

8-24-2005

The Role of White Hat Hackers in Information Security

Amit Anand Jagnarine
Pace University

Follow this and additional works at: http://digitalcommons.pace.edu/honorscollege_theses



Part of the [Other Computer Sciences Commons](#)

Recommended Citation

Jagnarine, Amit Anand, "The Role of White Hat Hackers in Information Security" (2005). *Honors College Theses*. Paper 14.
http://digitalcommons.pace.edu/honorscollege_theses/14

This Article is brought to you for free and open access by the Pforzheimer Honors College at DigitalCommons@Pace. It has been accepted for inclusion in Honors College Theses by an authorized administrator of DigitalCommons@Pace. For more information, please contact rracelis@pace.edu.

The Role of White Hat Hackers in
Information Security

Amit Anand Jagarine

Pace University
Phorziemer's Honors College
Thesis Paper
Due Date: 16 May 2005

The Role of White Hat Hackers in Information Security

Information security has become one of the most important concepts in our information and technology driven world. Because of this notion of ubiquitous computing and the on-demand flow and exchange of information, it becomes essential to protect and secure any and all critical information. Information security involves employing certain techniques and components to protect interconnected systems and more importantly, the data and information used by those systems. It revolves around maintaining three basic characteristics of information—confidentiality, integrity, and availability. The goal of information system security has now been augmented by what is known as “white hat” hacking. White hat hacking is an interesting development in the fight against keeping the bad guys out and securing sensitive information. The idea is that there exists a new breed of ethical-minded hackers that penetrate systems to aide companies and their systems administrators in securing the information and technology that keeps their businesses running. White hat hacking is an exciting new take on information security and is a fairly new concept where the premise is that if you want to catch a criminal you must be able to think like one to stay one step ahead. In the 21st century, computers are networked to share information and an ever-growing number of security threats and vulnerabilities are reported daily. Therefore, we can understand why the use of “white hat” hackers to aide in the battle to secure crucial information is a significant development in a world of 24/7 communications and information sharing that is not close to being 100% secure.

The dilemma surrounding information security has its roots in this concept of ubiquitous computing and the constant exchange of information. Ubiquitous computing refers to this notion that information is everywhere due to the fact that computers have made it almost effortless to disseminate and transfer it quickly and efficiently. Author Douglas Thomas (2002), in his book entitled *Hacker Culture*, comments upon the relationship between ubiquitous computing, hackers, and end users:

As computers become an increasingly ubiquitous part of life and the workplace, the demands for ease of use by consumers as well as demands for high levels of technological sophistication increase. As a result, consumers demand more from their technology while understanding it less. That gulf between the end-user and the expertise of the hackers is growing increasingly wide and provides the greatest threat to security. (p. 66)

Since modern day consumers demand user friendly machines, applications, and devices they are becoming less aware of how the technology works making them more susceptible to social engineering and hacking attempts. With the explosion of the desktop computer, the Internet, the client/server model, and distributed computing, information is everywhere, is non-stop, and more often than not, proves to be extremely critical. In every industry and arena, the increasing need for information security is evident. Businesses rely on secure networks to exchange information, want to make sure data integrity isn't compromised, and need to be certain that their operations can be carried out successfully and securely with as few hiccups and breaches as possible. The government and military need to be sure the systems that house confidential and classified information remains private and secured so the country can remain safe. The

personal user also wants to make sure that their information is kept secure. As information becomes available, easily accessible and the methods for using technology become ever more simplified, tech savvy hackers with malicious intent pose serious threats to securing information. This is why we want to have the best access control methodologies (i.e. passwords, fingerprint scanners) that will authenticate and verify the identities of legitimate users. We also want to implement firewalls and network monitoring tools to keep intruders out of our systems and away from critical data. With this concept of white hat hacking, not only can we use all the tools and technologies currently available but we can now employ hackers to help us to secure our information.

In the modern day sense, those who attempt to bypass information security access controls in an effort to pose as authorized users are generally classified as hackers. It is important to remember that a hacker is an unauthorized user who attempts to gain access into a system. They do not have permission to enter the system and do so with the risk of being caught and persecuted based upon established laws. In the new era of computing, there has been this emergence of a new breed of hacker known as the white hat hacker. The goal of the white hat hacker is very different from their counterparts, known as black hat hackers or crackers. The white hats attempt to infiltrate systems in an effort to help identify weaknesses so they can be patched in time before the black hats find and exploit these same vulnerabilities. Another group, known as the grey hats, are somewhere in the middle as their allegiance to a single side remains unclear. Regardless of the category of hacker, by definition, hackers essentially lack the permission to enter a system or view certain pieces of information. Hackers often trespass into computer networks and can intercept confidential information by using hacking tools and applications or can simply

evade authentication and authorization schemes to snoop around. However, since white hatters break in to help identify and patch the flaws then evidently intent is really the fundamental idea used in classifying hackers. With the plethora of terms used to describe hackers, it makes sense to start somewhere at the beginning of “hacker” history so that we can gain a better understanding of how these classifications have developed and why “ethical” hacking has become important.

The term hacker was originally used to describe those individuals who possessed a more advanced perspective and handle on the concepts behind computers and programming languages. Initially, there was no stigma or negativity attached to the term. The first generation of expert computer scientists, programmers, application developers, and technology leaders were hackers. Being called a hacker meant something different to the first groups of computer experts. It meant a high level of computer skill and technical know-how that placed them in a different category from their peers. A hacker was simply someone who was quite knowledgeable and could make a computer or system do something new or something that it wasn't designed to do.

Hackers were people who saw beyond the boundaries and limitations imposed by others and sought to use their skills toward improving or sharing knowledge. Steven L. Kleespie's (2000) article entitled “The Role of “White Hat” Hackers in Information Security,” provides clear and concise definitions of what it meant to be a hacker and what hacking was about prior to the recent stereotype:

‘Hacking’ is defined as making a modification to something to improve it or to make it do something it was not originally intended to do. Media coverage has given the term ‘hacker’ a negative connotation. However, the original usage was

complimentary, indicating someone with a high level of technical sophistication, or someone who enjoyed the intellectual challenge of overcoming or circumventing limitations. (¶1)

Kleespie points out that hacking in the true sense was about making changes to improve or change the way a system or application might function. The ultimate goal of the hacker was not to disrupt or destroy as most people seem to believe, but the objective was to take computing to the next level. Being called a hacker implied that you were knowledgeable, talented, and simply had that special knack with computers. The term hacker was not surrounded by the negativity that it is often now associated with.

By taking a look back at original hackers and the history behind their activities, it becomes easier to see how much has changed in terms of the goals and perspective of the hacker. Thomas (2002), in the introduction to his work, reveals this concept of what hacking was about and how it has changed over the last few decades:

Computer programmers from the 1950's and 1960's, who saw their work as breaking new ground by challenging old paradigms of computer science, think of hacking as an intellectual exercise that has little or nothing to do with the exploits of their 1980s and 1990s counterparts. (p. ix)

Thomas reveals that the hackers/programmers of earlier generations were involved in something ground-breaking—far from anything that could be considered criminal. These computer science gurus had very different goals. Rather than attempting to snoop, destroy or damage, hackers of the older generation wanted to create, share, and improve. They were the brilliant programmers and software developers who could create robust applications quickly and easily. The new hacker generation may have the same technical

expertise as the older generation yet have become mixed up in the darker side or underground-type activities. Gradually the idea of what a hacker is and does changed. The media and mainstream gave hackers a bad name and now a hacker is often associated with rebellious, unruly, and now even illegal activity.

It is important to remember that a hacker in general is anyone who attempts to utilize hacking techniques to find security flaws and loopholes in the systems they are attempting to infiltrate. To create a distinction between those hackers with malicious intent and those seeking to do something more positive, the term “cracker” came into use. The terms hacker and cracker are often used interchangeable although there is an important difference. A cracker is defined as someone who breaks into a system and has malicious intent. According to George Reynolds (2003), author of *Ethics in Information Technology*, a cracker is someone engaged in criminal activity: “Crackers break into other people’s networks and systems, deface Web pages, crash computers, spread harmful programs or hateful messages, and write scripts and automatic programs that let other people do these things” (p. 60). Crackers are the subset of the hacking community that attempt to circumvent security controls so they can gain unauthorized access to information and confidential material. Once they are able to sidestep security controls and exploit a flaw in the system, they can do any number of harmful things. What separates a cracker from a hacker is that crackers are those with destructive or evil intent while hackers and more specifically, white hat hackers have something very different in mind.

There are two major groups of hackers that have emerged in the 21st century. One group is known as “white hat” hackers while the other is known as “black hat” hackers

(crackers). These terms play on the old western movie conventions where the good guy could be recognized by their white hat, so the terminology used reflects the conventional good guy theme as represented by the color white. A white hat hacker is someone who attempts to find and point out those security flaws, loopholes, bugs, etc. to the company and people running the system or network. By reporting these issues, white hat hackers are providing a service so the information and technology being used can be further secured. After these “ethical” hackers have reported what they were able to do and how they went about doing it, the systems administrators or security consultants can make the necessary adjustments to keep the bad guys or “black hat” hackers out.

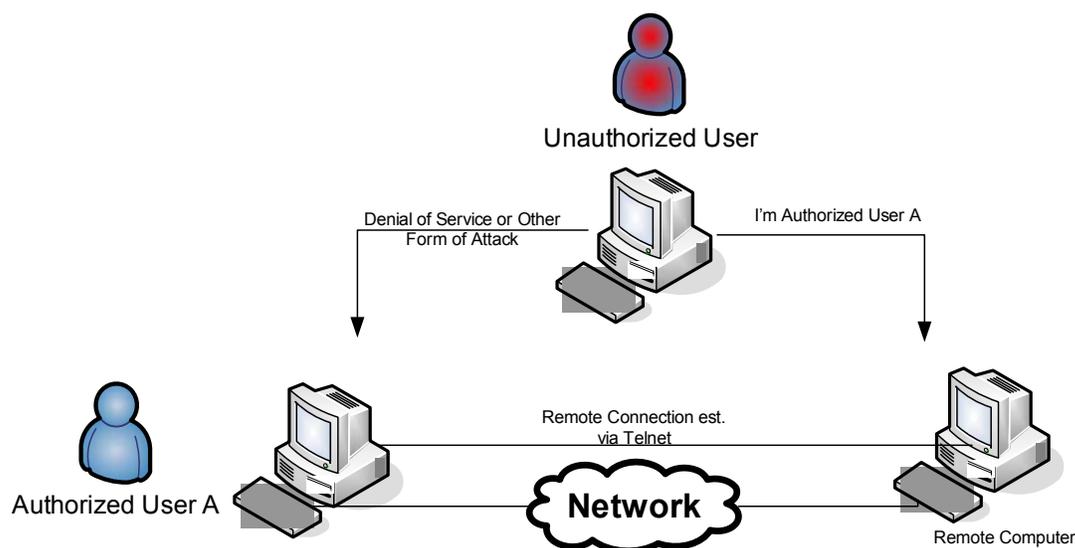
There are a number of key ideas that are very important to understanding why white hat hacking is of interest. First, it is foolish to believe that those programmers, network specialists, and administrators who create and design applications and systems will be able to recognize how their system can be exploited. Often times, those genius minds that are behind some of the greatest applications fail to address some of the most basic security issues. Just take Microsoft’s current Windows Operating System called Windows XP as an example. The Windows XP platform is probably the best Microsoft Operating System to date yet there have been so many security flaws that new patches are released every few weeks and “security packs” have been created to address bigger issues. Because the developers are the people who create security controls and are not the ones who are attempting to circumvent the controls, they are unable to find vulnerabilities. Bruce Schneier (2000), computer security expert and author of *Secrets & Lies*, states that hackers are very keen and are experts at examining the system from a perspective that often eludes system creators:

Hackers can have considerable expertise, often greater than that of the system's original designers. Hackers look at a system from the outside as an attacker, not from the inside as a designer. They look at the system as an organism, as a coherent whole. And they often understand the attacks better than the people who designed the systems. (p. 44)

If you want to protect your network, your software, your hardware, or any other component that directly impacts upon information security, you have to understand what makes it insecure. Finding the Achilles' heel and fixing the vulnerabilities is often difficult and usually doesn't come from the mind of the system creator, it comes from the mind of those who tries to exploit or expose your weaknesses. What makes white hat hacking so significant is that white hat hackers essentially have the same thought processes, skills, and tools as the black hatters allowing us to fight fire with fire so to speak.

A white hat hacker may employ the same techniques as their malicious counterparts, but after a weakness has been identified, they will report back to the company or system administrators so the vulnerability can be patched. There are many techniques that hackers use to gain unauthorized access to information. One technique is known as network scanning/probing. A scan or probe is considered to be a security compromise where a hacker may attempt to systematically find those communication ports along the network that are open and able to return information. Once the hacker knows what ports are open and what information can be returned, they have an insight into where the network may be exposed for a future attack.

Another technique used by hackers is known as session hijacking. When users attempt to establish one-time remote connections to other computers on a network, hackers look to steal these sessions so they can have the same privileges as the authorized user. The following diagram, taken from Harold F. Tipton's and Micki Krause's (2001) book entitled *Information Security Management*, gives us a graphical depiction of this common hacker employed technique known as session hijacking:



The authorized user is establishing a remote connection/session with another computer on the network by authenticating (entering username/password) and using the standard Internet protocol known as Telnet to remotely connect. This will allow the authorized user to view and edit files and execute commands on the remote machine. The unauthorized user hijacks this session by using a session hijacking tool to discover a weakness in the protocols or applications used. The unauthorized user will then pose as “Authorized User A” and is able to steal the session and execute commands during this exchange as an authorized user. In any security breach, it would be a nice to know and comforting to find out that the unauthorized user that may have previously probed your

network and was now able to steal a remote session was a white hat hacker. The white hat hacker would report that how they were able to find the open ports or how they hijacked your session alongside what methods were employed in making it a successful hack.

Some white hat hackers are hired for their services and become the security personnel or consultants who get paid to secure a company's systems. According to Kleespie's (2000) article, the consultants "believe their 'white hat' hacks provide a good starting point for network protection by offering a baseline for information security policy and practices." The idea is that white hat hackers can be hired to hack your system and point out any security weaknesses before black hat hackers do so and damage internal systems, business operations, or even company reputation. If a company's main selling point is its reliability and commitment to the customer, a single distributed denial of service attack (where multiple PC's are used to send continuous requests to a company's servers that overloads the system and service request from legitimate users cannot be completed) can ruin the company's reputation. Often times, it can be more costly if a black hat hacker were to hack into a system and make changes or release malware (malicious software i.e. viruses) that could negatively impact upon the company and its ability to function properly. White hat hacking proves to be a benefit as it promotes the main idea behind information security: maintain functionality while safeguarding our crucial information. If white hat hackers can help a company keep its information and data safe and help to safeguard the technological assets of the company which in turn will help the business to continue functioning properly, then white hat

hacking can be viewed as an extremely beneficial means of fostering a secure operating environment for any organization.

As white hat hackers have separated themselves and made their services available, companies have made use of their expertise and experience to protect and secure their systems. According to an article found in the on-line publication of Dataquest Magazine (2000), white hat hackers were initially perceived by corporations as a gift: “For desperate corporates keen to seek bugs in their network security and plug them before they are exploited for nefarious ends by malicious ‘black hackers’, white hat hackers were like manna from heaven.” As threats and vulnerabilities have steadily increased over the past few years, many large corporations have been making use of the newly emerging white hat hacking community and are using white hat hackers in some form or another. The article goes further to say that many of today’s biggest companies including KPMG and Computer Associates are hiring white hat hackers to be a part of their security personnel or part of specific IT units that are created specifically for security purposes: “These units build security into a newly-developed e-commerce package, identify the vulnerabilities and then design defense mechanisms accordingly” (http://www.dqindia.com/content/top_stories/100101410.asp#interact). As companies are beginning to understand the increasing benefits of having experienced white hat hackers on their side, they are starting to make good use of the talents and skill of this subset of the hacking community.

Hiring white hat hackers to be a part of the security personnel or security staff of major corporations has become a growing trend. Instead of sitting back and allowing black hats to break in, companies are now deciding to fight fire with fire. As reported by

Jack M. Germain (2004) in his article entitled “Moral Dilemma: Hackers for Hire,” companies are utilizing hackers to a greater extent:

Using hackers to bullet-proof computer networks is still going on. Companies employ former hackers to do their bidding. It's moving upstream to big companies. As a result of the recent increase in the number of virus and hacker attacks, corporate officials at higher levels are much more aware today of the need to test system security. (n.p.)

Company officials wish to create a safe, secure, and efficient operating environment for their businesses which is why they are turning toward hackers as another tool for creating such an environment. Just as companies make use of firewalls that inspect data packets traveling over the network and intrusion detection systems that monitor activity on standalone PCs or on the network itself, using white hat hackers to find vulnerabilities is becoming commonplace. The white hatters that are frequently hired are more often those with no criminal history yet have the same aptitude and skill as their black hat counterparts: “The practice of using good hackers is widespread. White Hat hackers are seasoned programmers with no criminal records” (Germain, 2004, n.p.). All corporations have assets and confidential information that need to be protected. The growing trend has been toward making use of white hat hackers to aide in the quest for information and system security on the corporate level.

Beyond the group of white hat hackers that are hired to be a part of a company's security staff, there are security consultant groups whose services can be outsourced. These organizations provide security services as they are not directly part of the company but are hired to perform a specific duty—in this case, to test a company's system and find

vulnerabilities. A company may outsource their security to these white hat hacking consultants as they may feel that their in house security staff is unable to find all weaknesses in their system.

There is also the group of unpaid, white hat hackers who are just “free spirits” as Kleespie (2000) reports in his article. The main difference between company hired white hat hackers and the unpaid, free spirits is their motivation. Security specialists are hired to provide general security for the organization, are restricted by company policy and procedures, and are paid to do a job. The free spirits on the other hand, adhere to an unwritten code of ethics that promotes ideas such as free and unrestricted access, less limitation, and creating a better lifestyle by using computers to their greatest potential. Free spirits hack into systems for any number of reasons—pleasure, fun, the allure of a challenge, and often hack as a hobby or pastime.

The free spirit group believes that their actions are meant to help even if they themselves seem to pose a threat. They feel that their role is to promote something positive and their hacking exploits are about aiding in the overall objective of securing and protecting. The ultimate goal of the unpaid, white hat hacker is to help identify security weaknesses by hacking into systems and reporting these weaknesses. Free spirit hackers attempt to utilize computers to do what seems to be impossible or to simply explore and go beyond established regulations or limitations. These free spirit, white hat hackers utilize their technical savvy in a way that can aide others. It is likely that the same technical savvy would be used in a malevolent manner so they truly believe they are providing an invaluable service.

Depending upon the type of white hat hacker, the method of reporting what they have discovered can vary. A company that has hired white hat hackers as part of their security team will likely have the individual white hat report and fix any problems they have found. Hired security consultants for a nominal fee, will penetrate a system and then report what they have found directly to the company. The free spirit white hat hacker however, has no direct contact with the company or administrators of the system they have found to have flaws. Probably the most interesting aspect of how these free spirits operate has to do with their method for reporting what they have found. Initially, they will attempt to inform the company directly with their findings. This is usually difficult because company executives and security officers are usually unwilling to listen to someone who claims to have hacked into their system. If the company fails to respond, the free spirit white hat hacker will post their findings on certain websites so that even if the company chooses to ignore their report, the hack has been made public. Once the hack has been made public, it forces the company to address the issue to keep others from exploiting the company's weakness.

The free spirit hackers are probably the best example of what true hackers seek: openness, cooperation, and freedom to explore. These ideas are central in understanding why someone would want to break into your system and then let you know how they did it. It is not so much about breaking in as it is about exploration and discovery. Hackers believe that secrecy and privacy are not the values associated with what has made computers such a significant part of the modern world. Openness, communication, and collaboration between entities are the pieces of the technology puzzle that consistently revolutionize the world. The attempt to stifle, privatize, and monopolize the information

and technology that drives our global economy is what destroys the creativity and teamwork that so much of our modern technology was based upon and furthermore, gives hackers more reason to explore and uncover.

The hacker community believes that information yearns to be free and that technology should be available in the more complete sense where there are few limits and restrictions. Author Pekka Himanen (2001) in his book entitled *The Hacker Ethic* discusses what this hacker ethic is all about: “(Hackers) are people who ‘program enthusiastically’ and who believe that information sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing free software and facilitating access to information and to computing resources wherever possible” (p. vii). Generally speaking, hackers believe in the notion of free information and utilizing advanced or previously unknown knowledge to make the best use of computers and technology. This notion can be directly applied to the thought processes of the free spirit white hats that break into systems for the sake of improving security. We place locks on doors and alarms on cars but in order to get that that point, we first discovered that without these features, security could easily be compromised. We have to initially break in to discover how to protect our homes, our cars, and now our computers and information. In order to protect, we had to first find new things and set new boundaries by exploring, communicating, and working together—the very ideas that are promoted by the hacker community and are important to understanding the intertwined relationship between hacking and information security.

Understanding that this bond between hacking and security plays a crucial in keeping our information confidential, there have been a number of specialized programs

that have surfaced promoting white hat hacking. In May of 2003, an article written by Julie Flaherty appeared in the New York Times entitled “Enlisting the Young as White Hat Hackers.” In her article, she talks about how a gentleman named Mr. Robinson running a small information security company, started an after school program for teens interested in the ethical side of hacking. The program is meant to teach the youngsters how to ethically hack into a system so that they can protect it from those black hat hackers who may want to do harm. This non-profit program takes students, regardless of their grades, and gives them an opportunity to apply their hacking skills toward protecting information. Most of the students who signed up have already had previous experience hacking into different systems and are not just script kiddies (novice hackers). As companies look to protect their systems, these students may be the next generation of security specialists that will be in demand. The students not only receive training in terms of hacking techniques, but they learn about the ethical dimensions of their actions as well as the legal consequences. Although the students are being trained to be hackers, Robinson makes an interesting point in the article: “We are teaching them to be hackers, but wouldn't you rather have them on your side?” By training these students and giving them the opportunity, the program may potentially lead to an elite group of white hat hackers whose skills go above and beyond those of their black hat counterparts. By fostering an environment where students are able to apply their current skills, learn new skills, gain exposure to the latest system and trends, and learn about morality and ethics, the program provides an ideal starting point for training real deal white hat hackers. Instead of hiring outsiders or consultants who may or may not be trustworthy, it is advantageous to hire a younger, fresh mind that has been trained specifically for

protecting information. This is the type of program that can produce highly skilled, white hat hackers who are ready to take on the challenge of securing and safeguarding the non-stop flow of critical information vital to a technology driven world.

GlobalNetTraining.com and Blackhat.com are two sites for organizations that seek to train white hat hackers. They offer workshops, conferences, and security briefings that are geared toward preparing better IT security professionals. The program offered by GlobalNetTraining is a five day course that gives the student a basic understanding of how systems can be compromised and what can be done to secure them. GlobalNetTraining assures that the program helps certify individuals in network security and teaches them to look for system weaknesses and vulnerabilities using the same knowledge and tools of the malicious hacker. GlobalNetTraining.com and BlackHat.com offer similar programs that expose their clientele to the same kinds of tools hackers use. By helping us understand the mind of the hacker and knowing how those individuals can take advantage of poor security implementations, these programs can help corporate security professionals keep the bad guys out and allow companies develop their own set of white hat hackers.

According to an article entitled *U.S. Military's Elite Hacker Crew* by John Lasker of WiredNews.com, even the U.S. military has reportedly assembled an elite group of white hat hackers to help protect the networks of the U.S. Department of Defense. Since the Defense Department was the target for some 75,000 intrusion attempts in the past year, the creation of such a group was deemed necessary. Based upon Lasker's report, it seems that unit is currently the world's most elite hacker group ever assembled for the purposes of security:

The U.S. military has assembled the world's most formidable hacker posse: a super-secret, multimillion-dollar weapons program that may be ready to launch bloodless cyberwar against enemy networks—from electric grids to telephone nets. The group's existence was revealed during a U.S. Senate Armed Services Committee hearing last month. Military leaders from U.S. Strategic Command, or Stratcom, disclosed the existence of a unit called the Joint Functional Component Command for Network Warfare, or JFCCNW. (2005 n.p.)

After September 11th and due to the increased potential for terrorist attacks, the government has made it a priority to seek the best white hats and make them work toward creating a secure homeland. As the need and demand for security specialists has increased due to the rising number of attacks and threats, the number of services and programs promoting white hat hacking has increased alongside the growing trend of hiring and utilizing white hat hackers to aide in information security. If the present is any indication of the future there will likely be many opportunities for skilled, ethical-minded hackers to cultivate their skills and utilize their abilities to work to protect the systems of companies recruiting for their security departments as well as government agencies and the military.

Although we hardly hear of them, there are a number of white hat hackers from all over the globe making real contributions toward creating a safer and more secure environment for all. Mr. T. Shimomura, a computational physicist and security expert, setup network monitoring tools, trace loggers, and used his own hacking skills to help the FBI catch Kevin Mitnick, one of most wanted cyber criminals of the 1990's. Neil Barret, a professional British white hat hacker has made a living hacking into systems, sneaking

into offices, and cracking passwords all for the sake of improving security. He has helped local police and customs agents as well as the military and National Criminal Intelligence Services improve their procedures with the appropriate security tools (Schell & Dodge, 2002). Juan Cuartango, a white hat hacker from Spain, found a serious flaw in Microsoft's Internet Explorer and Windows XP Operating System that could allow an intruder to access and control any PC running Windows XP. He quickly notified Microsoft of the problem and a patch for the flaw as soon released (Delio, 2001, n.p.). Mark Wieczorek, who does not consider himself to be a white hat hacker, found a serious flaw with Barnes and Noble's on-line user account system. The flaw allowed a user to create a new account using an old e-mail address with nothing more than a new password. The new account would then display the previous user's name, order history, address and addresses where items were shipped, and last four numbers of their credit card. Like the free spirit type white hat hacker, Wieczorek contacted Barnes and Noble directly and posted the flaw on his web log making the security issue public. This eventually forced Barnes and Noble to address the issue to avoid bad publicity and serious court cases. These white hats have used their skill and in some cases have just used some common sense to explore and find the loopholes and weaknesses that they've encountered. Sometimes intrusive but more often well mannered and helpful, white-hat hackers have made real contributions toward information security.

On the corporate level, most information security programs include the use of a fault management technique known as penetration testing. Penetration testing is often done to help monitor, identify, track, and diagnose any faults within the system as well as to assess the number of vulnerabilities present. According to Michael Whitman and

Herbert Mattford's (2003) book entitled *Principles of Information Security*, penetration testing is a very important part of discovering how well the security components of the system performs: "Penetration testing involves security personnel simulating or performing specific and controlled attacks to compromise or disrupt their own systems by exploiting documented vulnerabilities. Security personnel attempt to exploit vulnerabilities in the system from the attacker's viewpoint and are commonly referred to as whitehat hackers or ethical hackers" (p. 455). The same applications used by the hacker community, which include software programs like Ethereal, Nessus, NMAP, Sam Spade, and Snort (Whitman & Mattford, 2003, p. 456), that perform numerous network port scans and provide starting points for hackers, are the same tools that the supervisors of security programs and administrators should use to secure their systems. If you want to catch a criminal, you have to be able to think like one. The basis for protection revolves around the ability to find and fix vulnerabilities before someone else makes it their business to do so. Penetration testing accompanied by the very tools used by hackers is one of the foremost indicators of how this concept of white hat hacking has made its way into the very core of system and information security.

In an article by Jim Wagner of InternetNews.com—*Giving Hackers their Due*, he reported that Robert Lyttle, a hacker who defaced a number of web pages after the Recording Industry Association of America (RIAA) began its attempt at making file sharing illegal, made some interesting and somewhat profound statements regarding how security specialists could defeat black hat hackers like himself and went further to state that most security professionals are inept:

Only a hacker can beat a hacker. An average special agent compares nowhere close to a hacker. There is no competition. Do these agents spend countless amounts of hours learning the unthinkable? Don't count on it. Sadly, the hackers in the government field who have the correct mindset aren't the ones that are leading agencies like the National Infrastructure Protection Center (NIPC), when they should be. (Wagner, 2002, np).

As revealed from the viewpoint of a real black hat, the only way to prevent and catch a malicious hacker is to use the skills of another hacker. Since hackers spend the time to write malicious code and break into systems, they are experts in this area and often know more about security than those security professionals hired to safeguard the system. Whitman & Mattford also make a similar argument from an information security perspective: "The best procedures and tools to use in penetration testing and other vulnerability assessments are the procedures and tools of the hacker community" (p. 455). The only way to catch a crook, in the words of a true black hat hacker and security specialists alike, is to use the very tools and methodologies used by your adversary.

White hat hackers have become another tool that companies can use to safeguard the technology, systems, and information that are crucial to their continued operations. Although there are many benefits to utilizing the different forms of white hat hacking services available, there are a few dangers associated with hiring and using these "ethical" hackers to secure critical systems. It is often difficult to background check the security consultants hired to "ethically" hack your system. These consultants may not be very skilled or may not possess the knowledge needed to really help you in identifying weaknesses, what to do about these weaknesses and forming the right security policy to

make sure that everything is patched and protected. Also, a major concern is the transition of power that can potentially lead to the consultants gaining more control and authority over security policy and the way the system functions. The danger is that the more you rely on outsiders to do the security work, the more likely you will eventually be owned by the security consulting group. Kleespie (2000) reports that a number of consultants feel that companies should not rely too much on outsourcing their security work. Many of the consultants also recommended considering different white hat hacking proposals before deciding to go ahead with one.

Conceptually, white hat hacking has its roots in doing something positive and ethical. White hat hackers are like hackers with a conscience. Making use of white hat hacking techniques and skill to find vulnerabilities and security weaknesses can be advantageous—have the good guys find the flaw first and then report it and get it fixed before others can exploit it. However, it becomes difficult to draw the line between the good guys and bad guys. A white hat hacker is not that much different from a black hat hacker. They are both using hacking techniques to find flaws, but the white hats are doing so to improve security. The problem is that most white hat hackers at this point are probably involved or were previously involved in some form of black hat hacking. We don't know for sure that these hackers are completely ethical and have no inclination to do something wrong.

At the intersection of information and security, it becomes important to discuss the ethical dimensions involved. The integrity of each individual hacker comes into question. The white hat or good guy notion only goes so far because we cannot completely trust anyone nor can we be 100% sure of a hacker's core belief system.

Would you be willing to leave your home to a group of “ethical” thieves who would attempt to break in, not steal or look at anything sensitive, and then report back what they were able to do and how they were able to do it? It seems like an absurd question because most people would be unwilling to let someone break into their home to find out how it could be better secured. Furthermore, we are placing a high level of trust in other people. We cannot be sure that the ethical hacker or intruder will not steal or look at anything confidential. If we promote white hat hacking and intrusion for the sake of security, then we are saying that intruding and trespassing are acceptable means of creating a secure environment as long as it leads to better practices. A great deal of emphasis is placed upon that which makes the system insecure and how far can this concept of security through finding insecurities takes us is yet to be seen.

If I were the chief security officer of a company, I would feel very uneasy about allowing a group of “ethical minded” hackers to come in and attempt to break into my system. There is no guarantee that each individual person will follow the rules, the contract or some ethical code. For instance, a security flaw may purposely be overlooked or may not be reported. Eventually, a disgruntled white hat hacker or employee may attempt to exploit the weaknesses unknown to the upper level IT personnel. In this type of situation, employing white hat hackers can lead to serious security issues and endangers the company’s ability to function all because of a single individual failing to adhere to some unwritten white hat ethical standards.

Security is something that involves many different areas and aspects. If individual users, companies, the government, or the armed forces want to secure their systems, they must know their threats, vulnerabilities, and do a risk assessment. They

must hire the right people to perform these tasks and educate their personnel on security, policy, and have training programs that are centered upon the ethical issues involved and the seriousness of security. Hiring white hat hackers is just one way of helping to ensure that your systems and information remain secure. It is a good idea to get your own people involved or do your own testing to see how secure your system really is before possibly outsourcing your security work to white hats. It would be foolish to believe that the people hired to do the hacking will have complete respect and impartiality toward the company. The danger is that the white hat hackers hired to help you can potentially have too much authority over your security policy and systems. There is a point where you are relinquishing control of security and unknowingly placing it into the hands of others who may or may not have your best interests in mind. The idea is to have some sort of balance where you remain in control of your security policy and are not completely dependant upon white hat hackers.

When we see the term “white hat hacker” on paper, it is defined as someone who attempts to use hacking methods to find security flaws and help fix them. All of this looks fine when it is put in words or written down, but the problem behind white hat hackers has to do with each individual and how obliged they feel to adhering to those unwritten ethical codes and standards that are at the very core of white hat hacking. Someone who was a hardcore black hat and decides to switch sides may not be completely trustworthy or willing to adhere to the ethical code that a white hat hacker is meant to follow. Both types of hackers utilize the same techniques but the end result of using those techniques is what is different. I can foresee how a black hat hacker might attempt to misuse what it means to be a white hat hacker so they can gain access into a

company's systems to do harm. There is a very thin line between being the good guy and bad guy here. Being the white hat hacker who remains true to the cause is the ultimate goal. A fair number of the good guys will be tempted and fall victim to doing that which they are trying to oppose. Thomas (2002), states that hackers in general have an underlying thought process that drives them: "hackers believe that your security should be comparable to the value of the information you want to protect, and leaving gaping security holes is tantamount to an invitation to enter the system" (p. 44). Douglas is reinforcing this idea that all hackers are driven by the fact that security can be compromised. Regardless of the type of hacker you are, the fact that there are holes in a system is what drives you to do what you do best—hack. What you do after you have found these vulnerabilities is what defines your character as not only a hacker, but as an individual as well.

Ubiquitous computing, the non-stop flow and exchange of information, the ongoing advancements in technology, the needs of individuals, corporations, and government bodies, and the ethical and moral issues surrounding hackers have all contributed to this idea of securing information through the use of white hat hackers. White hat hacking plays a significant role in securing the information systems that are crucial in our computer driven world. That is not to say that it does not present some ethical problems in itself but if it is used correctly, it has tremendous potential in helping to secure information. Much of its success will come down to the morals and ethics that are at the core of the individual hacker. The more ethical-minded the individual, the more trustworthy and beneficial that individual white hat hacker will prove to be. We have already seen a number of white hat hackers using their skills to help catch criminals

and prevent others with mal-intent from exploiting vulnerabilities. Corporations, government agencies, and the military have all made use of white hat hackers to help protect, secure, safeguard not only our information but our businesses and our way of living. To catch a thief, you have to be able to think like one and that is exactly what a white hat hacker is all about. If you want security, you must be able to assess your weaknesses and address them accordingly. Security is about being protected and staying free from danger requiring that we think and plan ahead. Realizing and addressing threats and vulnerabilities before the enemy finds and exploits them can prove to be crucial in the struggle to secure information. If you fail to think ahead, your opponents will exploit your weaknesses at every opportunity. As we begin to realize the increased need for security and the potential benefit of utilizing white hat hackers, there will be an ongoing information security battle taking place between a newly trained group of white hat hackers and their opposing black hat counterparts in the years to come.

References

- “Black Hat Briefings.” (n.d.) Retrieved 9 May 2005,
from <http://blackhat.com/html/bh-link/briefings.html>
- “Certified Ethical Hacking™ CEH 5-Day Boot Camp” (n.d.) Retrieved 25 April 2005,
from http://www.globalnettraining.com/certified_ethical_hacking.asp
- Delio, Michael. (2001). “IE-hole finder in Odd Position.” *Wired News Online*
Available: <http://www.wired.com/news/technology/0,1282,42798,00.html>
- Flaherty, Julie. “Enlisting the Young as White Hat Hackers.” *New York Times Online*.
2003 May 29. Available: www.nytimes.com
- Germain, Jack M. (2004) “Moral Dilemma: Hackers for Hire.” *Linux Insider News*
Online. Available: <http://linuxinsider.com/story/38256.html>
- Himanen, Pekka. (2001). *The Hacker Ethic*. New York: Random House
- Kleespie, Steven L. (2000). “The Role of ‘White Hat’ Hackers in Information Security.”
Available: <http://www.wbglinks.net/pages/reads/wbgreads/misc/whitehat.html>
- Lasker, John. (2005). “U.S. Military’s Elite Hacker Crew.” *Wired News Online*
Available: <http://www.wired.com/news/privacy/0,1848,67223,00.html>
- Schell, Bernadette H., & Dodge, John L. (2002). *The Hacking of America:
Who’s Doing it, Why and How*. Westport: Quorum Books.
- Schneier, Bruce. (2000). *Secrets & Lies*. Indianapolis: Wiley Publishing, Inc.
- Thomas, Douglas. (2002.) *Hacker Culture*. Minneapolis: University of Minnesota Press.
- Tipton, Harold F., & Krause, Micki. (Eds.). 2001. *Information Security Management*.
Boca Raton: CRC Press LLC.

“White hat hackers: Use a hacker to catch another.” Retrieved 23 April 2005 from:

http://www.dqindia.com/content/top_stories/100101410.asp

Wagner, Jim. (2002). “Giving Hackers Their Due” Retrieved 24 April 2004 from:

http://www.internetnews.com/dev-news/article.php/10_965531