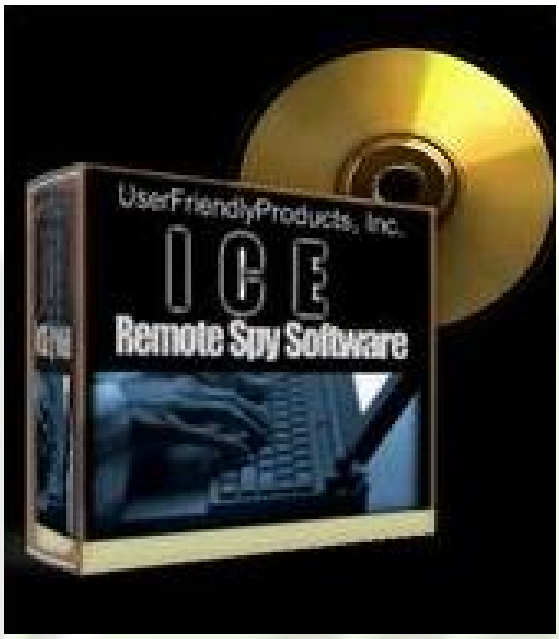
2.4.1

Spyware - Keystroke Logging

(ICE Remote Spy)



Objective

Stealthy spyware will be used to capture a PC operator's keystrokes and other online or local activities to a log file. Captured data can also be sent to another user via email.

Information for Laboratory

A. Students will install, configure, and operate the ICE Remote Spy software.
B. Students will log keystrokes, online and local activities. This may include authentication data (username and plaintext password), email messaging (all content read or written), Web sites / chat rooms visited, and both sides of instant messenger sessions.
C. Students will view the logs produced by the spyware program.
D. Students will see how to send local monitoring information to a remote user via email.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Estimated Completion Time

45 Minutes

Keystroke Logging & Spyware

Spyware is a generic term used to describe any software that is used to gather information about the user without the user's knowledge. It is related and oftentimes used synonymously with the term Adware, which is a contraction for Advertising Software. Adware is sometimes bundled with shareware programs. Adware is also a means by which Internet site owners can make income. Internet surfers are all too familiar with the popup advertisement, but it is often overlooked that the adware usually contains a spyware component as well. This acts to gather information to be sent back out to the Internet.

Adware/spyware usually tracks information relevant to

marketing, such as what internet sites you have visited, but they might track system resources, applications, etc. In short, spyware can be used to track a myriad of statistics and facts about your system and its use. This raises concerns over security and privacy while system resources are redirected.

A Keystroke Logger is a class of spyware that is used for surveillance, tracking details of how a computer is used right down to complete logs of keyboarding. Such programs usually have additional capability, such as monitoring the complete text of email sessions, chat rooms, instant messenger sessions, etc. A Keystroke Logger is the software equivalent to a "bug", or a listening device used by law enforcement or the intelligence community.

System administrators might place surveillance spyware on an employee's computer for the purpose of assessing appropriate use. Likewise, parents might use spyware to monitor their children's use of computers.

Users should also be aware of the possibility that an intruder could use spyware to discover logins, passwords, and other sensitive personal or proprietary information.

For this reason, users and administrators alike should be aware of spyware detecting software, but this is beyond the scope of the present lab exercise.

Using ICE Remote Spy Software 8 (or later)

Using this tool from UserFriendlyProducts, Inc., will familiarize the student with the features found in many commercial/ shareware/freeware keystroke loggers. Capabilities of the tool include the logging of a target user's typed keystrokes (including passwords), all email, all chat rooms, all Web sites (including activity), and all programs accessed. ICE Remote Spy is a commercial product, but a trial version is available. See the Appendix for information regarding installation files.

Step 1:

ICE Remote Spy does not start like a typical program by shortcut, start menu, or desktop icon. After installation it starts when the system boots at which time you should see the following dialog box:

Click on **Try Evaluation.**

Step 2:

You need a password to continue with the trial, and to obtain the password, you need to provide a valid email address. When successful you should see the following:

This dialog box is only for trial. For the commercial version ICE

Remote Spy will be completely hidden from the user.

Step 3:

While ICE Remote Spy is recording your actions, perform actions on your computer for a few minutes. These might include visiting a few Internet sites, writing a short piece of text in Notepad, reading or sending email, executing a few pings in a command window, or opening a few applications.

Click on **Expand Directions**, and as indicated, execute CTRL-ALT-SHIFT-H. After inputting the required **PASSWORD**, the following Hidden Viewer dialog box is displayed:

Step 4:

Explore the results of ICE Remote Spy by clicking on the following features within the Hidden Viewer as shown above:

View Recorded IMs

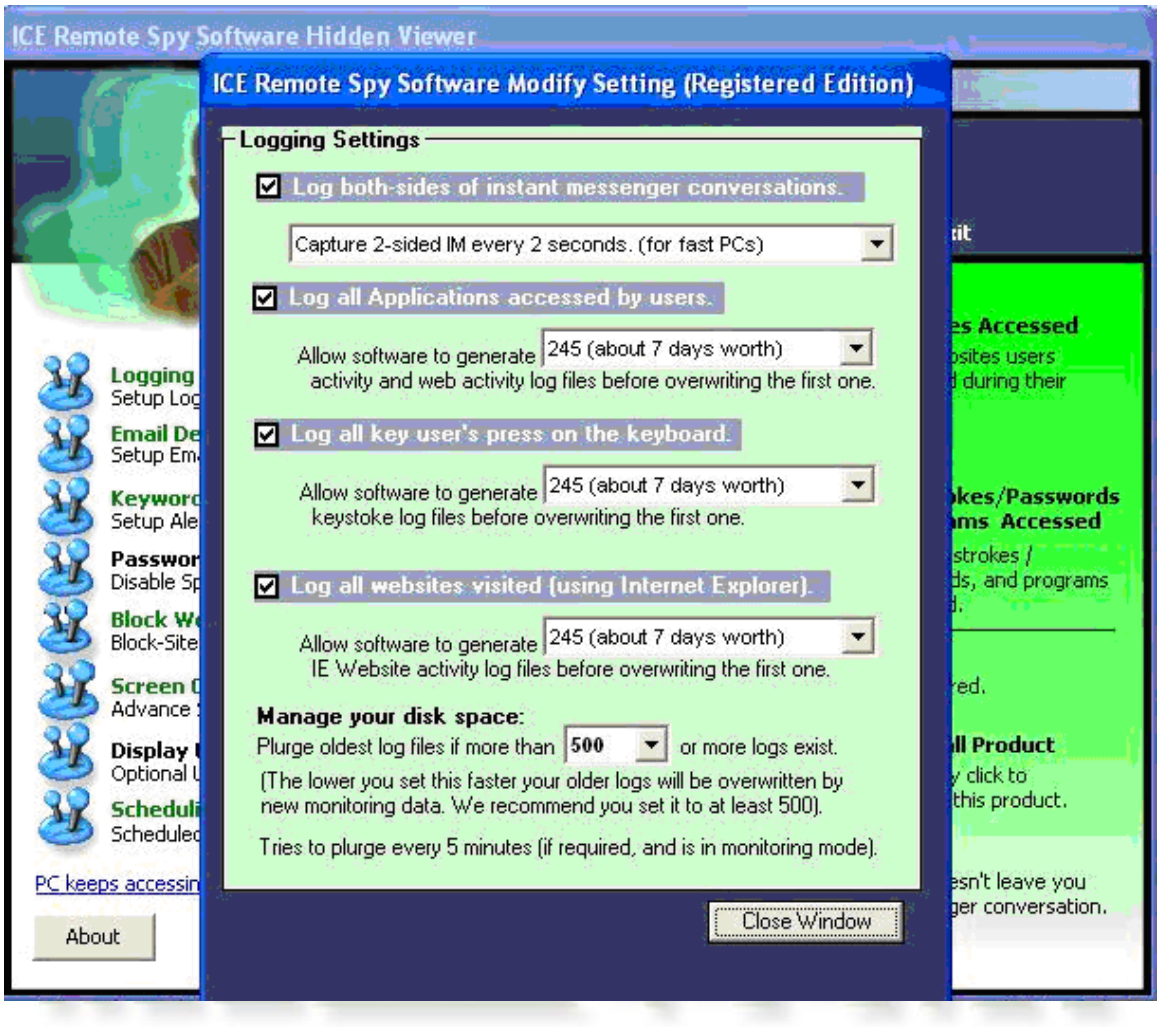
Websites Accessed

View Recorded Pics (This reveals a series of screen shots.)

Keystrokes/Passwords/Programs Accessed

Step 5:

Explore all the options, Logging, Email Delivery, etc., listed on the left side of the Hidden Viewer. The Logging dialog box is shown below:



Note that **Display User Warning** may be a legal requirement for use by administrators.

Step 6:

Look for the following files in the \Windows\System32 directory:

ANSMTP.dll	CapScrn.ocx
Dwshk36.ocx	DWSPY36.DLL

These are the files used by ICE Remote Spy. Adware/ Spyware detection programs would need to include these in their database in order to find and remove them. As of this writing neither Ad-aware nor Spybot, both free detection programs, would detect ICE Remote Spy. Spybuster is a commercial detection product by Bothwell Innovations, LLC. which was able to detect ICE Remote Spy. It may be found at www.nitrousonline.com.

Analysis

1) How useful would ICE Remote Spy be to parents of young children that use the Internet?
2) Compare the use of a Keystroke Logger such as ICE Remote Spy with other security tools such as management of user privileges and firewalls.
3) Is the commercial version of ICE Remote Spy suitable for network administrators?
4) Under what circumstances would a network administrator use a Keystroke Logger?
5) As a cyber security professional, what are the ethical dimensions of your usage of spyware and countermeasures? As a computer user, “same question”.

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

1) Research application software with similar functionality by searching the Internet. What keywords/phrases did you use and how many hits did you get? Which search engine did you use?

2) How do the application software packages compare in terms of features, price, licensing, and other considerations? Identify some other considerations besides features, price, and licensing restrictions. Be sure to include commercial, shareware, and freeware products in your research. Must you research each product individually? Or are there sources that can be trusted to do impartial evaluations of competitive products? Identify three of these sites that specialize in cyber security product reviews. How do you know that the product reviews published by these sites are not influenced by advertising revenue from product manufacturers and developers?

3) Is there hardware on the market to perform the same functions as the application software used in this lab exercise? Under what circumstances would a hardware solution be preferable to a software solution? And vice versa?

4) Explore the following site if you have not already done so:

   www.spychecker.com/spyware.html

Appendix

The lab was performed using, which can be found at,
The Windows operating system used was XP Professional version 2002 (Service Pack 1)

Appendix:

This lab was developed using ICE Remote 8 Spy Software, trial version, which can be obtained from:

-or-

http://www.download.com

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).