Global Information Assurance Certification Paper

How do we stop our children from becoming Black Hats?
Richard C Leitz Jr
1 September 2002

1. Introduction

Computers, typical of today's society, enable individuals of any age to retrieve and manipulate information as never before. Children now, possess the ability to learn and operate computers in numerous ways. The learning process begins, in many cases, as early as age two. The computer now ranks as a high priority item in most family budgets; parents recognize the necessity of this tool as a key to their child's academic success. It enables the child to compete on an equal plane with others in their schools, communities and even other countries.

Parents and children are confronted with problems unheard of in the past: peer pressure, drugs and gangs to mention a few. But, now society witnesses a new problem, one so criminal it may involve the Federal Bureau of Investigation, the world of computer crime.

This paper will cover the relevance of computer "hacking" as it compares to the danger of drugs and the dynamics of why and how some children become "hooked" on the practice of "hacking." Defined will be a "Black Hat vs. a "White Hat," different types of "hacking," today's laws and instructions on how to monitor your child and if required, intercede before it is too late. The goal of this paper is to educate today's parents and guardians in the area of computer crime and thus, possible prevent their child from becoming the next "Black Hat" of the 21st century.

New Hi-tech Drug Etc.

Computer crime for the young of the 21st Century is for them an experiment as was the use of drugs by many of their parents in the 1970's. For many "hackers" "The Rush" they achieve is the thought they can not be apprehended and they possess more power than adults: (parents, guardians, teachers, law enforcement, etc...) This new Hi-Tech drug is one that can land a child in jail or ruin any future they may have if it leads to a criminal conviction. It is our responsibility as parents or guardians to diligently watch over and question our children on what they do on the family computer.

What is a "Black Hat" vs. 'White Hat?"

The clearest way to define a "hacker" is to hear their explanation of the term. From the St. Petersburg Times article on hacking is the following quote:

"Many hackers are benign -- just intensely curious how software or computer networks work. Some hackers seem threatening but are little

more than pranksters spreading online graffiti on Web sites. But a growing number are hacking for personal profit, political cause or simply to inflict damage. Many hackers, trying to distance themselves, call these online abusers "crackers." [1]

Apparently the St. Petersburg Times believes that most "hackers" are in it for the fun and they do not like the stigma of being considered criminals.

To quote Max Butler, a "White Hat:"
"*He said, white hats used their computer skills to understand and secure systems, but black hats used their abilities to break into systems for profit or glory."*[2]

Most interesting is that Max Butler is currently imprisoned for crossing the boundary from "White Hat" to "Black Hat." This student agrees with Mr. Butler and many others in the computer security field that a "White Hat" uses his skills to impede the operations of a "Black Hat." We can equate this to the services provided to the public by our local, state and federal law enforcement official on a daily basis. One is considered a "Black Hat" if he or she is an individual of any age willing to commit criminal offenses by performing any of the various "hacks" listed below.

Having been in the computer field for more than two decades and after doing the research for this paper I find that many children who become black hats do so because they have no parent or guardian watching over them and giving them the moral and ethical background that is necessary for them to survive in today's world. Many black hats believe that it is their unalienable right to do as they please with no care for the penalties that they may receive or even worse the damages they are creating for other individuals and companies. For many parents and guardians it is another burden to try and keep up with the computer age as well as know how to properly supervise their children on computers. When a parent is told by the students teacher that they are very adept at computers or the parent sees that when ever there is a problem with the home computer that "Johnny" can fix the problem, they are delighted with their child's profound abilities. I can only hope that as the world becomes more computer competent parents will take the time to improve their own computer skills. My next topic area is on the types of Hacking that a child can perform.

Types of Hacking.

Bellow you will find the major areas of hacking that the typical "Black Hat" will attempt to perform.

a. Defacing of web sites: an example is the SANS Institutes web site which was defaced by "Fluffy Bun" on 13 July 2001. This can be seen at http://www.safemode.org/mirror/2001/07/13/www.sans.org/.

A compilation of defaced web sites can be viewed at http://www.attrition.org or http://www.alldas.org

This type of hacking is becoming the most prevalent upon the current class of young hackers. The writing of html code is easily learned like many other computer languages, as it is being readily taught in most school systems.

b. Writing or deploying malicious software against any other computer based system. Up to date information on the latest viruses may be found at http://securityresponse.symantec.com/ or http://www.mcafeeb2b.com/naicommon/avert/avert-research-center/default.asp

Coding of viruses has been getting worse year after year as more students are learning to program in languages like C, C++, Java, Visual Basic and HTML. Not only are the newest virus writers using these languages; they are also taking advantage of a lack of security in Microsoft Word and Microsoft Excels macros usage. It takes a student only one or two semesters of high school programming in any of these computer languages to be able to write a virus that can cause millions of dollars of damage. Many times the student is not proficient enough in the language to properly write the code. This causes more damage than was originally conceived. A perfect example of this is found in Robert Morris who created the first Internet virus while a student at Cornell University. In only 99 lines of code Morris had brought the Internet and many major computer systems to a complete stop because the program he wrote was replicating and infecting machines at a much faster pace than he had expected. The intriguing part of this is the fact that Morris was a graduate student in computer science and his father was a security expert with the National Security Agency.

c. There are four major types of malicious software –

"Viruses, worms, Trojan horses, and malicious applets. They are defined as follows:

1. *A virus is a piece of parasitic code (or program) written specifically to execute on behalf of the user without the users permission or knowledge.*
2. *A worm is a self contained program or set of programs, that is able to spread functional copies of itself to other computer systems.*
3. *Trojan horses are programs with an intended action that is not documented or revealed.*
4. *Malicious applets are code that attack the local system of a web surfer and involve denial of service, invasion or privacy, and annoyance."*[3]

d. Breaking and entering into computer and non-computer based systems, offices, environments or anything similar for the sole purpose of stealing, blackmailing, destroying or manipulating data.
i.e.: espionage, theft of personal information or credit card information, theft of information in order to blackmail the individual or organization.

e. Sabotage of a computer to cause financial loss.

f. Social engineering: the act of deceiving an individual or organization to gain pertinent information about the organization.

g. Scanning of wireless networks to gain either free internet access or access to private information on the exposed computers or network.

Wireless scanning, or war driving as most in the security field call it, is the latest type of hacking that hackers are using, to break into company and home networks and systems. This is accomplished by using any of the following tools.

A hacker can use a laptop, wireless network card and an external antenna with special scanning software. Some also add a GPS system to the setup to perform mapping of the scanned networks. There are also standalone devices that can be used to look for vulnerabilities in the wireless network. The last tool to scan with is a Pocket PC handheld with scanning software.

Most hackers are using software such as Network Stumbler or Mini Stumbler which are available for free from http://www.netstumbler.com/. Airsnort is another free package which is available at http://airsnort.shmoo.com/. Air Magnet sells a professional package that enables you to use your PocketPC for securing your network against any vulnerability. What these software packages do is look for a special id number called a SSID, being broadcasted out over the airways. The hacker can then use the SSID to program their computer to either just gain free Internet access or worse hack the network. For further in-depth articles please go to any of the following links.

http://www.computerworld.com/securitytopics/security/story/0,10801,72601,00.html
http://www.pocketpcmag.com/Nov02/e_warwalking.asp

These various types of hacking will usually fall into one of these areas: theft of services, stealing information, hatred or revenue gain, personal promotion, warfare, or knowledge. The next topic I shall cover is what is prompting this behavior in the children.

What prompts the behavior?

Now that we have explored the various types of criminal activity in which a child can engage, we question – what prompts this behavior. An explanation may be found in quotes by a few "Black Hats" and one supposed "White Hat" group.

"The Social Base of the Hacker
The Genocide2600 Manifesto

People generally believe that hackers have malicious intent as a general rule. This, pardon my language, is a crock of shit and obviously the ideal ramblings of the most generally uninformed people on the net. I do admit that "YES" there are those that are out to only destroy, and yes this group does occasionally add to that at a very small percentage (this will be explained later). But for the most part, we are in the pursuit of knowledge. I do not claim to be a 100% law abiding person, nor does the group. Obviously, if you have heard of us, or even after reading this, you will be shaking your head at this point.

People for all time have feared what they do not understand, what they do not know. You don't know us; you don't understand us. Some have labeled us as terrorists, others as criminals. Ok. Sure. Whatever. Go ahead take the criminals and terrorists away that fight for your rights. After you have lost the battle because your soldiers are gone at your own hand, you'll have no one to blame but yourself. We fight with the greatest tools of all, our intellect and courage.

*As a whole we believe in a collective good. We believe that people who try to shut out other people or people who try to censor our actions, language and activities are the people who deserve none of the above. We cling to our most basic civil rights. We also believe in retribution for what is lost. Eye for an eye mentality is spoken here. Take back what is yours. Bottom line is this: Don't [f***] with us. We do [f***] back.*

Perhaps the writer is more ignorant than this statement would imply, but most criminals feel that the world owes them something and they are going to take what they feel is rightly theirs, regardless of the rights of anyone else. Even the quote of an eye for an eye is taken out of context and ignores the statement of forgiveness first which follows.

The second hacker reasoning is the following.

Pr0metheus wants nothing more than to spread the word of Satanism. He views his Web site defacing activities as a sort of "hactivism"–activism through hacking. It's not about raising peoples awareness of Internet security issues, and it's not about the love of technology or the thrill of the hack that devotees of the true hacker ethos seek. It never was and never will be. He does not feel evil. Pr0metheus simply hates organized religion, especially those denominations that fall under the umbrella of Christianity. Hacking is just one way to strike back."[4]

People, who are so self centered that they believe "theirs is the only way" and can not accept that others who do not believe as they do are "doomed" and are much more dangerous to society as a whole. Terrorism is terrorism. They hack out of malicious desire to hurt.

Quote of arrested black hat Benjamin Troy Breuninger, "Konceptor" describing why he did hacking, "they were just having fun, learning, and, bottom line, not hurting anyone." [5]

"The founders of GhettoHackers, as the group is called, say its 30-odd members teach others how to crack security only to find flaws so that defenses can be hardened." [6]

A pro choice article to be a white hat would be "How to become a Hacker" by Eric Raymond at http://www.tuxedo.org/~esr/faqs/hacker-howto.html.

Although, these are simply a few opinions on what motivates a "hacker," it appears most are drawn into this activity due to any one of the previous types of "hacking."

How Do the young become Addicted to "Hacking?"

Personally, 23 years ago, this student was presented with the opportunity to play on a Tandy TRS-80 Model 1. This initiated my coding phase and interest in computers. This interest moved me to the purchase of an Apple IIe and a 300 bps modem, which subsequently led to dialing into bulletin boards, languishing on the thrills of the extensive information at my fingertips. Thus, one can only imagine what this present generation experiences, given the fact, they are provided with high speed networks in their growing years. Many have access via DSL or cable modems. This permits them to communicate with those having similar interests. It also provides the opportunity to acquire free information on various types of "hacking" that can be quickly absorbed.

Some of the popular web sites attracting this next generation are:

Chaos Computer Club	http://www.ccc.de
Genocide2600	http://www.genocide2600.com/
2600: The Hacker Quarterly	http://www.2600.com/
Hackers.com	http://www./hackers.com/
The Hacker's Defense Foundation	http://www.hackerz.org
Phrack Magazine	http://www.phrack.org

These represent just a few sites available for "newbie-hacker-wannabees" or as some call them the "script kiddies".

Noted hacker **Ankit Fadia was interviewed and asked,**

"What keeps you hooked to hacking?
Initially, it was the forbidden… because nobody knew much about it. But ever since I have begun hacking, the power to control the Internet on different operating systems has fascinated me. The power to make a computer work the way you want it to is an incredible high."[7]

A recent article on wired.com titled; "Defcon Keeps Hackers Hooked" is about why every year more hackers are attending Defcon to compete against others as well as learn the newest and latest and greatest. The article may be found at http://www.wired.com/news/print/0,1294,45248,00.html [8]

An article on Tech TV details how too much time online can become an addiction or compulsion. For 17 year old Jessica Nichols, her online time became an unmanageable situation. Jessica was loosing sleep and becoming suicidal because people did not respond to her instant messaging quickly enough. This type of addiction can lead to many psychological problems. "*Although a computer doesn't look anything like a drug, be warned that a high tech addiction can be destructive. People can name alcoholism or drug addiction, but the computer tends to wear a halo. People think of them in benevolent, benign terms."*[9]

For many of these children hacking, is a way to show their superiority in an area where others can not compete. Many hackers are not the school jock or the class brain and this results in their being picked on, or beat up, because they are not part of the "right group." This treatment by other students can be enough for the tortured student to decide to use these computer hacking skills to enact revenge against those who have given them trouble. Once the damage has been done, if no one is there to stop the hacking from continuing, the capability for further and more harmful hacking is only eminent.

The Law and Its Punishment of Hackers

Over the last 10 years the United States and many other countries have called for a halt to the harm being inflicted by "hackers." The FBI's first major case was the arrest of Kevin Mitnick, in 1995. He was charged with wire tapping, which enabled him to steal computer codes. This is turn gave Mitnick access to information on computer systems owned by Sun, Motorola and Nokia. These companies charged that they had lost close to 300 million dollars, due to hacking. The government sentenced Mitnick to five years in prison.

Following will be a summary of laws written to be used against computer crimes.

"Computer Security Enhancement Act of 2002 – A computer crime bill enabling the police to conduct telephone and/or Internet spying with out a search warrant. The bill also enables hackers who have committed malicious crimes to be sentenced to life in prison.

It is my belief that this law will not accomplish its goal, because most of the hackers that will commit crimes of the magnitude that would be affected by the law are not living and performing the crime within the jurisdiction of the United States.

Computer Fraud and Abuse Act – Written to prosecute any one that uses code to commit damage or economic harm. Mostly this was meant to cover virus writers, but it has been amended many times to stay up with the current times.

The Electronic Communications Privacy Act – This is an amendment to the Federal Wire Tap Act that protects against interception of data, voice or email from any source.

Economic Espionage Act created in 1996 – An act to stop against espionage foreign and domestic as well as theft of trade secrets.

Wire Fraud Act – Created to stop interstate usage of communication wire (Internet) to commit fraud.

National Stolen Property Act (NSPA) – Computerized transfer of funds valued at more than $5,000.

Identity Theft and Assumption Deterrence Act – Meant to stop anyone who steals another individual's identity for their own personal gain or causes harm to the individual who identity was stolen." [10]

Aside from these Federal Laws many individual states have in acted their own laws to combat computer crime.

A more thorough review of each of these laws can be found at http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html

In the State of New Jersey I will provide a brief review of what the current penalties are for various levels of computer crime. These are found under Title 2C of the New Jersey Code of Criminal Justice. Definitions for this act are found under 2C:20-23. They may be viewed at NJ Computer Crime Definitions.

Title 2C:20-25 Computer-related theft. Theft under section 4 of this act 2C:20-25 constitutes a crime of the 3rd degree.

Title 2C:20-26 Property or services of $75,000 or more; degree of crime; 2nd degree.

Title 2C:20-27 property of services between $500 and $75,000; degree of crime; 4th degree.

Title 2C:20-28 Property or services between $200 and $500; degree of crime; 4th degree.

Title 2C:20-29 Property or services of $200 or less; disorderly persons offense

Title 2C:20-30 Damage or wrongful access to computer system; no assessable damage; degree of crime; 3rd degree.

Title 2C:20-31 Disclosure of data from wrongful access; no assessable damage; degree of crime; 3rd degree.

Title 2C:20-32. Wrongful access to computer; lack of damage or destruction; disorderly persons offense.

A person is guilty of a disorderly persons offense if he purposely and without authorization accesses a computer or any of its parts and this action does not result in the altering, damaging or destruction of any property of services

The penalties for the different crimes are as follows:
1st degree: 10 – 20 years in prison
2nd degree: 5 – 10 years in prison
3rd degree: 3 – 5 years in prison
4th degree: Not to exceed 18 months in prison
Disorderly person's offense: Up to 6 months in prison.[11]

The penalties that the State of New Jersey has enacted were created to show hackers that the crime of "hacking" will not be tolerated without serious consequences. Possible penalties based on New Jersey laws are as follows.

A hacker may easily break into another person's computer with out causing any damage or theft and can be found guilty of Title 2C:20-32. A hacker found guilty of Title 2C:20-32 will receive a disorderly person's offense. This could end with the hacker going to jail for up to 6 months. As the hacker's level of damage increases so do the penalties.

I find it doubtful that a 15 year old hacker will consider the consequences of his actions for what he thinks is a fun time breaking into a company's network and stealing or damaging their systems. Simply stealing or damaging between $500 and $75,000, can land the hacker in jail from 18 months to 5 years. Many of these penalties with also leave them with a criminal record that will stop them from ever getting a computer job in many industries. If the conviction is considered a felony, the rights to vote as well as other privileges are lost.

Many large companies will bring litigation against any hacker that causes them financial hardship. These companies will also use many of their resources to push for maximum penalties against the hacker. The hacker does not think about the time and resources that will be used to solve the problems created, the lack of business being done due to the damage created, or the possible damage to the company's future integrity and business.

One of the worst penalties a hacker can be convicted of is a crime of the 2nd degree which could easily leave them in jail for up to 10 years. This type of penalty is mostly applied to the hacker that has committed a hack with a value of over $75,000, or has interrupted or impaired any type of public communications, transportation or other public service. This is meant to convict the hacker that takes down any utility company or service (electric, gas, water or phone).

Even with these laws in New Jersey, the Federal Government is attempting to pass, the "Computer Security Enhancement Act of 2002". It's meant to convict the hacker who has gone the final step by committing a hack that has caused the death of an individual or a crime of equal harm.

I hope that these laws will be useful in teaching the black hats of the future that the government is not willing to accept their behavior without an equal punishment. Black Hats must remember that don't do the crime if you are not willing to do the time.

Personal Experiences with Teenage Hackers

Having worked two years in a 7 -12 school district, I found that many of our upcoming students believed that they could accomplish anything when it came to computer programming and networking. This belief for many students inevitably became their downfall. Students who were in the advanced computer science courses or independent projects class certainly believed they had the ability to out think and outmaneuver their teachers, and the computer department, when it came to hacking against the school district. I have a few prime examples, of how overconfidence can destroy a future career.

The first case I was involved with was about a student sending a life threatening email to the President of the United States. The student sent an email with the signature of another boy from a different school district. This student believed that he was clever enough to forge a reply email address of the other student. Unbeknownst to the forger, the U.S. Secret Service received the email and started an investigation into the threat. They sent agents the following day to the home of the alleged student who had sent the email and questioned him as well as his family. They found out the student had been threatened by the forger with a threat that he would find a way to cause problems for him.

The Secret Service, during this time, had traced back the email to our school district. When they questioned our computer department we were able to look through our firewalls log file and find the machine where the forger had sent the death threat email. Our department was then able to look at our audit log files and find out who was signed on to the specific machine at that exact time. The Secret Service held a closed meeting with Superintendent of Schools, the forger, his father, and his attorney. The outcome of the meeting was never fully disclosed, the rumors were that there would be no jail time, but he was given an out of school suspension for five days. There would also be a copy of this crime put into his permanent school and civilian records.

My second case with overzealous hackers was with two students who were best friends and were in an advanced computer science class. The two boys blatantly told friends of how they were much better at computers and programming in the language of C than was their instructor. This belief in their abilities became a crucial downfall for both of them. The first trouble they got into was when they were caught with illegal programs in their personal folder on the school server. They combined this with writing programs that enabled them to break into the very core of the Microsoft NT 4.0 operating system. This initial breaking of the school's Computer and Internet Usage Policy caused them to be brought before the Vice Principal, their instructor, members of our computer department, and their parents. The father of one of the boys was a Vice President of computer security for a computer laboratory in New Jersey, which worked on research and development for major corporations. The father told us that he gave his son complete access to a Microsoft Developer kit from work and wanted him to use it to his better himself. The father said, "I want to give my son more than I had available when I was growing up, as well as give him an advantage when it comes to competing in college."

The student's instructor still had faith in the boys and asked that they be given a lenient punishment for their crime. They ended up receiving Saturday detentions for one month. Those of us in the computer department had pushed for further sanctions against the boys, but were turned down by the school.

We had all thought that there would be no further problems with either of the boys after this episode, but we were wrong. Less than six weeks after receiving their punishment our computer anti-virus program, Symantec's Norton Anti-Virus, sent us a message that it had caught a virus on a computer in one of the computer labs. Upon our investigation we found that these two boys had downloaded a virus engine off of the Internet and were including it as a part of a new virus they had been coding. What they didn't realize was when they finished the compile phase of the new virus Norton's blood hound technology detected the new executable, quarantined the program and alerted our department. We then reviewed our audit files and found the user id of the student responsible.

Upon gathering this information we looked through the student's folder on the server and found the rest of the virus engine package.

For these two boys their desires of a great college accepting them into their computer science program had just been destroyed. They were officially failed in the computer course, given a letter about the punishment in their permanent school records, and were not given any faculty recommendations for their college entrance applications. Here is a situation that may not have left the boys in jail, but they well may have ruined their entire future career in computer science.

My third case was with one boy who specialized in theft of services and passwords. He would steal other students' passwords and use their accounts to steal their work. We had many reports from other students on who they believed the culprit was, but we had did not have credible evidence against the student. His final crime was when our Unix Serve came to a screeching halt due to a lack of hard drive space. Upon our research we found out this student had downloaded files from other students, as well as the Internet, to his server folder. He had used up over 25 gigabytes of space on the server. Our downfall in this situation was that we had no quota management running, which would have stopped this before it had gotten out of control. This student finally had received enough warnings that the school suspended all of his computer privileges for the rest of the school year. This in turn caused him to fail a Calculus class, which had required him to use specific software in his class final project.

During the review of these three cases I can say that I learned as much about computer security, as the students learned about the consequences for being hackers and breaking school rules and policies.

How to Monitor your Child and Prevent them from Evolving into the next "Black Hat!"

Parents must be aware of their child's activity on the computer at all times. There must be concern if the child is spending more time on the computer than interacting with friends or engaging in other activities.

Simple things such as E-mail or Instant Messaging programs are especially instrumental in luring today's youth toward an addiction to the computer. In many cases, this addiction can lead to much more than a career in the computer field. It can, unfortunately, lead to a life of imprisonment.

Many surveillance software programs are available for purchase. They will enable you to oversee and track your child's activity, with or without their knowledge.

These tools are broken into the two categories of hardware or software. On the hardware side are keystroke loggers. These devices connect in between the keyboard and the computer. Two products available are KeyGhost keylogger and from Allen Concepts three models of KeyKatcher. These products are mostly different on how large the devices are and the amount, keystrokes they can record. More information on these can be found at http://www.keykatcher.com/ and http://www.keyghost.com/products.htm.

Being hardware based key loggers make it useful only for situations where the individual being watched can not see the back of the computer or if they can see it are not knowledgeable enough to know what a key logger is. Someone like my

wife would be perfect for using a key logger, for she doesn't know one end of a computer from the other. Another problem that I have with the hardware key loggers is that you must obtain access to the computer the device is installed on, in order to retrieve the captured data. If you are looking to capture data from a child that is very computer literate, I doubt a key logger will work for you. Most children in the family end up being the sole computer repair technician for their families. If these key loggers are not an option, you will need to move on to the software side of the family.

The software side is broken into two areas for family use. They are either key loggers or activity monitors, key loggers are like their hardware cousin, while activity monitors are capable of also taking screen shots, recording who and when the activity was taking place, as well as all keystrokes. Following are some of the software packages available for the home user.

iOpus Starr Pro edition	http://iopus.com/
NetObserve	http://www.exploreanywhere.com/
Spector Pro	http://www.spectorsoft.com/
Spytech SpyAgent	http://www.spytech-web.com/
WinRecon	http://www.winrecon.com/
WinWhatWhere Investigator 4	http://www.winwhatwhere.com/

A complete review of these products can be found in a great article from PC Magazine July 2002 called Watching You, Watching Me.
http://www.pcmag.com/article2/0,4149,45,00.asp
Another review of WinWhatWhere Investigator 4 can be found in the current issue of Security Magazine August 2002 as well as online at the
http://www.scmagazine.com/scmagazine/2002_08/survey/products_01.html#WinWhatWhere%20Investigator
If you would like to see how many spy programs are available please follow this link http://www.trapware.com/PressBigBrother.html

Many children will install software programs that allow them to change the computer screen to a fake word processing program or spreadsheet to fool the casual viewer into thinking they are doing homework. In these situations the only way to observe is to record with software based spy ware.

To get more information on these products I downloaded and installed on a Windows XP home edition system all of the above products expect Spector Pro, which was not at the time offering an evaluation version.

The first program I tested was WinWhatWhere Investigator 4. I was impressed with the screens shots and the depth of information that it saved, especially when it came to browsing on the web. I did notice that when working in Microsoft Outlook it failed to give me the name of the person that I had added in the To: box.

The second program that I tested was NetObserve. I liked the wizard that ran through all of the options upon initially starting the program. The quality of the screen captures were not as clear as what I observed with WinWhatWhere. I also had a problem with it incorrectly finding my IP address, instead of picking my computers address it picked up the routers. The logs were pretty valuable, but not as informative or thorough as that of WinWhatWhere. I did like the feature of being able to review instant messaging program chats.

The third program that I tested was WinRecon, which may have been a fine program, but I could never get it to capture screen shots without causing an error and shutting down.

The final package that I tried was IOpus Starr PC & Internet Pro edition. The software seemed to be more thorough than NetObserve, but not as thorough as WinWhatWhere. I tried doing an Instant Message, ran and typed in a few programs, and then went into the control panel to see how it would record these steps. The only problem with the screen shots settings was you could only take a picture with a minimum of one minute intervals. I would have preferred intervals based on seconds as well. I did like the fact that it could send information via email to anyone, and it could by pass a personal email account.

I am sure that if I had more time to review each of the products over a period of a week each, I could gather more critical data on them, but with the limited time available I would say my first choice would have been WinWhatWhere. I only wish that I could have reviewed Spector Pro to compare it to the competition. If you are interested, most of the packages will give you a 14 day trial of their software. If you are interested in even more information about the user, you may wish to combine these with a Web Cam solution.

Lastly, a means to oversee your child's computer activity is by using a combination of hardware and software with Web cam Surveillance software. These products connect a camera to your computer and take pictures of anyone sitting at the computer. They can be used as motion detection devices as well. Some products even allow you to watch over the Internet from anywhere in the world, over a broadband connection.

Some of the products available are as follows.

Capturix VideoSpy	http://www.capturix.com/english/index.asp
Gotcha!	http://www.gotchanow.com/
Watcher and RemoteView	http://www.digi-watcher.com/
WebCam Watchdog	http://www.webcam123.com/en/en-index.html

A complete review is available in the July 2002 issue of PC Magazine or at http://www.pcmag.com/article2/0,4149,120742,00.asp

If you decide to use of a web cam package you may or may not have much luck watching over a skilled child. They will most likely be able to circumvent any recording from these packages. I believe these are more useful for children that you have good trust relationship with, and only when you are using it a deterrent from the casual problems with Internet usage.

I can only recommend that you must decide whether to talk to your kids and tell them that you will be watching what they do or perform your surveillance with out their knowledge. If your child is very proficient on the computer, they could utilize software that is available that detects spy software on the computer.

Some of these products are:

Spy Cop	http://spycop.com/spyware-safety.htm
Who's Watching Me	http://www.trapware.com/index.html
Ad-aware ver 5	http://www.lavasoftusa.com/ *free*

Free Ways to Watch Over Your Child

If your computer system is using the Windows 2000 or Windows XP Professional operating system, there is a built in feature of file and printer auditing. This auditing enables you to view the date, time and person who has downloaded and installed any programs or saved any files. You can also see what has been printed by whom, and when it was done. This feature came in very handy for catching many students at a school district that I worked for when they were in the last row of computer labs, downloading and installing software.

Another option that I have found is available on Windows XP Home version is giving children limited user rights. As long as everyone's accounts are password protected the child will be limited to a degree on what they can install or do. This is not the cure all, but it is a free feature in this version of XP.

CLOSING

Hopefully this information will give you a review of why, and how, your child can become hooked on the art of "Hacking," as well the possible penalties. I suggest that you speak to your child and discuss the pros and cons of working with computers. This preventive action should be viewed in the same light as if you were talking with your kids about Alcohol and Drugs. Parallel the dangers of being drawn into computer crime, just as though you were informing them of alcohol and drug addiction.

Many children don't think past the current day, so they fail to realize the consequences of their actions. They may consider minor hacking fun and not of any danger to themselves or the family. We all want the best for our children, but with that new tool, the computer, in the family comes much responsibility for the parents or guardians. We all must not just plop the computer down and give our children full access to the computer, with out some sort of supervision. As our children use the computer to learn and grow, so should we the supervisors of the family. Take the time to learn about your computer and what can be done with it by looking into local computer classes. Many high schools or colleges offer adult programs. You can also look for Internet sites to educate yourself or find a mentor from your area. We must all continue to learn, to improve ourselves and protect our children.

ENDNOTES

[1] Robert Trigaux, The Underbelly of Cyberspace, June 14, 1998, http://www.sptimes.com/Hackers/underbelly_of_cyberspace.html

[2] Michelle Delio, "A White Hat Goes to Jail.," http://www.wired.com/news/infostructure/0,1377,44007,00.html, May 22, 2001

[3] The SANS Institute, GSEC course manual, November, 2001

[4] Dan Verton, Confessions of Teenage Hackers, 2002

[5] Tina Darmoyray, At Who's Expense?, April 2002, http://www.usenix.org/publications/login/2002-04/openpdfs/point.pdf

[6] Rob Lemos, Hacking their Image, 2 August 2002, http://news.com/2009-1001-947682.html

[7] Redif, Guide to the Net, 18 April 2002, http://www.rediff.com/search/2002/apr/18ankit.htm

[8] Declan McCullagh, Defcon Keeps Hackers Hooked, 16 July 2002, http://www.wired.com/news/print/0,1294,45248,00.html

[9] Matt Markovich and Suzanne Brahm, Tech Live, 22 March 2002, http://abcnews.go.com/sections/scitech/TechTV/techtv_netaddiction020322.html

[10] Frontline, Computer Crime Laws, PBS Television (WGBH Television, Boston) http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html

[11] Information from interview with a Criminal Attorney who wished to be left anonymous for this students paper.

Last Updated: September 24th, 2017

Upcoming Training

SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event