ShareSniffer: An interesting look at data sharing

By Jeremy Shane Horn
March 12, 2001

Introduction

Over the last few months, Napster has become a household name for anyone with a PC. But what is all the hype really about? Well, that depends which perspective you take on the situation. From the Napster point of view, we the public, should be allowed to share our data any way and with anyone we choose, in this particular case data meaning music files. However, from the perspective of record companies, and ultimately the courts, it is not legal or ethical to promote or make possible the sharing of copyrighted material with others. But what about the sharing of data other than music or MP3 files? Is this legal? Or more importantly, is it safe?

A Security Perspective on the Matter

The purpose of this paper is to discuss the concepts of data sharing over the Internet and to introduce a new software application, ShareSniffer, which has recently become available and strongly promotes data sharing in a dangerous way. But first, let me start by briefly describing the most popular, Napster, and one of its cohorts, Gnutella.

Napster is, or maybe I should say was, a client/server based application which enables users to locate and voluntarily share media files with other users. [(1)] Since the court ruling in early March, which prohibits Napster from encouraging or allowing the sharing of copyrighted music files over their network, many other data sharing applications have surfaced. Gnutella seems to be the most popular of the 190 applications that I have found.

As we all know, everything evolves and in the case of data sharing, the client/server topology is quickly evolving into a peer-to-peer (P2P) topology. This is where Gnutella comes into play. Gnutella essentially is a protocol, or technology if you will. Basically, the Gnutella client software serves as a tiny search engine and file serving system in one. Meaning no pesky servers because every Gnutella client acts as a client when it requests information and a server when it shares information. As you can probably see, with a P2P topology there is no one place to point the finger and say “Shutdown or else”. [(2)]

What does all this really have to do with security? I’m glad you asked. Applications like Napster or Gnutella, or the numerous other utilities out there, all have one important thing in common and that is ‘participate at your own risk’. If you are concerned about the spread of malicious code, Trojan horses, or someone finding a way into your PC from one of these applications then simply don’t use them. It is just that simple. But what happens when the choice to participate in data sharing is taken out of the users’ hands?

As most of us know, every computer connected to the Internet has an IP address assigned to it. Whether a computer connects via an Internet Service Provider (ISP) or by means of cable modem, the computer's assigned IP address is unique. This address can be thought of as the computer's street address where we might find it in the virtual world of the Internet. Therefore, if we know a computer's location or IP address, we can simply use Windows Explorer and type in "*// IP_address* " and if the computer is online and has any open shares on the machine, they will magically appear in Windows Explorer as if it were our own computer's file system. Unfortunately, if someone wanted to search a large number, or block, of IP addresses, it would take a very long time. This is where ShareSniffer takes over

What is ShareSniffer?

"ShareSniffer is a powerful shared resource browser." [3] In short, ShareSniffer is a GUI application that makes it possible to search a block of IP addresses for unprotected-shared information. Once the scan is complete, ShareSniffer returns a list of IP addresses with open shares. Once you have the IP address, and you know that open shares exist, you can do what you wish with the shared information (i.e. modify, delete, copy, etc.). Pretty scary stuff! Especially when you think of how many internet users are out there that have very little or no knowledge of information security. Now comes the really interesting part. When ShareSniffer locates unprotected shares, it creates a list of the new discoveries and creates a newsgroup message that posts these discoveries in an article to an Internet-based mail forum. By default this newsgroup is "*alt.sharesniffer*"[3 Now let's take a look at the interface and some additional functionality of ShareSniffer.

Tool Description

The following information is a brief summary of the product description that can be found at ShareSniffer's web page. [3]

System Requirements

Actually, the only specifications are that of any Windows operating system.

Protocol Requirements

It is necessary to have Client for Microsoft Networks (CMN) enabled. ShareSniffer will not work without this particular protocol. In addition to CMN, Windows File and Printer Sharing (WFPS) is required if the user wishes to have the ability to view public share IP addresses and their contents through Windows Explorer.

The Interface

ShareSniffer uses a Multiple Document Interface. On the main Window, resides the toolbar. As seen in Fig. 1

Fig. 1

The **Toolbar** is similar to other Windows based applications in its appearance. It contains the follow actions:

- **Start Sniffing** - which starts the sniffing process
- **Stop Sniffing** - which stops the sniffing process and resets the current NetBlock
- **Pause Sniffing** - which pauses the sniffing process, but does not reset the NetBlock
- **Properties** – This action enables users identify the owner of a given domain and e-mail the owner about any questions or concerns about that domain or NetBlock.
- **Cascade** – which cascades all child windows
- **Tile Vertical/Horizontal** – (2 separate features) these features tile all open child windows vertically or horizontally
- **Arrange Icons –** which arranges the icons of minimized child windows
- **Restore All –** which restores any child windows to their original state
- **Minimize All –** which minimizes all child windows
- **Close All –** which closes all child windows
- **Exit –** of course this is necessary to exit the application
- **Options –** This feature allows users to customize ShareSniffer

The previous features seem to be pretty standard for a Windows application. However, the next few Toolbar features are a key to making ShareSniffer work its hideous magic.

Slide List

Fig. 2

The Slide List feature is described as being part convenience and part necessity. The convenience part is that it is represented on the toolbar. The necessity side is that the lower portion of the Slide List Houses the ‘Nostril Array’. When clicked once with the left mouse button, a Nostril will be loaded and enabled. Another single click would unload and disable the Nostril.

Load ShareFeed

Remember the newsgroup that I mentioned earlier, alt.sharesniffer? Well, this is where it comes into play. When the user depresses the Load ShareFeed button, the application queries the newsgroup, which has been previously defined in the Communications tab of the Options feature, looking for new discoveries that have been posted by other ShareSniffer users.

NetBlock Query

Fig. 3

This feature allows the user to enter text related to IP addresses, which the ShareSniffer user can sniff for exposed shared resources. The NetBlock Query also gives users the convenience of drag-and-drop when it comes to the Discovery Engine window.

Discovery Engine

Fig. 4

The Discovery Engine window allows more of the drag-and-drop functionality. This feature allows any line items to be dragged from essentially any other ShareSniffer child window and dropped into the Discovery Engine window in order to target them for sniffing.

Discovery Results

Fig. 5

This feature is pretty much like it sounds. The Discovery Results window displays the open shares found during a recent sniff. Also, it is possible to right click, with the mouse, to edit the comment associated with the item.

Conclusion

What have we learned? Well, anyone using a Windows operating system can connect to another PC, via the Internet, by simply typing the target's IP address into Windows Explorer, and voila instant access to someone else's open shares. So, why should we be concerned about the ability to access someone else's machine by way of IP addresses? After all, it isn't like this is a new concept to the Windows world.

First of all, we have already seen the automated power that ShareSniffer brings to the table. ShareSniffers can target a whole block of IP addresses, rather than one at a time. ShareSniffers would never have to worry about time constraints of finding open shares across the Internet because with the help of the nifty little newsgroup postings of other ShareSniffers, a great deal of open share discoveries are made easily accessible. Secondly, it's true that the concept of ShareSniffer is not an entirely new one. However, as technology continues to progress, and more and more people jump on the Internet bandwagon, information security will continue to become very important to everyone, not just security professionals. With that said, I will close with a few simple solutions that would prevent users of ShareSniffer from discovering information you don't want them to.

The first and most important thing to remember is 'Know your system'! If you do not wish to share information with others, then make sure you aren't sharing information unintentionally. You can do this by using your Windows Explorer and making sure that under the 'Sharing' properties, 'not shared' is checked. Number two, if you intent to connect to the Internet, get yourself a 'personal firewall' for you PC. These are relatively inexpensive and usually come bundled with anti-virus software. Number three, if you do decide to share information with friends or colleagues then use a strong password. A strong password is one that is at least eight characters long and contains upper and lower case letters, numbers, and non-alphanumeric characters. This is very important, and it will probably be a good idea to change your password often. And finally the most important tactic to stopping ShareSniffers or any other unwanted intruders, make yourself more knowledgeable about the world of information security. Information is always going to need protecting. Whether it be from a ShareSniffer, or a Napster, or any other application that is bound to pop up sooner or later. Information security is an ever changing field that we must try to keep up with or we are destined to fall victim to such applications as ShareSniffer.

References:

1. Napster. “Company Profile” March 11, 2001
   URL: http://www.napster.com/company/

2. Gnutella. “Gnutella – are you read for the ride of your life?”
   URL: http://gnutella.wego.com”

3. ShareSniffer, Inc. “ShareSniffer, Inc.” URL: http://www.sharesniffer.com

4. Poulsen, Kevin. “ShareSniffer turns Windows hacking into a P2P play.” “Napster alternative: other people’s hard drives.”
   URL: http://www.securityfocus.com/news/159

5. Eldred, Lucien. “ShareSniffer – Hacking for Dummies” March 12, 2001
   URL: http://securityportal.com/articles/sharesniffer20010312.html

6. Lynes, Meredith. “Gnutella defeats many perimeter defenses” “Internet File Sharing” June 19, 2000
   URL: http://www.sans.org/infosecFAQ/firewall/gnutella.htm

7. Kasmir, Thomas. “Napster – Should You Be Worried About It?” October 16, 2000 URL: http://www.sans.org/infosecFAQ/napster.htm

8. URS. “UltimateResourcesSite.com”
   URL: http://www.pzcommunications.com/mp3/programs/main.htm