2004

Predator and Prey Alert System

Melissa R. Kryder

THE FLORIDA STATE UNIVERSITY

COLLEGE OF ARTS AND SCIENCES

PREDATOR AND PREY ALERT SYSTEM

By

MELISSA R. KRYDER

A Thesis submitted to the
Department of Computer Science
In partial fulfillment of the
Requirements for the degree of
Master of Science

Degree Awarded:
Spring Semester 2004

The members of the Committee approve the thesis of Melissa R. Kryder defended on April 16, 2004.

Mike Burmester
Professor Directing Thesis

Lois Hawkes
Committee Member

Alec Yasinsac
Committee Member

The Office of Graduate Studies has verified and approved the above named committee members.

To my mom, for making me the person that I am today.

ACKNOWLEDGEMENTS

I would first like to thank Dr. Mike Burmester, my major professor, for his continued support and guidance. He allowed me the freedom to think on my own, while also guiding me in the right direction when I would go astray. The amount of knowledge I learned from him is immeasurable, and I could not have possibly accomplished this thesis without him.

Next I would like to thank my committee members Dr. Lois Hawkes and Dr. Alec Yasinsac. Dr. Hawkes was an excellent source of information throughout my thesis project. Dr. Yasinsac devoted so much of his time towards helping me with my National Science Foundation Scholarship and job placement. To you I owe many thanks. I would also like to thank the National Science Foundation Scholarship for Service program for giving me the opportunity to focus my efforts on my studies.

I would like to thank my Dad and stepmom Kathy for their support through my undergraduate and graduate degrees. You were there to help guide me in many decisions that I had to make throughout college. Thank you for your wisdom and knowledge. I would also like to thank my friends for listening to me when I needed an ear, especially Juliette who probably heard the most of it.

Last but not least I would like to thank my Mom. Without her love, care and guidance I would not be where I am today. She always believed in me, even when I didn't, and stood by every decision I made. Words cannot begin to describe how I feel about what she has done for me throughout my entire life. Thank you Mom.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The Internet is an excellent source of information and entertainment. Children reap numerous benefits using the Internet for educational purposes, playing games and communicating with people all over the world. But along with these benefits comes a downside. Children are extremely vulnerable to Predators while on the Internet. These Predators seek to harass, intimidate and abuse children. Children must be protected while on the Internet, and these Predators must be put to a stop. We seek to do this through the use of our proposed Predator and Prey Alert (PAPA) System. This system will monitor and log a child while he or she is logged onto the computer and will also enable police to link to the child's computer while the child is communicating with the Predator so that evidence can be gathered and the Predator can be stopped.

CHAPTER 1

INTRODUCTION

The Internet is an excellent source of information and entertainment. Through the use of the Internet users can learn about different places, play games, and meet people all over the world. There are an estimated 604,111,719 users of the Internet worldwide, and this number continues to grow [7].

Of these 604 million users many of them are children. They too can experience many advantages of the Internet. However there are many dangers lurking on the Internet that children can fall victim to. Websites that deal with pornography, the purchase of drugs online, and instructions for making and building explosives or weapons are all things that are inappropriate and dangerous for children. But websites do not pose the only threat towards children. There are thousands of people on the Internet that Prey on children. They seek to take advantage of and abuse children in any way possible.

1.1 Statistics

According to the U.S. Department of Justice, 250,000-500,000 pedophiles reside in the United States [9]. Some of these pedophiles use the Internet as a place to meet new victims. They go to chat rooms or discussion boards that children frequent in hopes of finding a new target. Many will go to great lengths, spending large amounts of time, money, and effort, in hopes of establishing a relationship with a child.

"According to a Gallup Poll, 1.3 million children were victims of sexual abuse in 1995 alone, and that number continues to rise each year," [9]. There are no exact numbers on how many of these children met their abusers online, but this number surely continues to grow as the widespread use of the Internet continues.

1.2 A Solution

Children must be protected from cyber-predators. We propose a solution that seeks to do just that. Through the use of our Predator and Prey Alert (PAPA) System parents will be able to monitor their child's activities online and look for potential threats. If it is discovered that there has been suspicious activity, an Investigator (police or FBI) can use the PAPA System as a tool for gathering evidence to aid in the capture and conviction of the Predator.

In Chapter 2 we uncover the profile of a Predator. Chapter 3 gives an overview of the proposed PAPA System. Chapter 4 discusses the Monitor Toolkit portion of PAPA, while Chapter 5 covers the Guardian Angel Toolkit of PAPA. Then in Chapter 6 we outline Best Practices for PAPA. Chapter 7 goes over the installation and configuration of the PAPA System. Next in Chapter 8 we give some implementation suggestions. Chapter 9 details problems that could arise through the use of PAPA. Finally, we conclude in Chapter 10.

CHAPTER 2

PROFILE OF A PREDATOR

Identifying pedophiles in cyberspace is not always easy. Often times they portray themselves as children [2]. Pedophiles often seek out opportunities to be around children, so cyber chat rooms geared towards children are often used by pedophiles to meet new victims [18]. Prior to using the Internet, parents should caution children about talking to adults online or going into inappropriate chat rooms. They should tell children to ask the age of the person who they are communicating with. Parents could advise their children that if they are talking to someone that is substantially older than them they should end the conversation. But if a person lies and tells the child that he or she is of a similar age, the child should have no reason to fear that person, when in reality it is quite the contrary. A person that feels the need to lie to the child certainly does not have the best interests of the child at heart.

During the initial conversation predators will usually not do anything that would be considered inappropriate, instead they try to gain the confidence of the child [2]. This enables a bond to develop between the Predator and the child. Once a bond is formed between the Predator and child, the child will see the Predator as a friend and not as someone that could hurt them. The Predator will probably then try to get personal information from the child such as address, last name, school, or try to get the child to send the Predator nonsexual pictures. The child, seeing the Predator not as a threat but as a friend, might give the Predator what he or she is asking for.

Eventually things will escalate between the Predator and the child. The Predator might instruct the child to go to unsuitable websites or begin sending inappropriate pictures to the child [9]. The Predator can then use these images to try to convince the child that taking inappropriate pictures of children is ok, and that he or she should take pictures of themselves and send them to the Predator [27]. The child, wanting to make their friend happy, might oblige by sending

pictures to the Predator. As things progress, the Predator may begin making phone calls and sending gifts to the child. All this in an effort to eventually meet and potentially do harm to the child.

Some Predators take a different approach and try to drive a wedge between the child and the parents [27]. This will result in the child feeling alienated, that he or she cannot go to their parents for help or support. Once this happens there is no limit to the amount of abuse the Predator can inflict on the child.

Whether the child views the Predator as a friend or as a threat, he or she is unlikely to report this abuse to his/her parents. Because of this, parents need to make it a priority to know what their child is doing while on the computer. This is an almost impossible goal to achieve due to the fact that most parents do not have the time to be with the child while he or she uses the computer. Through the use of this proposed PAPA System parents will be able to watch over and protect their child without actually having to be there.

CHAPTER 3

PREDATOR AND PREY ALERT SYSTEM (PAPA) OVERVIEW

To solve the problem of predator stalking we propose a system that will both monitor and log the computer of a potential victim and then can be used in conjunction with police. This will be a piece of software that can be purchased by anyone and installed onto a home computer. The software will have two parts, the first part, the *Monitor Toolkit*, will monitor and log the user's account according to options that will be defined by the superuser (the parent). The second part, the *Guardian Angel Toolkit*, will be used in conjunction with police to help gather information about the Predator. The Prey will be able to talk to the Predator on their home computer while being offered protection by the police.

The purpose of the Monitor Toolkit is to help reduce the chance that children will come in contact with harmful people. It will have the option to allow a parent to view the conversations that their child had in chat rooms or instant messenger services, emails sent and received, etc. Since often the child will not be able to determine on their own that he or she is having harmful interactions with people, the parent will be able to protect their child while online without actually standing over them. After viewing a conversation that the parent deems inappropriate, he or she will have the option to contact the police. The parent will be able to submit the evidence that he or she has seen to be evaluated by an Investigator. The Investigator will determine the appropriate course of action, but will have the option to continue using the proposed software in their investigation.

The Investigator will use the Guardian Angel Toolkit portion of the PAPA system for this process. The Guardian Angel Toolkit will allow the Prey to connect with the Investigator while on their home computer. The Investigator will be able to see the conversation that the Prey is having with the Predator and will be able to advise the Prey on what to say or do through text messaging.

CHAPTER 4

THE MONITOR TOOLKIT

The Monitor Toolkit will have two main modes, the Overview Log Mode and the Detailed Log Mode, with the Detailed Log Mode having two different submodes, Level 1 Detail and Level 2 Detail. The main purpose of having different configuration modes is to help reduce the consumption of computing resources. As is always the case in computing you must balance security with usability [22]. If the software constantly consumed computing resources bringing the machine down to a crawl, few people would use the software. Thus the different modes will be created allowing higher consumption of resources only when absolutely necessary.

All of the logs created by the Overview Log Mode and the Detailed Log Mode will be written to a black box attached to the Prey's computer. These logs will be write-protected, so that they cannot be altered in anyway. It is crucial that the logs cannot be tampered with so they can later be used as evidence. The write-protected logs are still readable, and thus will be able to be viewed by the superuser for suspicious activity.

4.1 Overview Log Mode

The Overview Log Mode will do as the name suggests, give an overview of what the user did while logged onto the computer. It will create a log of the start and stop times of all applications run by the user while logged onto the computer. This log will be written to the black box where it will be write-protected to prevent tampering (see Figure 4.1). Again, this log will just be an overview, listing only the start and stop times and the names of the applications run. It will not list what the user did while using the application. This will be done for the sole purpose of keeping the size of the log file down.

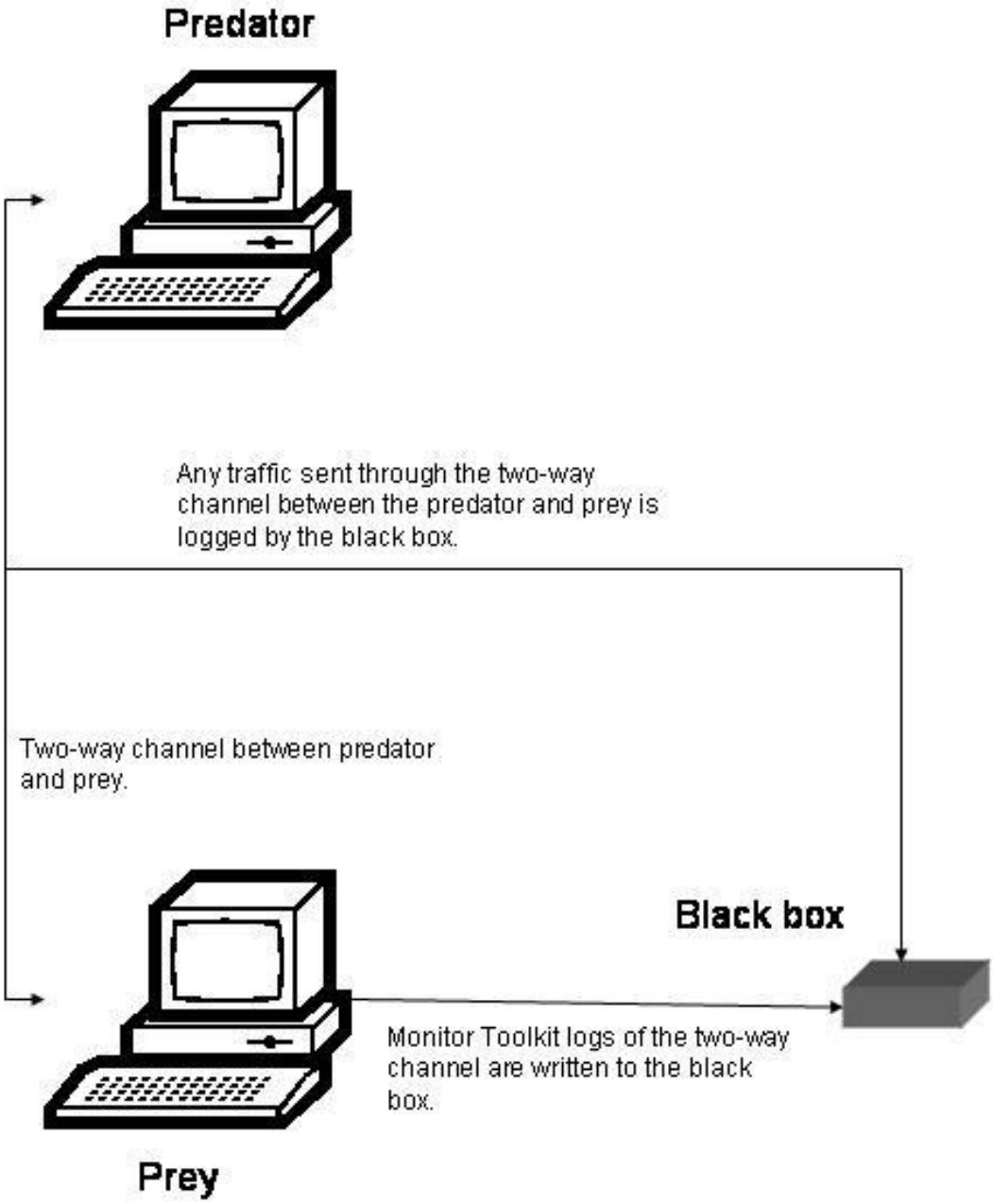

Figure 4.1 PAPA System black box: Illustration of Monitor Toolkit logging. The bidirectional arrows depict data flow in both directions. The unidirectional arrow between the Prey and the black box illustrates that data can only be written into write-protected logs.

Since essentially all this is doing is logging what the user is doing, it will not send any alerts to the superuser of suspicious activity by the user. The superuser will have to examine the Monitor Toolkit logs and view the user's activities while on the computer. It is recommended that the superuser view the Overview Mode logs in proportion to how often the user is logged onto the computer. If the user is only on the computer infrequently, then the superuser only needs to check the logs once every couple of weeks. However if the user is logged on to the computer every day for several hours, then the superuser is strongly urged to view the logs at least every few days. This is due to the inordinate amount of data the superuser might encounter when only viewing the logs occasionally. If the logs are only viewed once a month, there will be so much data for the superuser to sort through that something vital may accidentally be missed.

While viewing the logs, the superuser is looking for suspicious activity. Suspicious activity would include being in a chat room or talking on an instant messenger service for several hours. It will probably not be necessary to take immediate action after seeing that the user has done something suspicious, but rather look to see if this suspicious activity continues. If it is discovered that the suspicious activity continues over several days, then it is advised to change the Monitor Toolkit from the Overview Log Mode to the Detailed Log Mode.

4.2 Detailed Log Mode

The Detailed Log Mode logs more detail about the user then the Overview Log Mode. This mode can be used to monitor and log what the user is actually doing while using an application. As with the Overview Log Mode, the Detailed Log Mode will write its logs to the black box. The Detailed Log Mode should only be used after the superuser notices suspicious activity by the user while in the Overview Log Mode. Detailed Log Mode has two levels of detail that it can log at, Level 1 Detail and Level 2 Detail.

4.2.1 Level 1 Detail

The goal of Level 1 Detail of the Detailed Log Mode is to log more detailed and in depth information about the user while keeping the amount of useless data about the user to a minimum. In the Overview Log Mode, the superuser could only view which applications the

user ran while logged onto the computer. In the Level 1 Detail the superuser can see what the user actually did, such as sending email or chatting with friends, while using certain applications. The superuser does this by configuring the Monitor Toolkit to log more detailed information about the user.

To allow for the Monitor Toolkit to record more detailed logs of the user the superuser only needs to make some simple changes to the configuration of the Monitor Toolkit. The superuser will first log into the superuser account where the Toolkit is located. He or she will then go into the Detailed Log Mode section of the Monitor Toolkit. Once there, the superuser will select the option for Level 1 Detail. Upon doing this a record will be formed listing all of the applications installed on the user's account. The superuser will then traverse the list deciding which applications should be logged by the Monitor Toolkit. Any application that is not selected by the superuser at Level 1 Detail will still be logged by the Monitor toolkit but only at the Overview Mode level. Choosing which applications should be logged by the Monitor toolkit is at the discretion of the superuser. It is strongly recommended that applications including web browsers, such as Internet Explorer or Netscape, messaging software, such as AOL Instant Messenger or Yahoo! Messenger, and email clients, such as Microsoft Outlook be logged with Level 1 Detail by the Monitor toolkit.

With these new configurations, when the superuser views the logs recorded by the Monitor Toolkit he or she will see much more detail about the user's session. The superuser will now see what the user typed and what was sent to the user. For example, if the Monitor Toolkit is configured to record Level 1 Detail for Microsoft Outlook the logs will show all of the email that was received and sent by the user. It should be noted that the Monitor Toolkit will only log data at the Level 1 Detail for logs created after the configurations have been specified. Changing the configurations to Level 1 Detail will not affect the data recorded in previous logs.

Identifying specific applications the Monitor Toolkit should log at Level 1 Detail helps to keep the amount of data gathered, and the amount of space consumed reduced. It will consume more disk space than the Overview Log Mode, but it will consume less disk space then if it logged every application run by the user. If the superuser is unsure of which applications to select for the Level 1 Detail, or is afraid that he or she may not select all of the applications that the Predator might be contacting the user on, the superuser can choose Level 2 Detail.

4.2.2 Level 2 Detail

The Level 2 Detail is similar to Level 1 Detail of the Detailed Log Mode in that it logs more detailed information about the user. But unlike Level 1 Detail that logs only detailed information about specific applications, Level 2 Detail logs detailed information about all applications that the user runs.

Configuring the Monitor Toolkit to log at Level 2 Detail is similar to configuring the Toolkit to log at Level 1 Detail. The superuser will log into the superuser account to access the Toolkit. He or she will then go into the Detailed Log Mode section but this time will select the Level 2 Detail option. With the Level 2 Detail option the superuser will not be presented with a list of applications on the user's account as in with Level 1 Detail. This is because there is no option to pick and choose which applications to log in Level 2 Detail, the Monitor Toolkit will log all applications at the detailed level.

With the Level 2 Detail configurations the logs will show as much data as possible about the user while using every application. It will show all emails sent and received, instant message conversations, websites viewed, games played, etc. Again it should be noted that no logs created before the configurations were changed to Level 2 Detail will be altered.

Due to the level of detail that the Monitor Toolkit will be logging, these logs will have the propensity to grow quite large. If the user is logged onto the computer infrequently, or for only short periods of time, then the logs should still remain at a manageable size. However, if the user is logged onto the computer often, or uses the computer for extended periods of time, then the logs can become quite sizable. If the logs become very large, it may be difficult for the superuser to do adequate reviews of the logs causing valuable information to be missed. Due to this it is advised that Level 1 Detail be used.

CHAPTER 5

THE GUARDIAN ANGEL TOOLKIT

The Guardian Angel Toolkit is the most important portion of this package. Although the Monitor Toolkit portion is vital to the discovery of the criminal activity, the Guardian Angel Toolkit portion is what enables police involvement and the gathering of evidence to help put a stop to the Predator. Up to this point, the superuser has used the Monitor Toolkit to view the activities of the user. When the superuser discovers inappropriate conversations or activities by the user, the superuser should now proceed to the use of the Guardian Angel Toolkit.

5.1 Contacting the Authorities

Once the superuser views that something inappropriate occurred between the Predator and the user, the superuser should report to their local police. The superuser is urged not to wait to see if the inappropriate actions continue, but to notify police immediately, especially if the user gave out personal information to the Predator. The superuser should contact their local police force by emailing a detailed account of what the superuser has seen occur on the computer. It is suggested that the superuser copy and paste a sample of the information logged by the Monitor Toolkit into the email so that the police can have a better understanding of the situation. This email will not be able to be used as evidence, as there is no way of proving that the information was not tampered with, but will serve to educate the police officer on the circumstances [6].

An Investigator will then look into the email that he or she receives to see if the claim warrants an investigation. If the Investigator feels that the email provides sufficient grounds to

launch an investigation the Investigator can take advantage of the Guardian Angel Toolkit portion of the package.

It is recommended that parents should now sit down with their child and discuss the situation with them. They should tell their child that the conversations that the child has been having with the Predator are dangerous. Parents should be sure to tell the children that they are safe now, and that they will be protected by their parents and police.

When the Guardian Angel Toolkit is started the software will no longer be invisible to the user. When the superuser starts the Guardian Angel Toolkit an icon will become present on the user's desktop. Parents should familiarize their child with this portion of the software. Explain to them how it works, and make sure that he or she knows how to use the software in case the child should need to use it while the parents are not around.

5.2 Operating the Guardian Angel Toolkit

When the child is contacted by the Predator the Guardian Angel Toolkit should be launched. This will put the child into contact with the police. Once the connection has been established between the Investigator, child, and Predator the Investigator will be able to see an exact copy of the child's computer screen (See Figure 5.1). Anything that the child can see or do the Investigator can see or do. The Investigator will be able to monitor the conversation and interaction between the Predator and Prey. The Guardian Angel Toolkit will also allow the Investigator to talk directly to the Predator as if he or she was the child. The Investigator will connect with the Predator through the same means that the child is using. For example, if the child is using an instant messenger he or she will have a window open on his or her desktop displaying the conversation with the Predator. In order to talk to the Predator the child types the message into the text box and then sends the message to the Predator. If the Investigator wants to send a message to the Predator the Investigator will do the same as the child, by typing the message into the text box and then sending the message to the Predator. The child will see what the Investigator typed on his or her own screen, just as if he or she typed it themselves. Before the Investigator begins acting on behalf of the child the Investigator should instruct the child not

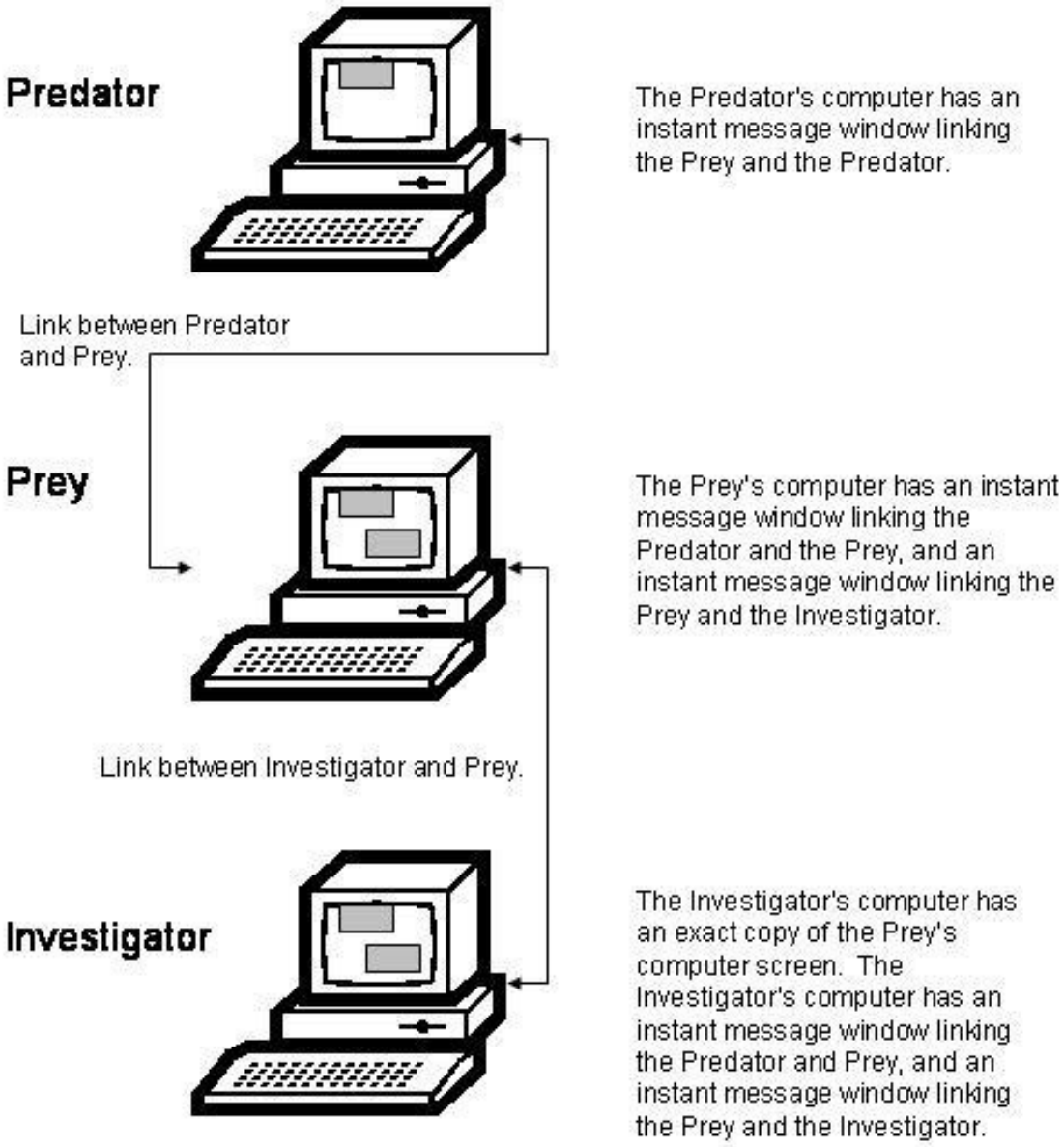

Figure 5.1 Links between Predator, Prey, Investigator, and instant message windows.

to send anything to the Predator unless told otherwise. This is so that the Investigator and the child do not talk to the Predator at the same time causing the Predator to become suspicious and perhaps lose the connection.

Along with the three-way conversation channel between the child and the Predator and Investigator there will be a two-way conversation channel between the child and the Investigator via an instant messenger service. Through this the Investigator can guide the child as to what to say to the Predator. In addition the Investigator will be there to assure and comfort the child in case he or she becomes unsure or scared.

While the Guardian Angel Toolkit is running, the Monitor Toolkit will still be logging all of the data received. When the Guardian Angel Toolkit is activated the Monitor Toolkit will default to running in Level 2 Detail mode to ensure that no evidence is lost. There could be an optional black box attached to the Investigator's machine that could also be used to log data. This could be used as a backup to the child's black box, or it could be later used to compare with the child's black box as evidence that the data was not tampered with. The Investigator's black box should not stop capturing information until the connection is lost between the Investigator and the child. Stopping the logging process too soon could result in the loss of crucial data.

It is important to note that this will all be invisible to the Predator. The Predator will have no idea that their conversation is being monitored. If the Predator became suspicious of police involvement the Predator might restrict what he or she says, resulting in no useful evidence gathered. Or worse yet, the Predator might disappear, cutting off all ties to the Prey, thus making it much more difficult to determine the Predator's identity and location.

CHAPTER 6

BEST PRACTICES

This section is about simple best practices for the protection of children from Predators. This chapter does not look to try to secure a computer system from cyberspace attacks, but to point out some of the crucial steps that must be taken in order for the PAPA system to work properly. The most important step in protecting children from cyber-predators is making sure that the parents are the ones in control of the computer, and not the child. General best practices should be followed by the parents to ensure this.

6.1 Restricting User Accounts

First, parents need to restrict the user accounts that are on the computer. Ideally no one should have administrative rights on the computer. While being run in the administrator mode configuration changes can be made to the computer that can not be reversed. Programs can be installed that contain viruses or worms that could destroy the system. "Running a computer in Administrative mode makes the system vulnerable to Trojan horses and other security risks," [17]. This can all be avoided if the administrator account is only used when absolutely necessary.

Children in particular should not have administrator rights. Limiting their rights to the "limited" status (in the Windows operating system) will restrict them from installing programs on the computer. This will prevent them from installing programs such as games that a parent feels are not appropriate for the child, or programs that may be downloaded from an unreliable or corrupt source. Parents should also make sure that the Guest account is disabled. "The Guest account is disabled by default, and it is recommended that it stay disabled," [17]. As well as being a major security risk, due to the fact that the Guest account has no password and thus is

easily compromised, a usable Guest account could allow the children to do things that the parents would be unaware of. It is difficult enough to monitor what a child is doing on one account, but that difficulty increases exponentially if the child has access to several user accounts.

As mentioned previously, children should not be able to install software on the computer. Without realizing it, they may install unsuitable or corrupted software. Worse they could install something given to them by the Predator that could potentially give the Predator control over the child's machine. This could send information back to the Predator on what the child is doing on the computer. It could also look for certain files on the computer, such as pictures, and send them back to the Predator. This would obviously be very harmful for the Predator to have pictures of the child.

6.2 Password Security

Lastly, password security is a very important issue when talking about computer best practices for two reasons. First, passwords must be secure to prevent intrusion of the computer by hackers. Second, and most important to our context, passwords must be secure enough to prevent the child from being able to hack into the other user accounts.

"Passwords provide the first line of defense against unauthorized access to your computer," [16]. If the passwords to the computer are weak, then the first line of defense for the computer is virtually useless. A weak password is one that can be easily guessed by a person or a password cracking program. Password cracking programs generally use one of two techniques: dictionary attack or brute-force attack. During a dictionary attack words from a dictionary of common passwords or combinations of passwords are entered until the password is cracked [10]. A brute-force attack is where every possible permutation of letters and numbers is entered until the password is determined. Given enough time a brute-force password cracking program can crack any password [11]. When choosing passwords for their accounts, users need to be sure that they are choosing strong passwords. A strong password would consist of a combination of uppercase and lowercase letters, numbers, and special characters such as # $ % [11]. Parents should help their child when choosing their password to make sure that he or she picks a strong password and one that is easy for the child to remember.

Although the child is an authorized user to the computer, he or she is only authorized to use a specified account, and should not be able to access the other accounts on the computer. If the child is able to log into the Administrative account he or she has gained control of the machine. He or she can now install programs without their parent's permission, and possibly even lock their parent out of the computer. Due to this it is imperative that parents choose a strong password for the Administrative account. This password should not be the family pet's name, or someone's birthday or anniversary date. These are all things easily guessed by the child.

CHAPTER 7

INSTALLATION & CONFIGURATION

The following are some suggestions for the installation and the configuration process. This software will be Windows compatible so it must be installed on a Windows operating system. While logged into the administrative account, the PAPA system should be installed onto the superuser account. Installers must make certain that they install the software onto the superuser's account and not the users account. Keep in mind that this software is supposed to be invisible to the user so thus should not be installed onto the user's account.

After installation is complete, the superuser needs to select which account the PAPA system should monitor. Parents might find it easier to have one account for the parents and one account for all of the children. This reduces the amount of work they have to do as far as monitoring their children is concerned. If the need arises, the parents should be able to confront their children in order to determine which child was having contact with the Predator.

Future configuration changes can only be made from the superuser account. There is the possibility that the child will not want to be monitored, and will try to turn off PAPA. By limiting all software access to the superuser, the software is as secure as the password that protects the superuser account.

CHAPTER 8

SUGGESTIONS FOR IMPLEMENTATION

This section looks to make some suggestions towards implementing the PAPA System. There is existing software that could be used to solve parts of the proposed system, but there is not one application that encompasses all of the aspects required for the PAPA System. The following two sections list some existing software products that could either be used as a guide during the creation of PAPA, or products that could be packaged together that in conjunction would form PAPA. It is figured that this PAPA System will be written for a Microsoft Windows platform due to the fact that Microsoft Windows accounts for over 90% of all of the Operating Systems run today [29].

8.1 Implementation Suggestions for the Monitor Toolkit

As discussed in Chapter 5, the Monitor Toolkit monitors and logs the activities of the user while he or she is logged onto the computer. There are several makers of spy software that have products that do just such things. One of the spy software products that I researched and liked for its ease of use was Activity Logger 2.2.

Activity Logger 2.2 is spy software created by SoftActivity. It runs on Microsoft Windows Operating Systems 95, 98, Me, NT, 2000 and XP [23]. The software logs data such as the URLs of websites that the user visited, and keystrokes in instant messengers, email, word processors and others [23]. It can also record screenshots, where it takes pictures of the current screen at periodic increments specified by the user, such as once a minute. The software can be configured to run silently in the background, and not show up in any start menus or add/remove programs lists. This makes it virtually invisible to an unsuspecting user. It allows for password protection of the logs and configuration settings, so only the installer of the software can make

changes to the system. This product retails at approximately $50.00, but a free, unlimited time trial may be downloaded. The free trial has almost all of the same features as the full version except that it limits the amount of data that can be stored into the logs. Once the logs fill up, the software stops logging data.

There are several spy software products that have similar features and have comparable prices to that of Activity Logger, such as Spy Agent by Spy Tech, Ace Spy by Retina-X Studios, and Desktop Spy by Alpine Snow [24, 1, 3]. These products although good, do not have the exact same features as the proposed Monitor Toolkit. For example, with these products you cannot specify which applications you want to have logged at higher detail. These products log all applications with a high amount of detail. Although they do not meet the exact criteria as the proposed Monitor Toolkit, after proper testing and evaluation, one of the suggested spy software products might work as a good substitute.

8.2 Implementation Suggestions for the Guardian Angel Toolkit

The basis of the Guardian Angel Toolkit as discussed in Chapter 6 is that the Investigator is able to link up to the Prey's computer and see exactly the same programs and information that the Prey sees. The Investigator is also able to interact with the Prey, and the Prey's applications. For instance, the Investigator can interact with the Prey via a two-way instant message conversation channel, and the Investigator can interact with the Prey's applications by communicating with the Predator via the two-way instant message conversation channel that has been established between the Predator and the Prey. The following two sections discuss two options that could be used to establish the link between the Investigator and the Prey.

8.2.1 Windows Remote Desktop

Microsoft Windows Remote Desktop allows users to connect remotely via TCP/IP to a system running Windows XP [14]. A Windows machine running the client software connects to a host computer running Windows XP. It works by sending keyboard and mouse input data to the host computer, the host computing that input data and sending display output data back to the client computer (see Figure 8.1). For our PAPA System, the Prey's computer would be

configured to allow users to remotely connect to it. With this configuration in place, the Investigator could then connect to the Prey's computer and have remote access to all of the data and applications.

Windows Remote Desktop has some drawbacks that prevent it from being the ideal means of connecting the Investigator's computer with the Prey's computer. First, the computer that is being operated remotely (i.e. the Prey's computer) must be running Windows XP Professional [15]. Not all home computers run Windows XP Professional, and upgrading the home system would be an expensive process. Second, the client computer (i.e. the Investigator's computer) must be running a version of Microsoft Windows 95 or higher [15]. Microsoft Windows XP comes with the Remote Desktop client software installed, but versions 95, 98, Me, NT, and 2000 do not have it installed [15]. These versions of Windows can either obtain a copy of the Remote Desktop client software from a Windows XP installation CD or can download it from the Microsoft website.

The last drawback of Windows Remote Desktop concerns the locking of the remotely operated computer. Once the connection is established between the client and the remote computer, the remote computer locks, prohibiting anyone from using the system. Therefore, the Investigator would be able to access the Prey's computer, but the Prey would be locked out of their system. The Prey would no longer be able to interact with the Predator, leaving the interaction and communication with the Predator solely to the Investigator.

Using Windows Remote Desktop to connect the Investigator to the Prey would only be an option if the continued interaction between the Prey and the Predator were not needed or desired. The Investigator could interact with the Predator on the Prey's behalf. However, since the Investigator will most times want to collect evidence of the Predator interacting directly with the Prey, the PAPA System will need a better way of connecting the Investigator to the Prey. The next section discusses a solution that does not suffer the same drawbacks as Windows Remote Desktop.

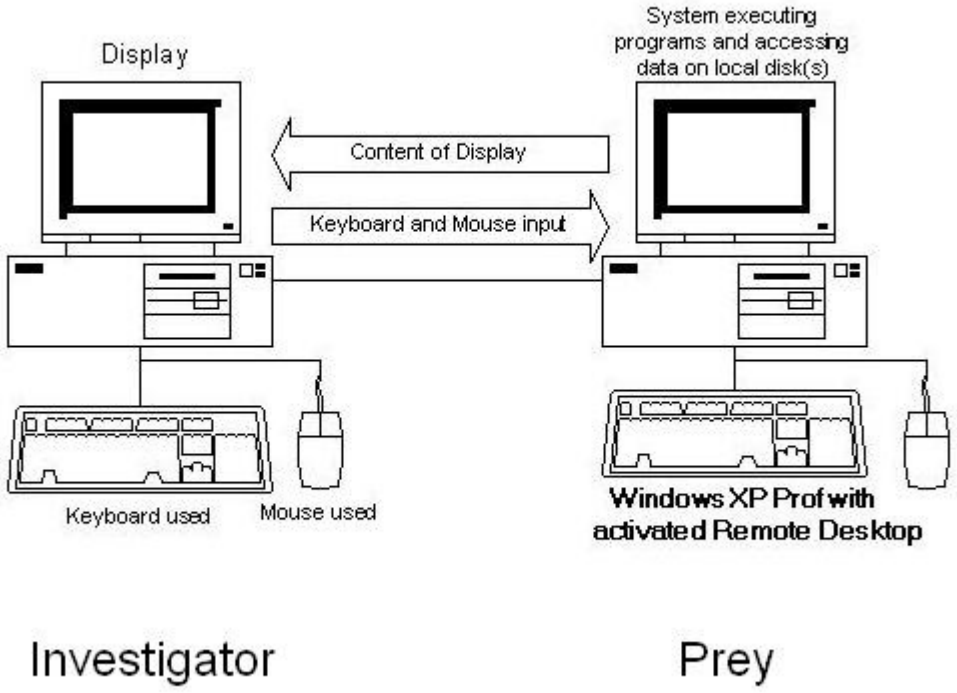

Figure 8.1 Transfer of data using Windows Remote Desktop: The Investigator's computer sends keyboard and mouse input data to the Prey's computer which is executed on the Prey's computer. Data that would normally be displayed on the Prey's monitor is instead sent to the Investigator's machine.

8.2.2 Virtual Network Computing

Virtual Network Computing (VNC), created by AT&T Laboratories Cambridge, enables the interaction with and viewing of a computer from any other computer or mobile device on the Internet [19]. VNC is open-source software based on a protocol called remote framebuffer (RFB) that allows for remote access to graphical user interfaces [20]. Due to the fact that the protocol runs at the framebuffer level, VNC is platform independent (see Figure 8.2) [24]. Similar to Windows Remote Desktop, there is a computer running the VNC Client and a computer running the VNC Server. For the PAPA System the Prey would be running the VNC Server and the Investigator would be running the VNC Client.

Both the Investigator and the Prey would need to have the VNC software installed onto their computers. To allow for the Investigator to connect to the Prey, the Prey would start the VNC server on their machine. A password is required to connect to the VNC server and must be exchanged with the Investigator prior to connection over a secure channel. Once the VNC server is running on the Prey's computer, the Investigator will try to establish a connection to the server using the VNC client. To connect, the Investigator only needs to input the IP address of the Prey's computer and the password to the server, which the Investigator has already received. Once connected, the Investigator can view the exact display that the Prey sees. The Investigator can interact with the applications on the Prey's computer while connected to the VNC server. Whatever the Prey does on their computer the Investigator will see on their screen, and whatever the Investigator does to the Prey's computer the Prey will see on their screen. For example, if while connected to the VNC server the Investigator opened up Microsoft Word on the Prey's computer the Prey would see all of the steps taken by the Investigator (i.e. clicking Start, going to the Programs list and selecting Microsoft Word) to open up the program along with the program execution.

The only downside that I have found during my use of VNC is that it loses responsiveness if the Internet connection speeds are slow. If either the Prey's or Investigator's computer where connecting to the Internet via a dialup modem the VNC software would be very sluggish. It is noted that although slower connection speeds may lower responsiveness of the software, there is no loss of features.

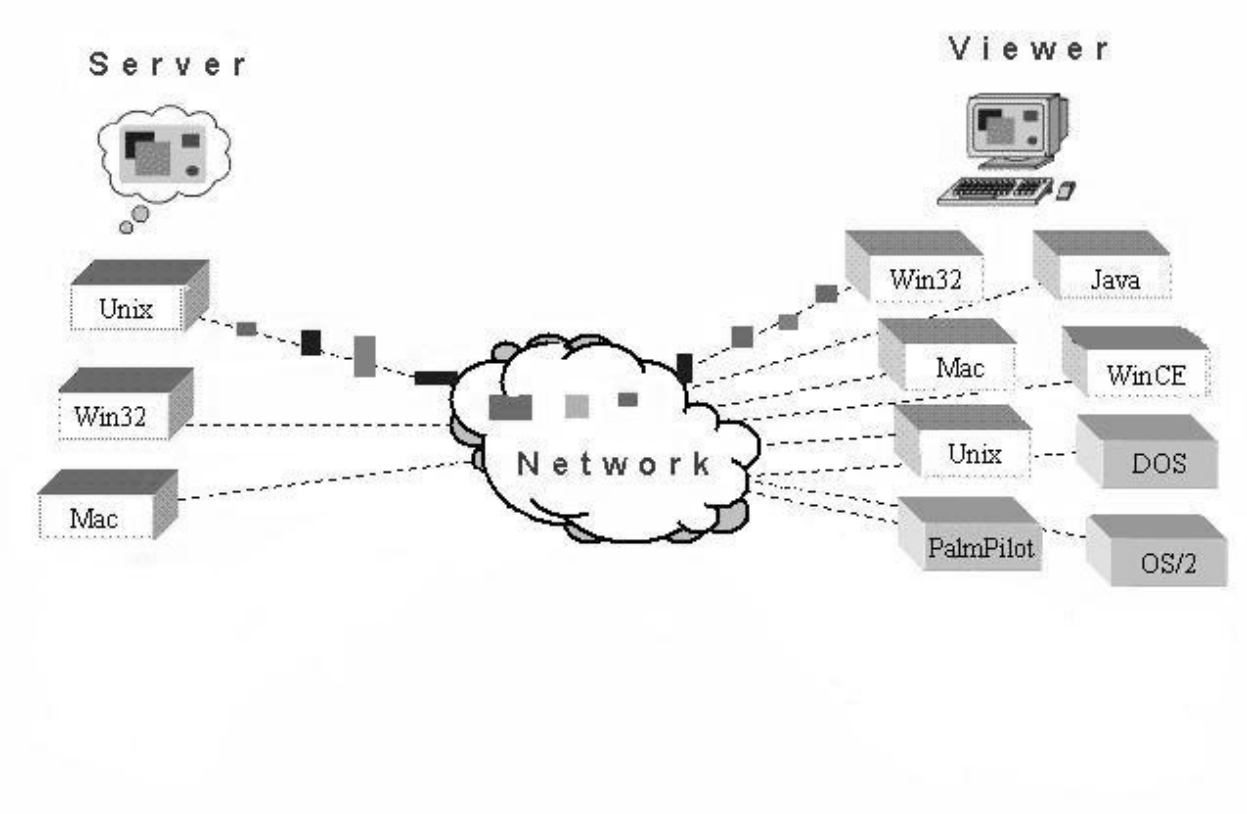

Figure 8.2 VNC server interacting with a VNC client: An illustration showing how VNC software can be used across platforms to view and interact with a computer running a VNC Server using the VNC Viewer on another machine.

CHAPTER 9

SECURITY ISSUES: PROBLEMS THAT CAN ARISE

Ideally, the PAPA System will be installed onto home computers by caring and concerned parents to help protect their children from the dangerous users of the Internet. They will use the Monitor Toolkit solely for the purpose of logging their child's activity so the parents can later view the logs for suspicious activity. The Guardian Angel Toolkit will then be used to link the child to police while the child is communicating with the Predator. The Guardian Angel Toolkit will only be used to collect evidence accurately and legally, to be used in the capture and prosecution of the Predator. Unfortunately we do not live in a perfect world, and while this scenario might happen 95% of the time, we need to be aware of the problems that could arise during that other 5%. While every possible issue cannot possibly be foreseen, there are two main concerns that must be kept in mind while using this PAPA System. These two concerns include framing people through the use of the software, and improper collection of data.

9.1 Using the PAPA System to Frame an Individual

Even when software products are designed with only the best intentions, people still find a way to use them for malicious means. When investigating the evidence, police need to make sure that the evidence that is presented to them by the parent is accurate. Although the logs on the black box are write-protected, and thus protected from altering, police should not assume that the logs were created by honest users.

It is possible that someone could have tricked the alleged Predator into saying things that he or she did not really mean. The alleged Predator might be someone that the parent is trying to take revenge on, like their boss, family member, or neighbor. The parent might log into the child's account and acting as a child, seek out the alleged Predator. The parent could then try to

get the alleged Predator to say incriminating things. Afterwards, the parent would contact the police and present them with the incriminating logs created by the PAPA System.

There is also a possibility that instead of the parent trying to trick someone it could be the child. Perhaps the child is trying to get back at a teacher or classmate that he or she is angry with and tells their parent about what the alleged Predator is doing. In this situation, the parent would actually believe that the Predator is doing something bad, and would report the incident to police. In reality the child has lied to the parent.

In both of these situations police resources would be wasted for a useless investigation. Worse yet, the alleged Predator could be found guilty and sent to jail for a crime that he or she didn't commit. To prevent this from happening, police need to be sure that they validate the claim of wrongdoing early in their investigation.

9.2 Improper Collection of Data

If the black box is functioning properly, the logs created by the PAPA System should be able to be used in court as evidence. However, in between the creation of the logs and using them in court as evidence is an open window of opportunity for tampering and mishandling of the logs. Investigators need to be sure that proper procedure is followed and documented so that the evidence can used. If it can be proven that the logs were altered, or there was a possibility that they could have been altered, the evidence will be thrown out. If the only contact between the Predator and the Prey was through the Internet, the loss of these logs as evidence would most likely result in a dismissal of the court case. The Predator would go free and continue Preying on other children.

CHAPTER 10

FUTURE WORK

Future work for PAPA will reside in the legality of the black box. Without the black box the logs would not be properly stored. If the logs were written to the user's computer, and not the black box, then it would be easy for someone to tamper with them. Someone could change the date or time that a conversation occurred, or alter the text of the conversation.

The evidentiary value of the black box must be explored. Researchers should work together with police and lawyers to make sure that the black box gathers information in a legal fashion. Researchers should also make sure that a procedure is developed with police to ensure that the evidence logged by the black box is collected properly. If the procedure for gathering evidence from the black box is not done accurately it could result in the inadmissibility of the evidence.

CHAPTER 11

CONCLUSION

We proposed a Predator and Prey Alert (PAPA) System that seeks to protect children from dangerous users of the Internet. PAPA consists of two parts: the Monitor Toolkit and the Guardian Angel Toolkit. The Monitor Toolkit logs data created while the child is logged into the computer. The Guardian Angel Toolkit links the child to police while the child is communicating with the Predator for the purpose of evidence gathering.

This system would be fairly easy to implement, if the suggestions stated in chapter 8 are taken into consideration. Easy implementation will result in this system being available sooner, and thus able to protect children sooner. Although it may be possible that this system could be abused by users, the use of black box technologies should make this more difficult. But the small possibility of abuse is far outweighed by the hundreds, perhaps thousands of children that could be safeguarded by this system.

BIBLIOGRAPHY

[1] Ace Spy. *AceSpy Software Full Description*. Retina-X Studios. http://www.acespy.com/index.html

[2] Action Against Infantile Pornography. *Pedophiles and Pederasts: How they act and what they like*. A.C.P.I. http://www.asociacion-acpi.org/pedofilg.htm

[3] Alpine Snow. *Desktop Spy 4.0*. Alpine Snow. http://www.alpinesnow.com/dspy.shtml

[4] Bates, John, Richard Pugh, and Neil Thompson. *Protecting Children: Challenges and Change*. England: Arena, 1997.

[5] Calhoon, John. *Mobile Computing with Windows XP*. Microsoft Corporation. 8 Aug. 2001. http://www.microsoft.com/technet/prodtechnol/winxppro/evaluate/mblxp.mspx

[6] Caloyannides, Michael A. Computer Forensics and Privacy. Massachusetts: Artech House, INC., 2001.

[7] Central Intelligence Agency. *The World Factbook 2003*. Washington, DC: Central Intelligence Agency, 2003.

[8] CERT Coordination Center. *UNIX Configuration Guidelines*. 04 Jun. 2003. Carnegie Mellon University. http://www.cert.org/tech_tips/unix_configuration_guidelines.html#A

[9] Child Lures Prevention. *Reports & Statistics*. 2004. Child Lures Prevention. http://www.childlures.com/research/statistics.asp

[10] Cisco. Cisco Response to Dictionary Attacks on Cisco LEAP. 11 Nov. 2003. Cisco. http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/2331_pp.htm

[11] Cliff, A. *Password Crackers – Ensuring the Security of Your Password*. 19 Feb. 2001. http://www.securityfocus.com/infocus/1192

[12] Donovan, Jim. *Child Protection, Exploitation, and Obscenity*. United States Attorneys' Bulletin. Mar. 2004 Vol. 52 Num 2. 1-40.

[13] Fahey, Drew. *Electronic Discovery & Computer Forensics.* Global Information Assurance Certification. 22 Jan. 2004. http://www.giac.org/practical/GSEC/Drew_Fahey_GSEC.pdf

[14] Helmig, Johannes. *How to use remote Desktop Access in Windows XP.* Articles & Tutorials. Windows Networking. 18 Dec. 2001. http://www.wown.com/j_helmig/wxprmdtp.htm

[15] Microsoft. *Get Started Using Remote Desktop*. 24, Aug 2001. Microsoft Corporation. http://www.microsoft.com/windowsxp/remotedesktop/

[16] Microsoft. *Strong Passwords*. 2004. Microsoft Corporation. http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/windows_password_tips.asp

[17] Microsoft. *Why You Should Not Run Your Computer As an Administrator*. 2004. Microsoft Corporation. http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/windows_security_whynot_admin.asp

[18] O'Connor, Tom. *Child Molesters and Crimes Against Children*. 21 Dec. 2003. http://faculty.ncwc.edu/toconnor/428/428lect19.htm#PEDOPHILES

[19] RealVNC Ltd. *RealVNC*. RealVNC Ltd. http://www.realvnc.com/what.html

[20] Richardson, Tristan. *The RFB Protocol*. RealVNC Ltd. Version 3.7. 12 Aug. 2003. http://www.realvnc.com/docs/rfbproto.pdf

[21] Richardson, Tristan, et al. *Virtual Network Computing.* IEEE Internet Computing Vol 2, Num 1. Jan/Feb 1998. 33-38.

[22] Robinson, Philip. *Workshop on Security in Ubiquitous Computing*. UBICOMP2002. Goeteborg, Sweden, 29 Sept. 2002. http://www.teco.edu/~philip/ubicomp2002ws/organize/outcome.pdf

[23] SoftActivity. *Activity Logger – Spy Software for Parental Control*. 2004. Deep Software. http://www.softactivity.com/spy-software.asp

[24] SpyPatrol. *Spy Agent Software – Powerful Local Computer Monitoring*. 2003. CyberWire, LLC. http://www.spy-patrol.com/spy-agent.html

[25] SysAdmin, Audit, Network, Security Institute. *The Twenty Most Critical Internet Security Vulnerabilities(Updated) – The Experts Consensus*. 08 Oct. 2003. Version 4.0. The SANS Institute. http://www.sans.org/top20/top20.pdf

[26] U.S. Department of Justice Federal Bureau of Investigation. *Innocent Images National Initiative: Online Child Pornography/Child Sexual Exploitation Investigations*. 24 Sept. 2003. Washington, D.C.: Federal Bureau of Investigation.http://www.fbi.gov/publications/innocent.htm

[27] U.S. Department of Justice Federal Bureau of Investigation. *A Parent's Guide to Internet Safety*. Washington, D.C.: Federal Bureau of Investigation. http://www.fbi.gov/publications/pguide/pguidee.htm

[28] United States Secret Service. *Best Practices For Seizing Electronic Evidence*. 2002. United States Secret Service. http://www.secretservice.gov/electronic_evidence.shtml#intro

[29] W3Schools. *Browser Statistics*. Refsnes Data. http://www.w3schools.com/browsers/browsers_stats.asp

BIOGRAPHICAL SKETCH

Melissa R. Kryder was born in Mt. Holly, New Jersey on May 26, 1980. She spent her most of her childhood dancing, singing, and performing in musicals. After graduating from Cherokee High School in 1998, she attended Florida State University. She attained her Bachelors of Science degree in Computer Science in 2002. While receiving her undergraduate degree, Melissa was a member of Upsilon Pi Epsilon - Honor Society in the Computing Sciences, Phi Eta Sigma - National Honor Society, and National Society of Collegiate Scholars. Melissa continued to graduate school at Florida State University where she began working on a Masters degree in Information Security within the Computer Science department. She later received the National Science Foundation Scholarship in Fall 2003. In her spare time, Melissa enjoys going to FSU sporting events, spending time with friends, and dancing.