Google. The unique application number is required for Google Desktop to work and cannot be disabled.

- If you choose to enable Advanced Features, Google Desktop may send information about the websites that you visit to provide enhanced Google Desktop functions, such as personalizing news displayed in Sidebar. Enabling Advanced Features also allows Google Desktop to collect a limited amount of non-personal information from your computer and send it to Google. This includes summary information, such as the number of searches you do and the time it takes for you to see your results, and application reports we'll use to make the program better.

Uses

- We use this information to deliver the best possible service to you, such as improving the Google Desktop user experience and providing automatic updates of new versions of Desktop.

Your choices

- You can choose to enable Advanced Features during installation and you can change your mind at any time in Desktop Preferences. Personally identifying information, such as your name or address, will not be sent to Google without your explicit permission.

- The business version of Google Desktop includes some functionality that is set by your administrator. Your administrator may choose not to have Google receive the unique application number associated with your copy of Google Desktop or the Advanced Features information and aggregate usage data described above.

- If there are any files or other data that you do not want indexed by Google Desktop, there are several ways that you can keep this data from being displayed, copied and indexed, as well as ways to remove it from the index after it has been included. You can see specific instructions on removing items in the user guide.

- You can uninstall the Google Desktop software through the "Add or Remove Programs" Control Panel at any time. When you uninstall the software, you can choose to delete the Google Desktop index and its copies of all items. If you choose to delete this information the original files and applications remain unaffected.

More information

Google adheres to the US Safe Harbor privacy principles. For more information about the Safe Harbor framework or our registration, see the Department of Commerce's web site.

Further information about Google Desktop is available here.

For more information about our privacy practices, go to the full privacy policy. If you have additional questions, please contact us any time. Or write to us at:

Privacy Matters
c/o Google Inc.
1600 Amphitheatre Parkway
Mountain View CA 94043 (USA)