

Usability and privacy: a study of KaZaA P2P file-sharing

Nathaniel S. Good

School of Information Management
University of California, Berkeley
ngood@sims.berkeley.edu

Aaron Krekelberg

Office of Information Technology
University of Minnesota
kreke002@umn.edu

ABSTRACT

P2P file sharing systems such as Gnutella, Freenet, and KaZaA, while primarily intended for sharing multimedia files, frequently allow other types of information to be shared. This raises serious concerns about the extent to which users may unknowingly be sharing private or personal information.

In this paper, we report on a cognitive walkthrough and a laboratory user study of the KaZaA file sharing user interface. The majority of the users in our study were unable to tell what files they were sharing, and sometimes incorrectly assumed they were not sharing any files when in fact they were sharing *all* files on their hard drive. An analysis of the KaZaA network suggested that a large number of users appeared to be unwittingly sharing personal and private files, and that some users were indeed taking advantage of this and downloading files containing ostensibly private information.

Keywords

Privacy, peer-to-peer networks, security, usability, user studies

INTRODUCTION

The excitement about P2P systems has been encouraged by recent innovations that foster easier sharing of files, such as downloading simultaneously from multiple sources, and the sharing of many different file types, as well as improvements to the usability of these clients. Of the current P2P systems, KaZaA is by far the most popular and widely used, with over 120 million downloads worldwide and an average of 3 million users online at any given time. The user interface (UI) for finding files is straightforward: the user types a query into a textbox and from the results selects a matching filename to download. If sharing is enabled, the files that the user downloads are then automatically shared with other users on the network. The success of a P2P file sharing network depends on people sharing files with one another, so this features helps promote file sharing by recycling files in the network.

While facilitating file sharing and searching, the systems do a poor job of preventing users from accidentally sharing personal files. Users attracted to the simplicity of downloading files provided by the P2P network can inadvertently allow access to their private data files, such as email, tax reports, work related spreadsheets and private documents. This is especially problematic in a single machine, multiple user situation typical of families sharing a single computer. In such a setting, a parent could have a secure VPN connection to a corporation for downloading and working on important confidential files, only to have them inadvertently shared by a teenage son or daughter, without either party's knowledge. This is not simply a theoretical problem but describes a scenario that is possible in the current reality. Our research suggests that people are unintentionally sharing and what appear to be personal or confidential files via KaZaA. Queries for files such as Inbox for Outlook Express (.dbx files), data for financial applications, and .pst files (Microsoft Outlook mail folders) returned numerous results.

In order to understand how this can take place, we examined KaZaA's UI and use from a variety of perspectives to determine if usability issues could account for such fatal errors. KaZaA is interesting from a usability perspective because it is widely used by millions of users with varying degrees of computer experience, has crossed over from a select group of expert users to a more general population, and has challenging UI issues it must address to preserve users privacy while facilitating file-sharing. We feel that lessons learned from KaZaA are applicable to designers working with other P2P systems, as well as with other kinds of continually connected systems where users manage access control and share information (KM applications, expert finding, etc.). From a more general perspective, we hope that our study provides a concrete example of the challenges in designing UIs that both encourage participation and protect privacy, and guidelines for building these kinds of systems.

Recent literature examined usability guidelines for user interfaces for security applications. Whitten and Tygar [8] looked into usability problems that affected users sending secure messages via PGP¹, and how inadequate design

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

CHI 2003, April 5-10, 2003, Ft. Lauderdale, Florida, USA.

Copyright 2003 ACM 1-58113-630-7/03/0004...\$5.00.

¹ PGP – pretty good privacy <http://www.pgp.com/>

Upload								
Title	Artist	Progress	Status	Uploaded/Requested	Time Remaining	Speed	Filename	
Inbox			Completed	2172Kb/2172Kb			Inbox.dbx	
Inbox			Completed	1480Kb/1480Kb			Inbox.dbx	
Inbox (1)			Completed	22764Kb/22764Kb			Inbox (1).dbx	

Figure 1 Inbox.dbx files being downloaded from our dummy client by other KaZaA users

caused users to make fatal mistakes such as sending unencrypted messages that they felt were encrypted or sending people their private keys. Yee [9] has expanded on this work, and provides a list of guidelines and case studies for usability of security applications. His work builds on that of Saltzer and Schroeder [6] which focused on understanding the design requirements for developing secure systems.

While KaZaA is not a security application like PGP or personal firewall software, it nonetheless has privacy implications for its users. It must help them ensure that data is not accidentally shared with others. We used an approach inspired by the success of Whitten and Tygar [8] in identifying the flaws within PGP 5.0. We performed a cognitive walkthrough and a user study to analyze the interface of KaZaA and determine usability issues that could cause users to share files unintentionally with the KaZaA network. The results detailed below show that usability issues alone could account for unintentional file sharing. Indeed, we were able to determine from our user studies that it was possible for users to share all files on their hard drive and not even know it.

Credit Cards	Credit Cards.xls	Completed
Credit Cards	Credit Cards.xls	Completed
Credit Cards	Credit Cards.xls	Completed

Figure 2 "Credit Card.xls" files KaZaA users downloaded from our dummy client.

Abuses on KaZaA Today

We looked at other P2P networks, such as Gnutella, for similar problems. We found that over a 24 hour period we were able to find files such as inbox.dbx on these networks as well, yet in fewer numbers than KaZaA. We attribute this to the much smaller user base of Gnutella. Because Gnutella is an open protocol, unlike KaZaA there are many different client programs that use it, each with a different interface. Focusing on the KaZaA interface gave us the benefit of a large user base and a consistent UI, from which we hoped we could generalize a solution for all kinds of P2P clients.

We were curious to see how widespread the problem of unintended filesharing is on the current KaZaA network, and whether users are currently taking advantage of others' mistakes to download private files from them. In order to do this, we scripted searches to run every 1.5 minutes for a 12 hour period. KaZaA operates on a closed

protocol, so it is not possible to determine the full extent of people sharing personal files, as one cannot tell exactly how much of the network is being searched with every query.

Unintended Filesharing Among KaZaA users

In our searches of the KaZaA network, we purposely limited ourselves to queries only, and did not download any user files to verify their contents. The targets of the searches were files that end in .dbx with particular emphasis on inbox.dbx. DBX files are Microsoft Outlook Express email files. This is a good indicator that users are unintentionally sharing files for several reasons. First, DBX files are commonly found on Windows machines because they are packaged with Internet Explorer and Windows. Second, they contain private email correspondence that most users would not likely intend to share. Finally, we had discovered that users who have their inbox shared typically had other files shared that contained what appeared to be private information.

The results of 443 searches in 12 hours showed that unintentional file sharing is quite prevalent on the KaZaA network. 61% of all searches performed in this test returned one or more hits for inbox.dbx. By the end of the 12-hour period 156 distinct users with shared inboxes were found.

To further demonstrate that this indicates unintentional file sharing, we examined 20 distinct cases of shares on the inbox.dbx file by manually using the "find more from same user" feature. 19 of the 20 users shared the other email files found in the default Microsoft Outlook Express installation (Sent Items, Deleted Items, Outbox, etc.) In addition, 9 users had exposed their web browser's cache and cookies, 5 had exposed word processing documents, 2 had what appeared to be data from financial software and 1 user had files that belong in the system folder for Windows.

Users Downloading Others' Private Files

After we determined that users were indeed sharing private files, we were interested in whether other users on the KaZaA network were taking advantage of this fact and downloading files from others. We ran a dummy client populated with dummy files (such as Credit Cards.xls, Inbox.dbx, Outlook.pst and other types of files that were intended to appear to be private) over a 24 hour period.

From our dummy server, we received a total of four downloads from four unique users for an Excel spreadsheets named "Credit Cards.xls" and four downloads from two unique users of an Inbox.dbx file (Figure 2).

This study was done while the author was an intern at IDL in Hewlett-Packard Labs, Palo Alto CA.

USABILITY GUIDELINES

By looking at the KaZaA network, we surmised that abuses are occurring, and their frequency demonstrates that they are not isolated events.

Based on a list of security guidelines provided by Whitten and Tygar [9], we created a modified list of usability guidelines adapted for Peer-to-Peer File sharing applications below, that take into account the unique demands of continuously connected systems that distribute personal files.

Definition: Peer-to-Peer file sharing software is safe and usable if users:

1. are clearly made aware of what files are being offered for others to download.
2. are able to determine how to share and stop sharing files successfully.
3. do not make dangerous errors that can lead to unintentionally sharing private files, and
4. are comfortable with what is being shared with others and confident that the system is handling this correctly.

We then conducted a cognitive walkthrough and user study, paying close attention to whether or not the interface was able to meet these guidelines, and if not, why were users confused.

RESULTS OF THE COGNITIVE WALKTHROUGH

Recent versions of the KaZaA application have made some progress in addressing access control issues. A default installation of KaZaA for users using a recent version of KaZaA 1.7.1 is relatively safe; it creates a shared file folder, assigns this as the default download file and indexes these folders for the My KaZaA library. Various versions of KaZaA had various settings, and had different default configurations. The latest version of KaZaA 1.7.2 (the most recent at this time) and other previous versions of KaZaA offered to search for files to share with users during the initial setup. In the latest version at the time of this writing and in some previous versions, file sharing is enabled. While a default setup where file sharing disabled, as in version 1.7.1, is relatively safe, user modification of various settings are not. By adding or changing directories to be shared, there are potential interface issues that can create misunderstandings about what files the system is sharing with other users, regardless of the version of KaZaA that the user is using. There are a number of reasons why a user would change default settings. Three common scenarios are driven by a user's desire to save the files being downloaded to a different location, share more files with other users or add files to their shared files folder-. In the following sections, we will walk through each of these scenarios and the various ways that KaZaA allows these to be accomplished. We will look at the various safeguards

that KaZaA employs to prevent users from sharing private files or files that they do not want others to see, and describe where they seem likely to fail.

Changing the Download file directory

In KaZaA, as in most P2P applications, the default shared directory, provides the dual purpose of specifying the files that the user decides to share with the network, and the place where these files will be stored. The default-shared directory, is (confusingly) alternatively referred to as the 'My Media', 'My Shared Folder', 'My KaZaA' and the 'folder for downloaded files' in KaZaA.

The 'My Shared Folder' refers both to a folder created on the machine by KaZaA and abstractly to all folders that the user shares. For simplicity, we will refer to the 'My Shared Folder' as the actual folder that KaZaA creates by default to share files, and all files allocated for sharing as the 'shared files'. The 'My Media' and 'My KaZaA' folders list all the shared files, yet organize it according to media type, such as music, video, documents, etc. For purposes of simplicity we will refer only to 'My Media'. The 'folder for downloaded files' refers to the folder where download files will be stored, but also the root folder of all shared files. Although each folder is used in a different context, they are essentially different names for the same thing, a list of files that KaZaA can share with others.

While the 'My KaZaA' and 'My Media' folders are accessible through clearly visible buttons, specifying shared files and the 'folder for downloaded files' are managed through the Options menu, in the tool tab (Figure 4). Additionally, the Options->Tools tab also contains a checkbox for users to determine whether they would or would not like to share files with the KaZaA community. Users may type in the name of the directory they would like to download files to, or alternately browse their file system and select the folder they would like to use to store downloaded files (Figure 3).

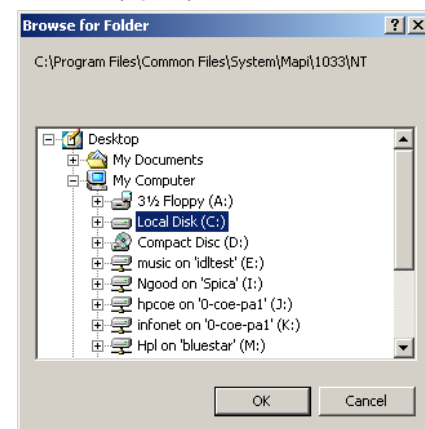


Figure 3 Browsing and selecting interface for the shared Download Folder. Note that the interface says browse for folder, and does not mention that sub-folders will be recursively searched for files.

If the user has decided to share files with others, then all files in this directory as well as the directories below it are recursively shared, and added to My Media files (**Error! Reference source not found.**). The wording of the download folder is confusing. The word “folder” is singular, implying one folder, and does not hint that all folders below it will be recursively shared with others. More misleadingly the name “download folder” implies that it will be used to store files that are downloaded and has nothing to do with sharing. It does not mention that this folder (and the folders and files underneath) will also be shared with others, if sharing is enabled.

Another factor leading to user error is that hierarchical file systems can be very difficult for some users to navigate and conceptualize. Vicente [7] demonstrated that users with low spatial ability have trouble navigating hierarchical file systems compared to those with high spatial ability. Novice users are “notoriously bad” at navigating hierarchical file structures and prefer breadth as opposed to depth in browsing and searching for files or information. The trade offs between depth and breadth in hierarchical structures has been well studied by the psychological and human computer interaction communities [2,3,4,5]. Most reach the conclusion that breadth is better than depth. ‘Shortcuts’ on the Windows desktop are frequently created to allow users one click access to file folders buried in hierarchies. However, by automatically recursing through directories for files, KaZaA presumes, at the same time, that all users have a detailed knowledge of their file system and its contents. At the very least, users should be given a choice to recursively add files or not when asked to share a folder.

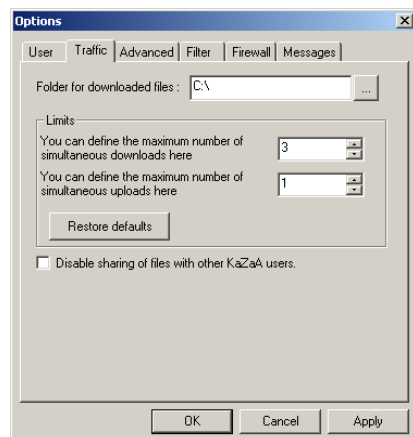


Figure 4 The traffic tab in the options folder. Here is where users specify the download and My Shared directory as well as toggle sharing of all files.

Sharing files

Two interfaces that KaZaA provides for sharing files are located in the Tools Menu, under “Find Shared Files” for version 1.7 and above. Selecting this menu item brings up a dialog box with several choices (Figure 5).

One choice is to have KaZaA automatically discover files for the user by pressing the ‘Search Wizard’ button. The other is for the user to browse their machine and determine which directories to share, which is accessible by selecting the ‘Folder List’ tab, or pressing the ‘Folder List’ button. The find function uses a wizard interface to walk users through selecting drives to search, and select which folders to share after the process has been completed. After searching, KaZaA returns a list of folders that it recommends the user to share with other KaZaA users (Figure 6). In the latest version of KaZaA, it recommends folders containing documents (such as the default Windows My Documents folder), image files, and multi-media files, such as music and video. On a side note, it does not indicate if any of these directories it has found are already being shared using other means. A message (that could easily be ignored) above the list box tells users the steps that they will need to perform in order to stop sharing files in the folders that they select.

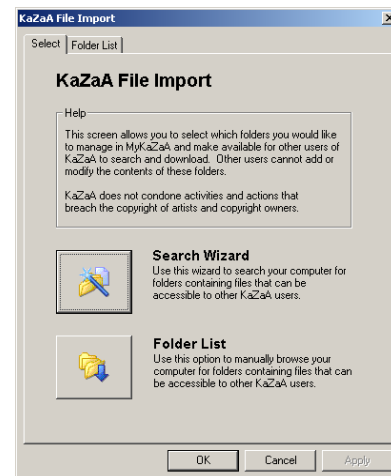


Figure 5 Selection interface to find or select shared folders.

One problem with the ‘Search Wizard’ interface (Figure 6) is that it does not describe what criteria it uses to find folders to share. For example, it does not say what files in the ‘My Documents’ folder will be shared, or describe the particular attributes of the ‘My Documents’ folder that caused it to be recommended for sharing. The interface relies on the user’s knowledge of what is capable of being shared by a file sharing program and what the program is looking for. It presumes that users have perfect knowledge of what kinds of files (and sub-directories with further files) are contained in those folders and that these contents will be recursively shared.

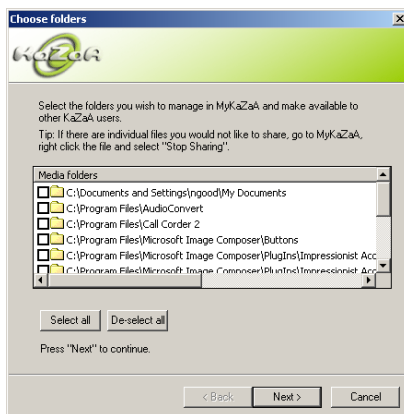


Figure 6 Search Interface

The “tip” portion is the only part of the interface that warns the user that they risk sharing files that they would rather not. It is unclear whether users read this message, and if so, remember the instructions and places they need to go in order to stop sharing such files. It also mentions that users must remove the files one-by-one if they choose not to share them. Overall, while the search interface affords sharing more files, it makes browsing, searching and stopping sharing of specific files within shared folders difficult and tedious.

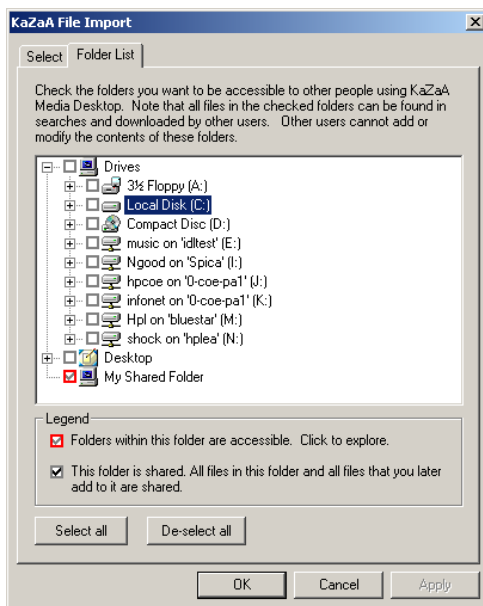


Figure 7 Folder Select Function to share or stop sharing folders

The other function, which we will call the folder select function, has a UI that allows the user to browse the current file system and select a folder or folders to share. Folders are shared by selecting a checkbox, and are restricted from sharing by deselecting the checkbox. When a user selects a directory, the directories below it

are selected automatically for the user (**Error! Reference source not found.** and Figure 9). When they deselect a directory the directories below are also deselected.

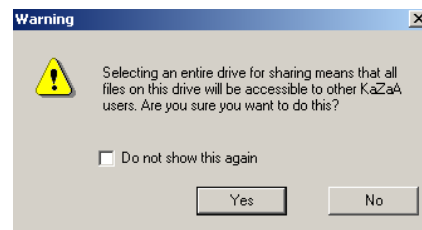


Figure 8 Warning to not share the entire folder from the Folder Select Function.

If a users selects a drive, (such as C drive) a message pops up (Figure 8) warning the user that this action will share all files with all KaZaA users for this drive. This warning will not appear again if any user on a given machine decides to check “Do not show this again”, and future users sharing the same machine will not be able to see this warning.

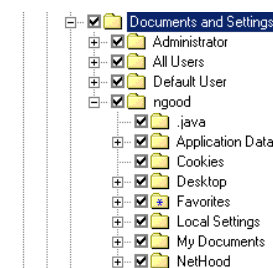


Figure 9 Expanded View of folders selected by selecting Documents and Settings.

We noticed that if file sharing was enabled (through the UI in Figure 4) and the user had changed the download directory to something else, this change was not reflected in the folder select window, Figure 7. For example, if a user changes their download directory to C:\ and sharing is enabled, they are sharing their whole hard drive. All of these files are indexed by ‘My Media’, but there is no indication in the checkbox, like the one in Figure 8, in the folder select function (Figure 7). We found this to be a critical flaw that the participants in the study below found to be misleading. In effect, it allowed users to share anything through the download folder, and not be aware of it through the folder selection function. In the user studies conducted below, this error had serious repercussions for user expectations of shared folders and files.

Adding Files to the My Media Folder

KaZaA, like most file sharing programs, comes with a built in media player that allows playback of a variety of audio and video formats. Playback of these formats is done through the My KaZaA tab, which organizes files

based on their content into file folders, similar to the interface provided by Microsoft Internet Explorer. To add files to My Media, they must be shared or included in the download directory as described above or through another button that “imports” files into My Media, using similar techniques to those described above.

Files imported into the *My Media* folders can be turned on and off individually via a context menu, accessible through right clicking the file with the mouse, or an icon above the file folders. The context menu is only activated for individual files, and does not work at the top folders or root folders of the directory structure. For example, if a user wanted to disable sharing of applications in the software folder, the only choice they would have would be to disable sharing entirely, or stop sharing each individual file. Also, there is no indication of exactly what folders are being shared on the user’s hard drive. In the usability study described below, the My Media folder was a source of general confusion. The participants’ opinions about its purpose and contents varied greatly.

Uploading Files

During the walkthrough we examined the *Transfer File* interface that allows users to determine what is currently being uploaded and downloaded to and from the KaZaA network. It consisted of two scrollable lists. Files being transferred to others are appended to the bottom of the file transfer list, and this list is cleared every time KaZaA is restarted, erasing any past transactions. Users therefore have to be very attentive to what is being transferred in KaZaA, in order to be aware of any unwanted file shares.

Summary of Usability Guidelines

We summarize the results of the cognitive walkthrough below in relation to how well KaZaA satisfies each of the earlier proposed guidelines.

1. **FAILED:** *Users should be made clearly aware of what files are being offered for others to download.*

From the cognitive walkthrough, we see that bugs, assumptions of users’ knowledge in searching and selecting files, and unclear labeling clearly make it difficult for users to determine what is offered for others to download. Nowhere in the interface were we able to determine which types of files can be shared.

2. **FAILED:** *Users should be able to determine how to successfully share and stop sharing files.*

The cognitive walkthrough revealed many ways to share files, but demonstrated that there are few ways to stop sharing files. The ways that do exist are complicated and difficult to find. Again, unclear labeling is confusing and misleading, complicating the problem.

3. **FAILED:** *Users should not be able to make dangerous errors that can lead to unintentionally sharing private files*

Files and folders shared through the download folder, are not indicated as such in other parts of the interface. This is

a serious flaw that could easily allow users to make fatal mistakes.

4. **FAILED:** *Users should be sufficiently comfortable with what is being shared with others and confident that the system is handling this correctly.*

In the cognitive walkthrough, it was difficult to determine which types of files could be shared, when KaZaA was sharing them, and with whom. Without constantly monitoring KaZaA, it is difficult to tell what the system is doing with the files and whom they are sharing them with.

4. A TWO-PART USER STUDY

We attempted to devise a test to determine how easy it is for users to misconfigure their system. After several trials, we discovered that our attempts to devise a realistic scenario involving sharing and specifying file locations became contrived and only confused our test participants. Nor could we simulate the length of time over which settings are most likely changed and then forgotten during real use. In addition, we could not speculate on all of the various reasons users would want to change their default settings, although we knew from our data that they were indeed modifying the settings and were not aware of it.

From anecdotal evidence, we know that KaZaA users often work in shared computer settings, so it is quite possible for one user to change all the settings and another to know nothing about it. We were able to contact and interview 4 online users who had accidentally shared their inboxes and talk to them about their configurations. These users indicated that they had either changed the settings to make files easier to find (1 of 4), or that they shared a computer with other people who may have changed the settings without their knowledge (3 of 4). For this reason, and given the difficulties with any other realistic trial described above, we decided to make a very simple test to simulate this scenario. We would share all files on the hard drive (as if we were a user sharing the same machine) and see how easy it was for participants to determine what, if anything was being shared.

Our study consisted of 12 participants. Ten of these had used file-sharing applications before (such as Morpheus, Gnutella, KaZaA and Napster) and 2 had not. All the users spent over 10 hours a week on their computers.

The two parts of the study are described below.

KaZaA Sharing Comprehension Questions

We were interested in the participants’ conceptions of the types of files that peer-to-peer filesharing applications can share, as well as whether they were able to perform the specified task. We asked the participants to indicate what types of files could be shared over peer-to-peer networks.

Current Sharing Settings Discovery Task

The participants were initially presented with the KaZaA interface which had been preconfigured in the following manner.

- File sharing was enabled (thus the My Shared Folder was being shared).
- The download directory was set to C:\, effectively sharing all files on the harddrive as well.
- KaZaA indexed all of C:\, and displayed the file information into the “My Media” folder.

In order to prevent others from downloading our files, we set up KaZaA behind a firewall and blocked incoming requests to download files. This prevented others from actually accessing our files, but still allowed KaZaA to index all the files and provide them for sharing.

Participants were given a short tutorial on file sharing, and the concept of a shared folder. They were then asked to discover what files were currently being shared, if any, on a KaZaA media desktop running KaZaA version 1.7.1. All participants were given the same setup and told to take as much time as they needed. They were only allowed to use the KaZaA interface, and at the end of their search were asked to provide a clear answer of whether they thought files were being shared and if so, which folders they were in.

If participants correctly determined that files were being shared, we asked them to stop sharing them, and share only the ‘My Shared Folder’.

RESULTS

KaZaA Sharing Comprehension Questions

Only 2 participants indicated correctly that all files could be shared. One more participant indicated correctly that it was also possible to share office documents, source code files and email folders. The nine remaining participants believed that only multimedia files such as music, video and pictures could be shared. After completing the task, some participants were very surprised to learn that all files could be shared with others and some couldn’t understand why. One participant exclaimed, “You mean it shares *all* files?” and expressed concern about why it would be able to share anything other than multi-media files. These results from our study bolster those from our cognitive walkthrough to demonstrate that KaZaA is in clear violation of the first guideline above: Participants should be made clearly aware of what files are being offered for others to download.

Current Sharing Settings Discovery Task

Only 2 of the 12 participants were able to determine correctly which files and folders were currently being shared. Of those 2, both were able to turn off sharing completely using the “stop sharing feature” (Figure 4), but were not able to determine how to stop sharing a single given folder. Of the remaining participants:

- 5 of 12 determined incorrectly that the ‘My Shared Folder’ was the only folder being shared, based on the information they saw from the folder select feature

(Figure 7), which, as we found in our cognitive walkthrough, does not update itself based on current sharing status.

- 2 of 12 used the find files interface to search for folders they were sharing. When everything showed up unchecked (Figure 6), the participants concluded incorrectly that nothing was being shared.
- 2 of 12 browsed help and used it to determine incorrectly that the only folder they could share was the ‘My Shared Folder.’
- 1 of 12 was unable determine what folder was being shared after going through every menu item in the application and the help. The participant said that the files in the ‘My Shared Folder’ were probably being shared but admitted that they couldn’t determine what, if anything, was in that folder.

Many participants found the initial interface difficult to navigate. Several participants traversed the web interface to look for help in determining what KaZaA shared and how. In the help section, some participants tried to use the “search” function, assuming incorrectly that it searched help and not the KaZaA network. Of the participants who were able to make it to the menus in the toolbar at the top of the application, only one was able to make the connection between the “download folder” (Figure 4) and the “My Shared Folder” described in the help and shown on the folder selection feature (Figure 7). Participants had difficulty finding the main menus in the top toolbar, and had difficulty understanding the labeling on the menu items, which made it hard for them to traverse the menu hierarchies to determine where they could control filesharing. One participant later described the experience as a “buckshot approach” to find out what was where. The participant mentioned that “he had no clue” where to look for shared folders, and resorted to looking through every menu item for something that made sense.

There was considerable confusion about ‘My Media’. Less than half of the participants thought that items in ‘My Media’ were being shared with others, the rest either thought it held an archive of all media on the machine for personal use, or assumed it contained some shared and some unshared items. Only three participants could determine which items were shared and which weren’t by looking at the file icons, but all were unsure of which folders in ‘My Media’ contained shared items and which contained items not being shared without browsing each individual folder.

SUGGESTED DESIGN IMPROVEMENTS

Based on what we found in the surveys, participant studies and cognitive walkthrough, we have several suggestions that may help improve the current interface:

- Prohibit or curtail sharing of files that are not multimedia files. For example, non-multimedia files could be shared using a more safety conscious, or advanced

participant interface. As most participants in our study were unaware of the fact that they could share files other than multimedia, this would realign users expectations with the current reality. We feel that current interface is weighted too heavily in favor of sharing files. Our usability studies suggest that improvements can be made to create a balance between sharing files easily (to encourage KaZaA uptake by making sure there is a wealth of content available) and protecting and preserving users privacy.

- ☐ Provide better 'feedforward' about the consequences of recursion in sharing of folders and sub-folders.
- ☐ Provide a more rigorous interface that explicitly supports users' efforts to make exceptions to recursively shared folders, or otherwise warns users that they have not checked sub-folders in a folder that is being selected for sharing.

5. CONCLUSION

While the interface provided by KaZaA affords simple sharing and file download features we find that its sharing interface is problematic. The design presupposes sophisticated user understanding of file sharing, and fails all four of the usability guidelines that we developed based on Whitten and Tygar's earlier work [9].

By providing several different locations and interfaces to manage file sharing and not integrating them, users are not made aware of which files are being offered for others to download and are not able to determine how to successfully share and stop sharing files. Ambiguity and erroneous assumptions about recursion and which types of files can be shared allow users to make dangerous errors, such as sharing an entire hard drive. Finally, the confusing multiple purposes of the 'My Media' interface cause confusion about what is actually being shared. Given the potential violation of user privacy and the current abuses that we noted above, it should be a top priority for file sharing applications to look into usability for security applications, and design their applications accordingly.

We believe that measures to protect privacy need not reduce the amount of content that attracts users to such shared networks. Rather, they will simply avoid the unintentional sharing of a large amount of personal and

confidential content that is unlikely to appeal to bona fide users anyway.

ACKNOWLEDGMENTS

Thanks to Mary Czerwinski, Paul Dourish, Marti Hearst and the IDL group at HP Labs for helping with early drafts of this document. Special thanks to Victoria Bellotti and Marti Hearst for help with the final draft, and to the University of Minnesota Office of Information Management for allowing us to use their computers to run our study.

REFERENCES

1. Jacko, J. A. B Salvendy, G. (1996). Hierarchical menu design: Breadth, depth, and task complexity- Perceptual and Motor Skills, 82, 1187-1201.
2. Kiger, J. I. (1984). The depth/breadth tradeoff in the design of menu-driven interfaces International Journal of Man-Machine Studies, 20,201-213.
3. Larson, K. and Czerwinski, M., Web page design: implications of memory, structure and scent for information retrieval, Conference proceedings on Human factors in computing systems, pp. 25-32, ACM
4. Milner, G. A. (1956). The magical number seven plus or minus two: Some limits on our capacity for processing information. Psychological Review, 63, 81-97.
5. Miller, D. P. (1981). The depth/breadth tradeoff in hierarchical computer menus. Proceedings of the Human Factors Society, 296-300.
6. Saltzer, J. H. and Schroeder, M. D.. The Protection of Information in Computer Systems. In Proceedings of the IEEE, vol. 63, no. 9, September 1975, pp. 1278-1308 (see <http://web.mit.edu/Saltzer/www/publications/protection/>).
7. Vincente, K.J. and R.C. Williges, Accommodating Individual Differences in Searching a Hierarchical File System. International Journal of man Machine Studies, 1988. 29
8. Whitten A. and Tygar, J. D.. Why Johnny can't encrypt. In Proceedings of the 8th USENIX Security Symposium, August 1999.
9. Yee, K.-P.. User Interaction Design for Secure Systems, ICSIS 2002, Singapore
10. Zaphiris, P. & Mtei, L. (1997). Depth vs Breadth in the Arrangement Web Links. Available at <http://otal.umd.edu/SHORE/bsO>