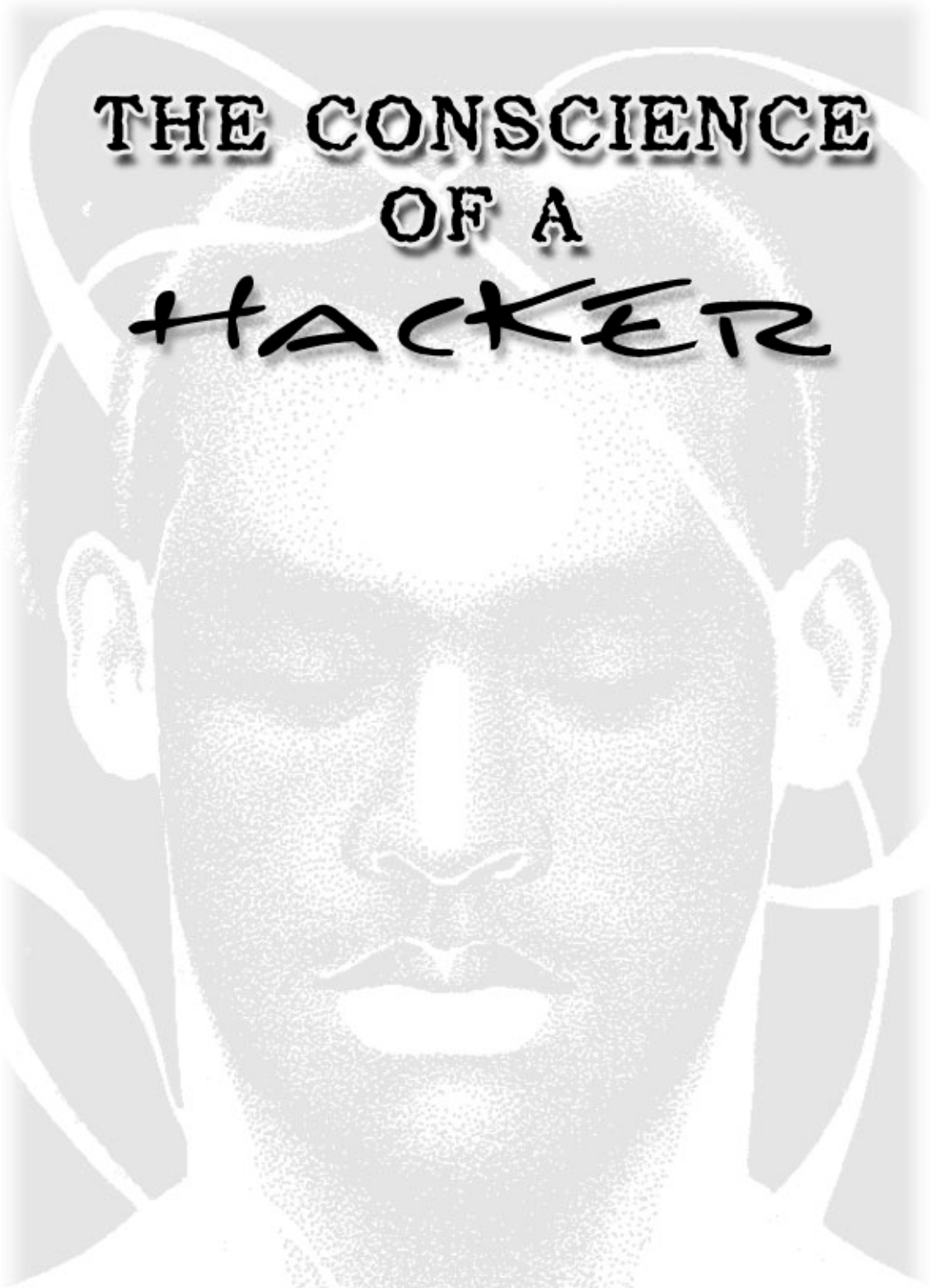


THE CONSCIENCE OF A HACKER

By: Java Boy

Abstract

A diffuse group of people called ``hackers'' has been characterized as unethical, irresponsible, and a serious danger to society for actions related to breaking into computer systems. This report makes an attempt to construct a picture of hackers, their concerns, and the discourse in which hacking takes place. This report also discusses what is behind the mind of a hacker? What makes him to hack? What motivates them? What are their morals and ethics? What do they say about computer security and privacy? My initial findings suggest that hackers are learners and explorers who want to help rather than cause damage, and who often have very high standards of behavior. My findings also suggest that the discourse surrounding hacking belongs at the very least to the gray areas between larger conflicts that we are experiencing at every level of society and business in an information age where many are not computer literate. These conflicts are between the idea that information cannot be owned and the idea that it can, and between law enforcement. Hackers have raised serious issues about values and practices in an information society. Based on my findings, I recommend that we work closely with hackers, and suggest several actions that might be taken.

“It’s about thrill, excitement and sensation”

Introduction

Another one got caught today, it's all over the papers.
"Teenager Arrested in Computer Crime Scandal", "Hacker
Arrested after Bank Tampering"...

Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's
techno brain, ever take a look behind the eyes of the hacker?
Did you ever wonder what made him tick, what forces shaped him,
what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school. I'm smarter than
most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers
explain for the fifteenth time how to reduce a fraction. I
understand it. "No, Ms. Smith, I didn't show my
work. I did it in my head."

Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer.

Wait a second, this is cool. It does what I want it to.
If it makes a mistake, it's because I screwed it up.

Not because it doesn't like me...
Or feels threatened by me...
Or thinks I'm a smart ass...
Or doesn't like teaching and shouldn't be here...

Damn kid. All he does is play games. They're all alike.

And then it happened. A door opened to a world rushing

through my phone line like heroin through an addict's veins,
an electronic pulse is sent out, a refuge from the day-to-day
incompetencies is sought... a board is found.

"This is it... this is where I belong."
I know everyone here... even if I've never met them, never
talked to them, may never hear from them again... I know you all.

Damn kid. Tying up the phone line again. They're all alike.

You bet your ass we're all alike... we've been spoon-fed baby
food at school when we hungered for steak... the bits of
meat that you did let slip through were pre-chewed and tasteless.
We've been dominated by sadists, or ignored by the apathetic.
The few that had something to teach found us willing pupils,
but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch,
the beauty of the baud. We make use of a service already existing
without paying for what could be dirt-cheap if it wasn't run by
profiteering gluttons, and you call us criminals.
We explore... and you call us criminals. We seek after knowledge...
and you call us criminals.

We exist without skin color, without nationality, without
religious bias... and you call us criminals. You build atomic
bombs, you wage wars, you murder, cheat, and lie to us and
try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is
that of judging people by what they say and think, not what
they look like. My crime is that of outsmarting you, something
that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual,
but you can't stop us all...

After all, we're all alike.

By: Mentor[1] (January 8, 1986)

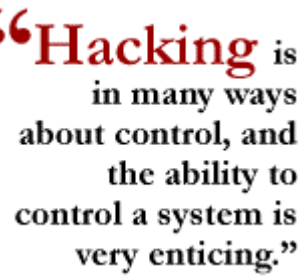
What is a hacker?

Hacker (n).

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.
3. A person who is good at programming quickly.
4. An expert at a particular program, or one who frequently does work using it or on it; as in `a Unix hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.)
5. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.
6. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.

Understanding the etymological history of the word ``hacker'' may help in understanding the current social situation.

The concept of hacking entered the computer culture at the Massachusetts Institute of Technology in the 1960s. Popular opinion at MIT posited that there are two kinds of students, tools and hackers. A ``tool'' is someone who attends class regularly, is always to be found in the library when no class is meeting, and gets straight A's. A ``hacker'' is the opposite: someone who never goes to class, who in fact sleeps all day, and who spends the night pursuing recreational activities rather than studying. There was thought to be no middle ground.



What does this have to do with computers? Originally, nothing. But there are standards for success as a hacker, just as grades form a standard for success as a tool. The true hacker can't just sit around all night; he must pursue some hobby with dedication and flair. It can be telephones, or railroads (model, real, or both), or science fiction fandom, or ham radio, or broadcast radio. It can be more than one of these. Or it can be computers. [In 1986, the word ``hacker'' is generally used among MIT students to refer not to computer hackers but to

building hackers, people who explore roofs and tunnels where they're not supposed to be.]

A ``computer hacker,'' then, is someone who lives and breathes computers, who knows all about computers, who can get a computer to do anything. Equally important, though, is the hacker's attitude. Computer programming must be a *hobby*, something done for fun, not out of a sense of duty or for the money. (It's okay to make money, but that can't be the reason for hacking.)

A hacker is an aesthete.

There are specialties within computer hacking. An algorithm hacker knows all about the best algorithm for any problem. A system hacker knows about designing and maintaining operating systems. And a ``password hacker'' knows how to find out someone else's password. That's what *Newsweek* should be calling them.

Someone who sets out to crack the security of a system for financial gain is not a hacker at all. It's not that a hacker can't be a thief, but a hacker can't be a *professional* thief. A hacker must be fundamentally an amateur, even though hackers can get paid for their expertise. A password hacker whose primary interest is in learning how the system works doesn't therefore necessarily refrain from stealing information or services, but someone whose primary interest is in stealing isn't a hacker. It's a matter of emphasis.

History of Hacking

Hacking has been around for more than a century. In the 1870s, several teenagers were flung off the country's brand new phone system by enraged authorities. Here's a peek at how busy hackers have been in the past 40 years.

Early 1960s

University facilities with huge mainframe computers, like **MIT's artificial intelligence lab,** become staging grounds for hackers. At first, "hacker" was a positive term for a person with a mastery of computers who could push programs beyond what they were designed to do.

Early 1970s

John Draper makes a long-distance call for free by blowing a precise tone into a telephone that tells the phone system to open a line. Draper discovered the whistle as a give-away in a box of children's cereal. Draper, who later earns the handle "Captain Crunch," is arrested repeatedly for phone tampering throughout the 1970s.

Yippie social movement starts *YIPL/TAP* (Youth International Party Line/Technical Assistance Program) magazine to help **phone hackers** (called "phreaks") make free long-distance calls.

Two members of California's **Homebrew Computer Club** begin making "blue boxes," devices used to hack into the phone system. The members, who adopt handles "Berkeley Blue" (Steve Jobs) and "Oak Toebark" (Steve Wozniak), later go on to found Apple Computer.

Early 1980s

Author **William Gibson** coins the term "cyberspace" in a science fiction novel called *Neuromancer*.

In one of the first arrests of hackers, the FBI busts the Milwaukee-based 414s (named after the local area code) after members are accused of **60 computer break-ins** ranging from Memorial Sloan-Kettering Cancer Center to Los Alamos National Laboratory.

Comprehensive Crime Control Act gives **Secret Service** jurisdiction over credit card and computer fraud.

Two hacker groups form, the **Legion of Doom** in the United States and the **Chaos Computer Club** in Germany.

Magazine 2600

The Hacker Quarterly is founded to share tips on phone and computer hacking.

Late 1980s

The **Computer Fraud and Abuse Act** gives more clout to federal authorities.

Computer Emergency Response Team is formed by U.S. defense agencies. Based at Carnegie Mellon University in Pittsburgh, its mission is to investigate the growing volume of attacks on computer networks.

At 25, veteran hacker **Kevin Mitnick** secretly monitors the e-mail of MCI and Digital Equipment security officials. He is convicted of damaging computers and stealing software and is sentenced to one year in prison.

First National Bank of Chicago is the victim of a **$70-million** computer heist.

An Indiana hacker known as "**Fry Guy**" -- so named for hacking McDonald's -- is raided by law enforcement. A similar sweep occurs in Atlanta for **Legion of Doom** hackers known by the handles "Prophet," "Leftist" and "Urvile."

Early 1990s

After **AT&T** long-distance service crashes on Martin Luther King Jr. Day, law enforcement starts a national crackdown on hackers. The feds nab St. Louis' "Knight Lightning" and in New York grab Masters of Deception trio "Phiber Optik," " Acid Phreak" and "Scorpion." Fellow hacker "Eric Bloodaxe" is picked up in Austin, Texas.

Operation Sundevil, a special team of Secret Service agents and members of Arizona's organized crime unit, **conducts raids** in 12 major cities, including Miami.

A 17-month search ends in the capture of hacker **Kevin Lee Poulsen** ("Dark Dante"), who is indicted for stealing military documents.

Hackers break into **Griffith Air Force Base,** then pewwwte computers at **NASA** and the **Korean Atomic Research Institute.** Scotland Yard nabs "Data Stream," a 16-year-old British teenager who curls up in the fetal position when seized.

A Texas A&M professor receives **death threats** after a hacker logs on to his computer from off-campus and sends 20,000 racist e-mail messages using his Internet address. In a highly publicized case, **Kevin Mitnick** is arrested (again), this time in Raleigh, N.C., after he is tracked down via computer by **Tsutomu Shimomura** at the San Diego Supercomputer Center.

Late 1990s

Hackers break into and deface federal Web sites**,** including the U.S. Department of Justice, U.S. Air Force, CIA, NASA and others.

Report by the General Accounting Office finds Defense Department computers sustained **250,000 attacks** by hackers in 1995 alone.

A Canadian hacker group called the Brotherhood, angry at hackers being falsely accused of electronically stalking a Canadian family, break into the Canadian Broadcasting Corp. Web site and leave message: "**The media are liars.**" Family's own 15-year-old son eventually is identified as stalking culprit.

Hackers pierce security in **Microsoft's NT operating system** to illustrate its weaknesses.

Popular Internet search engine Yahoo! is hit by hackers claiming a "**logic bomb**" will go off in the PCs of Yahoo's users on Christmas Day 1997 unless Kevin Mitnick is released from prison. "There is no virus," Yahoo! spokeswoman Diane Hunt said.

In 1998

Anti-hacker ad runs during Super Bowl XXXII. The Network Associates ad, costing $1.3-million for 30 seconds, shows two **Russian missile silo crewmen** worrying that a computer order to launch missiles may have come from a hacker. They decide to blow up the world anyway.

In January, the federal Bureau of Labor Statistics is inundated for days with hundreds of thousands of fake information requests**,** a hacker attack called "spamming."

Hackers break into **United Nation's Children Fund** Web site, threatening a "holocaust" if Kevin Mitnick is not freed.

Hackers claim to have broken into a Pentagon network and stolen software for a military satellite system. They threaten to sell the software to terrorists.

The U.S. Justice Department unveils **National Infrastructure Protection Center,** which is given a mission to protect the nation's telecommunications, technology and transportation systems from hackers.

Hacker group L0pht, in testimony before Congress, warns it could **shut down nationwide access to the Internet** in less than 30 minutes. The group urges stronger security measures.

Ecount: A hacker circumvented the Internet defenses of the Philadelphia-based company's gift certificate service and notified customers of the breach in an e-mail that included their home addresses. The hacker then demanded $45,000 from the company to keep him from exposing the personal information of 350,000 customers.

Egghead.com: A hacker infiltrated the e-tailer's system in December 2000. After three weeks of investigation, the company said the intruder did not obtain the personal information of its 3.7 million customers, but many banks said they spent millions of dollars to issue new credit cards in the meantime.

Creditcards.com: Also in December 2000, a hacker broke in to systems maintained by the company, which enables merchants to accept payments online, and made off with about 55,000 credit card numbers. The hacker tried to extort the company and, when executives refused to pay, exposed the numbers by posting them on the Web.

Western Union: In September 2000, a hacker exploited an opening in the Web site of the financial services company and got away with more than 15,000 credit card numbers. Human error left "performance management files" open on the site during routine maintenance, allowing the hacker access.

CD Universe: About 350,000 credit card numbers were stolen from the online music company in January 2000, one of the first large-scale hackings of its kind. The thief, identified only as "Maxus," held the card numbers hostage and demanded a $100,000 ransom. When the company refused, the hacker posted the numbers on a Web site.

Ethics and Aesthetics

Throughout most of the history of the human race, right and wrong were relatively easy concepts. Each person was born into a particular social role, in a particular society, and what to do in any situation was part of the traditional meaning of the role. This social destiny was backed up by the authority of church or state.

This simple view of ethics was destroyed about 200 years ago, most notably by Immanuel Kant (1724-1804). Kant is in many ways the inventor of the 20th Century. He rejected the ethical force of tradition, and created the modern idea of autonomy. Along with this radical idea, he introduced the centrality of rational thought as both the glory and the obligation of human beings. There is a paradox in Kant: Each person makes free, autonomous choices, unfettered by outside authority, and yet each person is compelled by the demands of rationality to accept Kant's ethical principle, the Categorical Imperative. This principle is based on the idea that what is ethical for an individual must be generalizable to everyone.

Modern cognitive psychology is based on Kant's ideas. Central to the functioning of the mind, most people now believe, is information processing and rational argument. Even emotions, for many psychologists, are a kind of theorem based on reasoning from data. Kohlberg's theory of moral development interprets moral weakness as cognitive weakness, the inability to understand sophisticated moral reasoning, rather than as a failure of will. Disputed questions of ethics, like abortion, are debated as if they were questions of fact, subject to rational proof.

Since Kant, many philosophers have refined his work, and many others have disagreed with it. For our purpose, understanding what a hacker is, we must consider one of the latter, Sören Kierkegaard (1813-1855). A Christian who hated the established churches, Kierkegaard accepted Kant's radical idea of personal autonomy. But he rejected Kant's conclusion that a rational person is necessarily compelled to follow ethical principles. In the book *Either-Or* he presents a dialogue between two people. One of them accepts Kant's ethical point of view. The other takes an aesthetic point of view: what's important in life is immediate experience.

> *The choice between the ethical and the aesthetic is not the choice between good and evil, it is the choice whether or not to choose in terms of good and*

> *evil. At the heart of the aesthetic way of life, as Kierkegaard characterises it, is the attempt to lose the self in the immediacy of present experience. The paradigm of aesthetic expression is the romantic lover who is immersed in his own passion. By contrast the paradigm of the ethical is marriage, a state of commitment and obligation through time, in which the present is bound by the past and to the future. Each of the two ways of life is informed by different concepts, incompatible attitudes, rival premises.* [MacIntyre, p. 39]

Kierkegaard's point is that no rational argument can convince us to follow the ethical path. That decision is a radically free choice. He is not, himself, neutral about it; he wants us to choose the ethical. But he wants us to understand that we do have a real choice to make. The basis of his own choice, of course, was Christian faith. That's why he sees a need for religious conviction even in the post-Kantian world. But the ethical choice can also be based on a secular humanist faith.

A lesson on the history of philosophy may seem out of place in a position paper by a computer scientist about a pragmatic problem. But Kierkegaard, who lived a century before the electronic computer, gave us the most profound understanding of what a hacker is. A hacker is an aesthete.

The life of a true hacker is episodic, rather than planned. Hackers create ``hacks.'' A hack can be anything from a practical joke to a brilliant new computer program. (VisiCalc was a great hack. Its imitators are not hacks.) But whatever it is, a good hack must be aesthetically perfect. If it's a joke, it must be a complete one. If you decide to turn someone's dorm room upside-down, it's not enough to epoxy the furniture to the ceiling. You must also epoxy the pieces of paper to the desk.

Steven Levy, in the book *Hackers*, talks at length about what he calls the ``hacker ethic.'' This phrase is very misleading. What he has discovered is the Hacker Aesthetic, the standards for art criticism of hacks. For example, when Richard Stallman says that information should be given out freely, his opinion is not based on a notion of property as theft, which (right or wrong) would be an ethical position. His argument is that keeping information secret is *inefficient*; it leads to unaesthetic duplication of effort.

The original hackers at MIT were mostly undergraduates, in their late teens or early twenties. The aesthetic viewpoint is quite appropriate to people of that age.

An epic tale of passionate love between 20-year-olds can be very moving. A tale of passionate love between 40-year-olds is more likely to be comic. To embrace the aesthetic life is *not* to embrace evil; hackers need not be enemies of society. They are young and immature, and should be protected for their own sake as well as ours.

In practical terms, the problem of providing moral education to hackers is the same as the problem of moral education in general. Real people are not wholly ethical or wholly aesthetic; they shift from one viewpoint to another. (They may not recognize the shifts. That's why Levy says ``ethic'' when talking about an aesthetic.) Some tasks in moral education are to raise the self-awareness of the young, to encourage their developing ethical viewpoint, and to point out gently and lovingly the situations in which their aesthetic impulses work against their ethical standards.

Computer Hacking and Ethics

> *[Neal Patrick] said he and his friends, who named themselves the ``414s'' after the Milwaukee area code, did not intend to do any damage and did not realize they were doing anything unethical or illegal. In fact, when asked [at a Congressional subcommittee hearing] at what point he questioned the ethics of his actions, he answered, ``Once the FBI knocked on the door.''*
>
> *-- "`Common Sense' Urged on Computer Break-Ins," 26 Sept 83; Copyright 1983 New York Times News Service*

It's no secret that a mature sense of ethics is something a person develops over time. Parents are supposed to exercise authority over their children because the children are not expected to know how to make certain decisions for themselves. We have a juvenile court system separate from the adult criminal court system because we believe that a young person is not *capable* of criminal intent in the same sense that an adult is capable of it.

Within this century, the obvious idea that the ethical sense of an adolescent isn't the same as that of an adult has become the focus of scientific research. Psychologists have entered a field once left to philosophers: moral development. The best-known attempt to formalize this development is probably the six-stage theory of Harvard psychologist Lawrence Kohlberg. Here is his description of Stage 3, the Interpersonal Concordance or ``Good Boy-Nice Girl'' Orientation:

> Good behavior is that which pleases or helps others and is approved by them. There is much conformity to stereotypical images of what is majority or ``natural'' behavior. Behavior is frequently judged by intention--the judgment ``he means well'' becomes important for the first time. One earns approval by being ``nice.'' [Kohlberg, p. 18]

Is Neal Patrick at this third stage of moral development? He seems to judge his own actions in terms of intention. From the perspective of the stage theory, we can see this as an improvement over ``Our mistake was to get caught'' or ``What have those computer companies done for me,'' responses that would be typical of the earlier stages.

I don't mean to give too much weight to the specifics of the third stage. It's not scientifically valid to assign Patrick to a developmental stage on the basis of one quoted sentence. Also, not every researcher accepts Kohlberg's stages. But the important point is that Patrick is *roughly* at the stage of moral development appropriate to his age. He is not some new kind of monster spawned by computer technology; he's a kid with all the strengths and weaknesses we expect from kids in other situations.

Compare a bunch of adolescents breaking into a computer system with another bunch of kids hot-wiring a car for a joyride. The latter would probably argue, with complete sincerity, that they were doing no harm, because the owner of the car recovered his property afterward. They didn't keep or sell it. It's a ``naughty'' prank to borrow someone's property in that way, but not really serious.

These hypothetical car thieves would be wrong, of course, in making that argument. They might lack the sensitivity needed to give weight to the victim's feelings of manipulation, of fear, of anger. They may not understand how the experience of such a random attack can leave a person feeling a profound loss of order and safety in the world--the feeling that leads half our population to hail Bernhard Goetz as a hero to be emulated. Some adolescents don't have the empathy to see beyond the issue of loss of property. Some may show empathy in certain situations but not in others.

“They don’t have the same morality in the virtual world as they have in the real world because they don’t think computers are part of the real world.”

The point is that the computer raises no new issue, ethical or pragmatic. The password hacker who says ``we aren't hurting anything by looking around'' is exactly analogous to the joyrider saying ``we aren't stealing the car permanently.''

(The two cases need not seem analogous to an adolescent. There may be many computer abusers who would never break into a car for a joyride, but who don't understand that breaking into a computer account raises the same ethical issues. But the analogy still holds for us as adults.)

The professional car thief and the teenaged joyrider are both social problems, but they're *different* problems. To confuse the two--to treat the teenager like a career criminal--would be a disastrously self-fulfilling prophecy.

In the context of computer systems, there is a similar dichotomy. There are some career criminals who steal by electronic means. This small group poses a large problem for society, but it's not a new one. Thieves are thieves. Just as banks use special armored cars, they must also develop special armored computer systems. But the rest of us don't use armored cars for routine transportation, and we don't need armored computer systems for routine communication either. (Of course there is a large middle ground between heavy security and no security at all. My purpose here is not to decide exactly what security measures are appropriate for any particular computer system. Instead, I just want to make it clear that, while in this paper I'm not trying to address the problem of professional criminals, I'm not trying to deny that there is such a problem either.)

There is also a middle ground between the young person who happens to break unimportant rules in the innocent exercise of intellectual curiosity and the hardened criminal. Consider the hypothetical case of a young man whose girlfriend moves to Australia for a year, and so he builds himself a blue box (a device used to place long distance telephone calls without paying for them) and uses it to chat with her for an hour every other day. This is not intellectual curiosity, nor is it a deliberate, long-term choice of a life of crime. Instead, this hypothetical adolescent, probably normally honest, has stepped over a line without really noticing it, because his mind is focused on something else. It would be inappropriate, I think, to pat him on the head and tell him how clever he is, and equally inappropriate to throw him in prison. What we must do is call his attention to the inconsistency between his activities and, most likely, his own moral standards.

Two Models for Moral Direction

What to do about it? Saying that the problems of computer ethics are like other ethical problems doesn't solve them. Many approaches are possible. We are starting to hear among computer experts the same debates we've heard for centuries among criminologists: prevention, deterrence, retribution, cure?

Among all the possible approaches, it may be instructive to consider two strongly opposed ones: first, control of the technology, and second, moral training. As examples of these approaches, compare the registration of automobiles with instruction in karate.

Automobile registration is certainly a good idea in helping the police control professional crime. As thieves have learned to steal cars for their parts, rather

than to sell whole, the technology of registration has had to grow more sophisticated: we now see serial numbers on each major component, not just on the door frame. But registration doesn't help against joyriders.

Other technological security measures can help. Steering column locks have made joyriding harder, but not impossible. Many adolescents are expert locksmiths, not because they're dishonest but because locks and keys pose a technical challenge much like that of passwords in a computer system. Also, increased security has made the consequences of juvenile car theft more serious, because the easiest way to defeat a steering column lock is to destroy it by brute force.

The example of karate instruction shows a very different approach to the problem of adolescent moral limitations. Instead of using technology to limit the power of young people, this second approach deliberately empowers them. Skill in karate is a deadly weapon; to give that weapon to a young person is an affirmation of trust rather than suspicion.

Why do karate classes for kids work? Why don't they lead to an epidemic of juvenile murders? This paper can't present a definitive answer. But I want to suggest some possibilities and use them to draw analogies for computer education.

One probable reason is that every person responds to his or her situation. If I know you're trusting me with something important, I'll try to live up to your trust. If I sense that you consider me untrustworthy, I may decide that I might as well live up to your low expectations.

Another vital reason, though, is that the technical instruction in karate techniques is part of a larger initiation into a certain culture and its rules. Karate schools don't begin by telling novices, ``Here's how to kill someone.'' They begin with simple, less dangerous techniques; the criteria for advancement include *control* and self-discipline as well as knowledge of particular moves. Instructors emphasize that karate is an art that should not be abused. Students learn to demonstrate punches and kicks without injury by stopping just short of contact with the opponent's body.

Empowerment in Computer Education

How can we *teach* young computer enthusiasts to be responsible members of the electronic community, without defining them as criminals? The analogy of karate instruction suggests that the answer is to combine ethical training with real empowerment. To turn this broad slogan into a practical program requires several changes in our approach to educational computing and to computing in general.

> Growth, like any ongoing function, requires adequate objects in the environment to meet the needs and capacities of the growing child, boy, youth, and young man, until he can better choose and make his own environment. It is not a ``psychological'' question of poor influences and bad attitudes, but an objective question of real opportunities for worthwhile experience.... Thwarted, or starved, in the important objects proper to young capacities, the boys and young men naturally find or invent deviant objects for themselves; this is the beautiful shaping power of our human nature. Their choices and inventions are rarely charming, usually stupid, and often disastrous; we cannot expect average kids to deviate with genius. [Goodman, pp. 12-13]

Paul Goodman was discussing traditional juvenile delinquents, not password hackers. But the problem is fundamentally the same. How can we provide a worthwhile culture for young computer enthusiasts to grow into?

1. Serious adult models. In karate instruction, discipline is not only for novices. The adult instructors follow the same discipline themselves. The ethical principles taught to beginners are taken seriously in the adult community. As a result, young students don't see the discipline of karate as an arbitrary imposition on them; they see it as part of what it means to be a full member of the community.

In the computer culture, adults rarely take seriously the idea of belonging to a community. The social ideal is the self-serving entrepreneur. Our heros are the ones who become millionaires by doing a slick marketing job on yet another spreadsheet program. (When my high school programming students discovered that I actually knew how to program a computer, many of them decided I was crazy. Why should anyone want to teach when he could make more money

programming?) In this context, why should any young person listen to our moral lecturing?

Fundamentally what is needed is personal action by each individual computer professional. But we can act as a society to encourage this individual commitment. We can urge our colleagues to devote part of their time to *pro bono publico* activities, like other professionals. We can give special public recognition to computer professionals who choose a life of disinterested public service over the quest for personal gain. Some corporations allow their employees paid sabbatical leave for public service work; we should encourage this policy.

2. Access to real power. Another important part of the karate analogy is that there are not two kinds of karate, one for adults and one for kids. What beginners learn may be elementary, but it's a start down the same road traveled by experts. The community into which young karate students are welcomed is the real, adult community. That's not how things work with computers. How many adult computer scientists put up with CP/M, BASIC, and floppy disks? The technology available to most young people is not a simpler version of what experts use; it's a completely separate, more arcane, fundamentally less powerful medium. That medium--the programming languages, the file storage, the editing tools, and so on--is simply inadequate to challenging intellectual work.

The community of computer professionals has come to take for granted easy access to electronic communication with colleagues anywhere in the world. Those of us lucky enough to be on the Arpanet have instantaneous communication supported by taxpayers. Even the less fortunate who communicate over dialup networks like uucp, though, have the cost of their mail supported by computing facilities other than their own; the general agreement among even competing private businesses to forward one another's mail is a remarkable example of disinterested cooperation. Some of this mail traffic is serious business. But some of it is also ``junk mail'' like sf-lovers (for science fiction enthusiasts) and human-nets. Is it surprising that young computer enthusiasts want a slice of the pie too?

Adolescents are excluded not only from access to equipment but also from access to ideas. The password hackers' preoccupation with magic words and magic numbers is harmful to *themselves* as well as to the rest of us; it's an intellectual dead end that gives them no real insight into computer science. They learn a bag of isolated tricks rather than powerful ideas that extend to solving other kinds of problems. Instead of just telling them what's forbidden, we would do better to

show them the path to our own understanding of algorithms, formal theory of computation, and so on. We all know you can't program well in BASIC; why do we allow manufacturers to inflict it on children?

To take positive steps toward this goal requires action on two fronts, access to technology and access to ideas. The latter requires training high school teachers who are themselves qualified computer programmers. In the long run, this means paying teachers salaries competitive with industry standards. That's a matter for government action. Another approach may be to promote active cooperation between university computer science departments and high schools. Perhaps college faculty and graduate students could contribute some of their time to the local high schools. (This is not a new idea; outside experts are donating time to secondary schools to help teach other areas of science. Such partnership brings its own problems, because both the goals and the techniques of college teaching are different from those of high school teaching. Still, this collaboration has sometimes been fruitful.)

The problem of access to equipment is economically more difficult, but it's getting easier. The availability of 32-bit microprocessors means that serious computational power should be affordable in the near future. Equipment manufacturers should take the high school market seriously, as an investment in future technical workers. Another approach is for interested educators to establish regional computing centers for adolescents, not part of a particular school, where kids can come on their own time. Economies of scale may allow such centers to provide state-of-the-art equipment that a single high school couldn't justify economically.

3. Apprenticeship: challenging problems and access to expertise. The karate student is given not only access to a body of knowledge, but also the personal attention of a master in the field. The instructor is responsible for the moral development of his students as well as their technical skill. He steers them in the direction of challenges appropriate to each one's progress, and his own expertise is available to help the learner.

For many years, the MIT Artificial Intelligence Laboratory ran a computer system with no passwords and no file protection at all. (It was pressure from their Defense Department funding agency, not internal needs, that forced them to implement a password scheme.) Even now, the laboratory has a liberal ``tourist'' policy: anyone can have an account, provided that someone at the laboratory is willing to be his or her mentor. The philosophy behind this policy is

that most ``malicious'' computer abuse is the result of ignorance, misunderstanding, and thoughtlessness, rather than truly malign intent. With a particular person responsible for each new user, tourists learn to share the values of the community. They are taught that the vulnerability of MIT's system is a price researchers pay willingly for the open exchange of information that that vulnerability allows. Treated as legitimate members of the community, even young tourists quickly learn to act responsibly toward the group.

Not every computer facility can be expected to share the vision of MIT-AI. Certainly the computers that control the missiles and the banking transactions should not be so open to visitors. But a typical large company has several computers, not all equally sensitive. Many could allow access to young people in their communities in the evenings, especially if some of their professional staff members are interested in serving as volunteer mentors. It's the mentor/apprentice relationship that makes all the difference. Just giving a kid an account on your machine may be asking for trouble, but making a friend of the kid is a good investment.

In particular, universities often treat their undergraduate student users like irresponsible children. Undergraduates are generally second-class citizens, with limited access to the school's computing resources, including human resources (faculty). Universities should allow undergraduates to function as true members of serious research teams, as graduate students do. This policy would provide both access to faculty mentors and challenging, useful tasks.

For secondary schools, the issue is partly one of curriculum. Too many teenagers are taught (not only in the schools but also in the magazines) that true computer expertise means knowing what number to POKE into what address in order to change the color of the screen on some brand of microcomputer. Such learning is not intellectually challenging. It does not lead to a feeling of fruitful apprenticeship.

4. A safe arena for moral experimentation. The beginning karate student might be afraid to try his or her skill with a fellow student, lest he or she injure or be injured. But it's safe to fight a match with a black belt instructor. ``I won't hurt you,'' says the instructor, ``and I won't let you hurt me.'' To allow for safe sparring between students, classes begin with half-speed motions and no body contact allowed. Later they may progress to rules that allow light body contact but no contact to the opponent's head. These rules allow students to feel safe as they experiment and develop their skills.

Young people have a similar need for safety in moral experimentation. One of the reasons for the appeal of role-playing games like Dungeons and Dragons is that a player can say ``I'm going to be a thief,'' or ``I'm going to be evil,'' trying on these roles without actually harming anyone. Similarly, a good school should be a place where students feel safe, a kind of ``ethics laboratory.''

Neal Patrick's first exposure to an ethical dilemma should not have involved the FBI. He should have confronted the issue of information privacy while using a computer system in his school. He could have learned how his antisocial acts hurt and angered the legitimate users of the system, without risking really serious trouble for himself or for anyone else. For one thing, it's hard for a young person to understand the chain of reasoning from the abstract corporate owner of a computer system to the actual human beings whose lives are affected when that system breaks down. It's easier to understand the issues when the users are one's friends and classmates, and the social effects of malicious password hacking are immediately apparent.

(None of this is meant to excuse Patrick or the other 414s. Neither ignorance of the law nor misunderstanding the ethical issues is accepted in our culture as an excuse for lawbreaking. But I am not writing for a court of law meeting to settle Patrick's guilt or innocence. The question for us is how, as a society, we can act to make the next generation of teenagers less likely to paint themselves into this particular corner.)

As a practical matter, what's needed to build an ethics laboratory for computing students has already been recommended in another context: adequate computing power to support a user community, as opposed to a bunch of isolated, independent microcomputer users. Whether this means timesharing or a network of personal computers with a shared file server is a technical question beyond the scope of this paper. But sharing is essential. The ethical issues of a living community don't arise in the context of isolated individuals using microcomputers separately with no communication among them. (If we do not fill this need, we leave a void that in practice is filled by ``pirate'' bulletin boards that build a sort of outlaw community around illegal computing activities.)

What Is Hacktivism?

Hacktivism is the fusion of hacking and activism; a merger in which technically proficient hackers engage in electronic direct action in order to bring pressure on institutions engaged in unethical or criminal actions, particularly in relation to the Internet and computer technology. Hacktivism is the expression of hacker skills in the form of electronic direct action. Neither the tactics nor the objectives of hacktivism are static. Rather, hacktivism is a continually evolving recombinant and open form of activism/protest combined with a willingness to creatively solve the problem being addressed.

Background:

Since hacktivism is a recombinant initiative comprised of two divergent communities (hackers and activists) it is necessary to understand their respective backgrounds in order to analyze this historic merger and to examine its challenges and future capabilities. This may explain how hacktivism may or may not overcome both "hacker intolerance for the technologically impaired, and activist intolerance for those who are not politically correct" in order to become a secure network operating for social and political change worldwide.

Tenets of Hackers:

The hacker ethic formulated by Steven Levy in his 1984 book "Hackers: Heroes of the Computer Revolution" outlines the hacker tenets:

1. Access to computers should be unlimited and total.
2. All information should be free.
3. Mistrust authority - promote decentralization.
4. Hackers should be judged by their hacking not bogus criteria such as degrees, age, race, or position.
5. You create art and beauty on a computer.
6. Computers can change your life for the better.

These principles combined with technological skill have endowed hackers with the capability to create solutions and solve problems in a truly amazing way. Eric Raymond explains the successes and technological advancements created by hackers, creative solutions that benefit society:

> *"There is a community, a shared culture, of expert programmers and networking wizards that traces its history back through decades to the first time-sharing minicomputers and the earliest ARPAnet experiments. The members of this culture originated the term `hacker'. Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers run Usenet. Hackers make the World Wide Web work. If you are part of this culture, if you have contributed to it and other people in it know who you are and call you a hacker, you're a hacker."*

However, these developments coincided with the practice of "short-cuts" that extended to the use of unauthorized computer access. Bruce Sterling suggests that "Some off-the-cuff experience at computer intrusion was to be in the informal resume of most "hackers" and many future industry giants." Indeed a culture of computer intrusion developed along side the understanding that such intrusions would not involve malicious damage to the affected systems.

The anti-authoritarian and anti-bureaucratic sentiments have led hackers to believe that information should be freely accessible. Moreover, hackers abhor censorship especially when it is combined with mistrust of restrictive legislation that encroaches on free access to information and cherished electronic privacy. Thus a natural aversion to restrictive governments and predatory private institutions has developed. In Phrack magazine Dr. Crash explains that computer technology is being misused not by hackers but by governments and corporations:

> *"The wonderful device meant to enrich life has become a weapon which dehumanizes people. To the government and large businesses, people are no more than disk space, and the government doesn't use computers to arrange aid for the poor, but to control nuclear death weapons."*

This sentiment is not an isolated rant. There is definitely a trend within hacker culture that not only focuses on technical aspects of computing but political aspects as well. In the "Hacker's Manifesto" the ment0r explains:

> *We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals.*

You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Whereas “In the 1960s, definitions of 'property' and 'privacy' had not yet been extended to cyberspace” the information economy of the 1990's has thrust hackers into an environment where cyberspace is increasingly becoming “privately-owned unreal-estate” subject to severe restrictions. Hackers faced serious questions and allegations of criminal behavior regarding computer intrusions. In fact, both the word “hacker” and hackers themselves have become nearly synonymous with computer criminality - however misguided it may be. As a result, there is now an array of words intended to highlight the difference between hackers and computer criminals. Persons who use hacker technology with the primary purpose of breaking into secured systems are known as “crackers”. But, Bruce Sterling explains that there is still plenty of confusion surrounded the term because “'hacker' is what computer intruders choose to call themselves.” The hacker\cracker debate aside, there has been antagonism between government\corporate restrictions and domination of computer technology and the hackers who want to ensure free access to information and prevent monopoly control and censorship of that technology.

Activists:

The integration of activism and computer\Internet technology has been easily accomplished. The new technology plays a complementary and beneficial role and seems to fit perfectly with existing activist networks. In fact, “Many non-governmental groups now depend on the Web and e-mail to motivate, activate and communicate their uncensored messages.” From its inception the Internet, and its predecessor ARPANET were designed to facilitate communications transfers. Although its initial function was linked to the military Bruce Sterling explains, “ARPANET's users had warped the computer-sharing network into a dedicated, high-speed, federally subsidized electronic post-office.” The dominant network traffic was “news and personal messages” and there was a proliferation of newsgroups. “There are no official censors, no bosses, no board of directors, no stockholders” and it is not unimaginable why activists saw this as a golden opportunity. Stephen Wray points out “The origins of computerized activism extend back in pre-Web history to the mid 1980s.” Wray notes that the creation of PeaceNet, a text-based newsgroup service, in 1986 allowed “political activists to communicate with one another across international borders with relative ease and speed.”

As the growth of the Internet skyrocketed in the early 1990s technology, such as the graphical web browser was developed in order to allow the less technically proficient access to the Internet. This has allowed activists with little or no technical skills to utilise the benefits of digital communications. With the previous methods “telephone, fax or mail it was prohibitively expensive to share information or build links between different organizations.” (The Economist Dec 11 1999 p 21). The organizational component revolves primarily around the use of email, which is essentially free. Email, and now instant messaging systems, allow for speedy interaction and exchange of information. The BBS (Bulletin Board System) and real time chat also allow for online debates and discussions in which relevant data can be hyper-linked and accessed by the participants in no time at all. The convergence of meetings, debates, and research in one convenient and fast medium greatly enhances not only the organizational capabilities but also the ability of non-violent activists to react to a constantly changing world in a timely manner. In order to educate the public and promote causes and campaigns activist organizations have adopted the use of the web page. This allows the group to have an accessible, updateable, interactive, and international presence that was previously difficult if not nearly impossible to maintain.

Hacktivism is the fusion of the evolution of computer activism with the politicization of the hackers. The evolutionary progress of both communities has put them in a position where they can compliment each other because they increasingly face the same institutions. The fusion has emboldened each community and provides a conduit for electronic activism. Oxblood Ruffin of the cDc[2] explains:

> *Hacktivism forges conscience with technology and girds us against the disagreeable nature of conflict. It allows us to mount better arguments, rally unseen allies, and take on any tyranny.*

The methodology of hacktivism is being developed and thus subject to change. Hacktivism could be as simple as posting banned or censored material on the Internet. However, the media rarely reports such events and hacktivists have taken to “bending” the law in order to attract attention to particular causes. Indeed, there is a strong relationship between hacktivism and civil disobedience since both thrive on the edge of legality - some would indeed say illegality. This dichotomy is well articulated by CountZero of L0pht & cDc:

> *"Hacktivism" is the evolution of activism in a wired, global community. Using hacking "techniques" to achieve activist goals. And like "real*

world" activism, sometimes "hacktivism" involves breaking the law.....spraypainting slogans on a public wall vs. altering a website...both are the same level, in my mind. Also, what some people call "hacktivism" is, in my mind, really "information warfare." InfoWar is about nuking your enemy..stifling their expression...and that's something that "hacktivism" definitely is NOT.

The debate surrounding the tactics of hacktivism (especially in the media) have focused on web site defacements. (In addition to attrition.org's defaced web page mirror there is a website (http://www.freespeech.orgesistance) that catalogues politically motivated defacements.) Additionally, the use of email bombs, viruses, worms, and denial of service methods have been included by some as hacktivist tactics.

The actualization of politicized hacking continues to occur primarily in the form of web site defacement - although this would more properly be labelled as “cracking” since it involves illegal computer access and the alteration of data. While there is major objection to and contestation of the motivation and methodology of such activities some major events are:

- X-Ploit hacked Mexico's finance ministry Website, replacing it with the face of revolutionary hero Emiliano Zapata, in sympathy with the Zapatista rebellion in the Chiapas region in southern Mexico.
- The Portuguese group Kaotik Team hacked 45 Indonesian government Websites, altering Web pages to include messages calling for full autonomy for East Timor.
- The New York Times had its Website replaced with a long screed calling for the release of jailed hacker Kevin Mitnick
- Political activists took over an Indian government Website and posted messages and photos calling attention to alleged government-sponsored repression and human rights violations in the contested northern Indian state of Kashmir.
- Nike.com was "hijacked" and visitors were redirected to an Australian labour rights site.
- Milw0rm hacked the Web site of India's Bhabha Atomic Research Center (BARC) to protest nuclear weapons testing.

These are some of the often quoted and publicized cases cited as examples of hacktivism. Since unauthorized access can be sensationalized cases like these seem to be prominent in the media.

Hacktivism gives expression to electronic civil disobedience through the capability to actualize both blockade and trespass, conducted in a manner that reflects traditional street based civil disobedience. There have been two major electronic civil disobedience campaigns organized on the basis of denial of service techniques along with mass public participation. They are the FloodNet campaign by the Electronic Disturbance Theatre and the "virtual sit-in" organized by the electrohippies to coincide with street based demonstrations occurring in Seattle at against the World Trade Organization meeting.

Critiques of Hacktivism:

Some veteran hackers believe that hacktivism just provides "more ammunition for anti-hacker hysterics to demand get-tough measures, with little to show for the sacrifice." Brian Martin of Attrition.org is quoted as saying, "Do these kids think that by defacing some Web sites, it's going to make the country change? I understand what they are doing, but they are deluding themselves if they think it is going to help." Indeed, "Most infiltration into cyberspace has either been playful vandalism, politically misguided espionage, or personal revenge against a particular source of authority." Furthermore many hackers denounce the denial of service strategy used in ECD campaigns and suggest better strategies. Oxblood Ruffin argues "One does not make a better point in a public forum by shouting down one's opponent." The debate surrounding hacktivism is quite vibrant and diverse.

From the activist perspective, hacktivists are considered to be "shadowy" and acting from behind the cover of anonminity. Some feel that it actually detracts from the activists cause. For example, when kkk.com was domain-jacked and visitors were redirected to HateWatch.org the director of HateWatch David Goldman objected, "This type of action, hacktivism, is not only [against] the First Amendment [of US law] but it also takes away one of the greatest civil rights tools we have -- using the words of bigots against them".

In contrast others have spoken out on behalf of tactics such as web page defacement. Alex Fowler of the Electronic Frontier Foundation is quoted as saying, "Graffiti is about a space for the disenfranchised to cry out and inform those around them, even when anonymity has been forced upon them" in

seemingly direct support of such tactics. Others, such as ZDNet's Kevin Poulsen distinguish between vandalism and hacktivism:

> *"Vandalism is malicious destruction or damage, not artful and subversive tampering. The proof for protest is in the quality of the work, the clarity of the message, and the motives behind it."*

The discussion and critiques of hacktivism abound, but that is one of its strengths rather than a weakness. By widening the range of debate and possibilities the impossible becomes possible and solutions are created. This recombinant concept, hacktivism, is being defined and redefined and practice and theory evolve with actualization.

Hacktivism vs. Activism

Hacktivism is not strictly the importation of activist techniques into the digital realm. Rather it is the expression of hacker skills in the form of electronic direct action. It acknowledges that neither the tactics nor the objectives of hacktivism are static. Rather, they must continually evolve in order to be effective. Thus a distinction is made between hackers engaged in activism and activists attempting utilize the technical aspects of hacking to mimic and rationalize traditional forms of activism. This sentiment is summed up by Oxblood Ruffin of the cDc:

> *"Hacktivism is about using more eloquent arguments - whether of code or words - to construct a more perfect system. One does not become a hacktivist merely by inserting an "h" in front of the word activist or by looking backward to paradigms associated with industrial organization."*

Disruption (whether by computer break-ins on denial of service), in this regard, is no longer a viable option. Instead, it is argued that the focus of hacktivism should be shifted from electronic disruption to problem solution. Oxblood Ruffin explains:

> *"Hacktivism is an open-source implosion. It takes the best of hacking culture, and the imperatives of the quantum community, and fuses a solution."*

Indeed, the evolution of technology and the development of political theory have clearly shown that effectiveness requires the ability to look to the future. To

remain confined in the comfortable static bunkers is to renounce the ability to adapt for the better. That is, through creative thinking, practical solutions and applications, new and possibly more effective methods of Hacktivism can be developed.

An example the actualization of this line of thought is the work of the Cult of the Dead cow and the Hong Kong Blondes in trying to assist democracy activists in China. In addition the cDc is organizing a project called hacktivismo. "The specifics are still secret, but the group will reportedly write applications to defeat government content filters in totalitarian countries." A solution-oriented project like this will require a lot of time an effort but hacktivismo organizer Oxblood Ruffin assures that "hackers have a lot of stamina for harsh bug fixes when they believe in the program."

The Future:

Although in its relative infancy, hacktivism has emerged as a vibrant, new mechanism to achieve social and political change, specifically by applying pressure to institutions engaged in unethical or criminal behavior and by drawing attention to specific cause and thus widening the range of debate surrounding relevant issues. However, in order to reach a higher level of effectiveness the bugs must be worked out of both hacktivist theory and methodology. This needs to be done in an open manner in which criticism is positive and constructive not malicious and destructive. Furthermore, the debate needs to extend beyond legitimization and protest but to focusing on problem solving through creative and critical thinking. Through this process, perhaps, the hacker\activist schism can be overcome thus creating a secure a stable hacktivist network.

Interview with GForce Pakistan

India Cracked[12] had an email-based interview with **GForce Pakistan**, well-known hacker group from Pakistan. Below are the answers that **"Heataz"** the co-founder of GForce Pakistan provided on behalf of GForce Pakistan.

*** When did you form the GForce Pakistan group? How many members are there in the group?**

GFP: There are currently eight members of GForce Pakistan. It was formed shortly after the Nuclear Explosions by India & Pakistan, which resulted in instability in the Kashmir region and led to many false stories created by the Indians and being spread by their media. To raise public awareness about the truth in Kashmir, we got together and created GForce Pakistan.

*** What does the word "GForce" mean? Are you are from Pakistan?**

GFP: Actually, to be honest I have no clue what the word means. It's just a word. Like aircraft-related high alpha maneuvers or something. Sounds cool. Yes, most of the members are from Pakistan.

*** In real life, what are your professions?**

GFP: Most of us are students, some of us have pursued jobs in the IT industry.

*** What is your favourite music group?**

GFP: I personally prefer Slipknot and KoRn, but I don't think the other guys will agree with me :-)

*** Where do you guys hang around online?**

GFP: Well, we're mostly on irc.ssc.net, which is a nice, fast, and secure network unlike undernet/efnet. The channel is, of course, secret :-)

*** Why do you deface website? Is it for the fun/excitement of it, or for political reasons or combination of both?**

GFP: We deface websites for a cause, which is for the good of our Muslim brothers. INNOCENT PEOPLE are being killed in Kashmir & Palestine by Indians and Israelis. No one is doing anything to stop them. We try and raise public awareness about them.

*** You said that "To raise public awareness about the truth in Kashmir" you all created GForce Pakistan. At this point of time, do you think GForce has been successful? Is yes, how/why do you think so?**

GFP: Yes, to a certain extent we have succeeded in raising awareness about the Kashmir issue. Though it has not influenced any political decisions yet. The cease-fire in Kashmir right hopefully enough to prevent people from dying. But there is no such cease-fire in Palestine, and people are still being killed there as I write this.

*** Which OS do you think is more vulnerable to break in? Why do you think this is so?**

GFP: Windows NT is the most vulnerable operating system ever created by mankind. It's default install is probably one of the most vulnerable ones in history, and it is not open sourced, so we have to depend on the coders at Microsoft to audit their code for vulnerabilities (which they don't).

*** Do you code your own exploits or do you use scripts/codes available on the web?**

GFP: We code our own exploits for vulnerabilities already found by other people on the internet and discussed in public forums. We do not find vulnerabilities in software on our own.

*** Do you help webmaster/admins fix their holes if they ask for your advice/help?**

GFP: Well, not many admins have asked for our help, but those who have, have been helped by us in every way possible to give them advice on how to secure their systems.

*** Are the break-ins group's work or individual effort?**

GFP: Most of the time it is an individual effort, though group break-ins are

usually used on extremely high profile sites that have good security.

*** Do you just replace the index page when you deface or do you do further damage like get emails/delete files etc.?**

GFP: We ONLY change the website of the servers we break into. We do not damage any other part of the system in any way.

*** Which break-in of yours, if any, did you find the most challenging?**

GFP: Well, we really liked the **http://www.setindia.com/** defacemement, as it was a very high profile Indian site (it was the site of their leading TV Network). They were initially running Windows NT which was WAY to easy to break into, but later on they switched to Linux and it pretty challenging to break into it again...but eventually we did.

*** Has there been a brush with the law enforcement agencies so far?**

GFP: Nope ;-)

*** Which are the sites that you visit to keep yourself updated on security issues?**

GFP: Some of the good sites are:

www.securityfocus.com
www.securityfocus.com/bugtraq/archive
www.technotronic.com
www.slashdot.org
www.freshmeat.net
www.linuxsecurity.com
www.whitehats.com
www.cert.org
packetstorm.securify.com

Public Image and Treatment

Hackers express concern about their negative public image and identity. As noted earlier, hackers are often portrayed as being irresponsible and immoral. One hacker said that ``government propaganda is spreading an image of our being at best, sub-human, depraved, criminally inclined, morally corrupt, low life. We need to prove that the activities that we are accused of (crashing systems, interfering with life support equipment, robbing banks, and jamming 911 lines) are as morally abhorrent to us as they are to the general public."

The public identity of an individual or group is generated in part by the actions of the group interacting with the standards of the community observing those actions. What then accounts for the difference between the hacker's public image and what they say about themselves? One explanation may be the different standards. Outside the hacking community, the simple act of breaking into systems is regarded as unethical by many. The use of pejorative words like ``vandal" and ``varmint" reflect this discrepancy in ethics. Even the word ``criminal" carries with it connotations of someone evil; hackers say they are not criminal in this sense. Katie Hafner notes that Robert Morris, who was convicted of launching the Internet worm, was likened to a terrorist even though the worm did not destroy data.

Distortions of events and references to potential threats also create an image of persons who are dangerous. Regarding the 911 incident where a hacker downloaded a file from Bell South, Goldstein reported ``Quickly, headlines screamed that hackers had broken into the 911 system and were interfering with emergency telephone calls to the police. One newspaper report said there were no indications that anyone had died or been injured as a result of the intrusions. What a relief. Too bad it wasn't true." In fact, the hackers involved with the 911 text file had not broken into the 911 system. The dollar losses attributed to hacking incidents also are often highly inflated.

Thomas and Meyer say that the rhetoric depicting hackers as a dangerous evil contributes to a ``witch hunt" mentality, wherein a group is first labeled as dangerous, and then enforcement agents are mobilized to exorcise the alleged social evil. They see the current sweeps against hackers as part of a reaction to a broader fear of change, rather than to the actual crimes committed.

Hackers say they are particularly concerned that computer security professionals and system managers do not appear to understand hackers or be interested in their concerns. Hackers say that system managers treat them like enemies and criminals, rather than as potential helpers in their task of making their systems secure. This may reflect managers' fears about hackers, as well as their responsibilities to protect the information on their systems. Stallman says that the strangers he encounters using his account are more likely to have a chip on their shoulder than in the past; he attributes this to a harsh enforcer mentality adopted by the establishment. He says that network system managers start out with too little trust and a hostile attitude toward strangers that few of the strangers deserve. One hacker said that system managers show a lack of openness to those who want to learn.

Stallman also says that the laws make the hacker scared to communicate with anyone even slightly ``official,'' because that person might try to track the hacker down and have him or her arrested. Drake raised the issue of whether the laws could differentiate between malicious and non-malicious hacking, in support of a ``kinder, gentler'' relationship between hackers and computer security people. In fact, many states such as California initially passed computer crime laws that excluded malicious hacking; it was only later that these laws were amended to include non-malicious actions. Hollinger and Lanza-Kaduce speculate that these amendments and other new laws were catalyzed mainly by media events, especially the reports on the ``414 hackers'' and the movie ``War Games,'' which created a perception of hacking as extremely dangerous, even if that perception was not based on facts.

Hackers say they want to help system managers make their systems more secure. They would like managers to recognize and use their knowledge about design flaws and the outsider threat problem. Landreth suggests ways in which system managers can approach hackers in order to turn them into colleagues, and Goodfellow also suggests befriending hackers. John Draper (Cap'n Crunch) says it would help if system managers and the operators of phone companies and switches could cooperate in tracing a hacker without bringing in law enforcement authorities.

Drake suggests giving hackers free access in exchange for helping with security, a suggestion that I also heard from several hackers. Drake says that the current attitude of treating hackers as enemies is not very conducive to a solution, and by belittling them, we only cause ourselves problems.

Some of the hackers have been asked whether they'd be interested in breaking into systems if the rules of the ``game'' were changed so that instead of being threatened by prosecution, they were invited to leave a ``calling card'' giving their name, phone number, and method of breaking in. In exchange, they would get recognition and points for each vulnerability they discovered. Most were interested in playing; one hacker said he would prefer monetary reward since he was supporting himself. Any system manager interested in trying this out could post a welcome message inviting hackers to leave their cards. This approach could have the advantage of not only letting the hackers contribute to the security of the system, but of allowing the managers to quickly recognize the potentially malicious hackers, since they are unlikely to leave their cards. Perhaps if hackers are given the opportunity to make contributions outside the underground, this will dampen their desire to pursue illegal activities. Several hackers said that they would like to be able to pursue their activities legally and for income. They like breaking into systems, doing research on computer security, and figuring out how to protect against vulnerabilities. They say they would like to be in a position where they have permission to hack systems. Goodfellow suggests hiring hackers to work on tiger teams that are commissioned to locate vulnerabilities in systems through penetration testing. Baird Info-Systems Safeguards, Inc., a security-consulting firm, reports that they have employed hackers on several assignments. They say the hackers did not violate their trust or the trust of their clients, and performed in an outstanding manner. Baird believes that employing people who have exploited systems can better identify system vulnerabilities.

One hacker suggested setting up a clearinghouse that would match hackers with companies that could use their expertise, while maintaining anonymity of the hackers and ensuring confidentiality of all records. Another hacker, in describing an incident where he discovered a privileged account without a password, said ``What I (and others) wish for is a way that hackers can give information like this to a responsible source, AND HAVE HACKERS GIVEN CREDIT FOR HELPING! As it is, if someone told them that `I'm a hacker, and I REALLY think you should know...' they would freak out, and run screaming to the SS [Secret Service] or the FBI. Eventually, the person who found it would be caught, and hauled away on some crazy charge. If they could only just ACCEPT that the hacker was trying to help!'' The clearinghouse could also provide this type of service.

Hackers are also interested in security policy issues. Drake expressed concern over how we handle information about computer security vulnerabilities. He

argues that it is better to make this information public than cover it up and pretend that it does not exist, and cites the CERT to illustrate how this approach can be workable. Other hackers, however, argue for restricting initial dissemination of flaws to customers and users. Drake also expressed concern about the role of the government, particularly the military, in cryptography. He argues that NSA's opinion on a cryptographic standard should be taken with a large grain of salt because of their code breaking role.

Some security specialists are opposed to hiring hackers for security work, and Eugene Spafford has urged people not to do business with any company that hires a convicted hacker to work in the security area. He says that ``This is like having a known arsonist install a fire alarm.'' But, the laws are such that a person can be convicted for having done nothing other than break into a system; no serious damage (i.e., no ``computer arson'') is necessary. Many of our colleagues admit to having broken into systems in the past, e.g., Geoff Goodfellow and Brian Reid; Reid is quoted as saying that because of the knowledge he gained breaking into systems as a kid, he was frequently called in to help catch people who break in. Spafford says that times have changed, and that this method of entering the field is no longer socially acceptable, and fails to provide adequate training in computer science and computer engineering. However, from what I have observed, many hackers do have considerable knowledge about telecommunications, data security, operating systems, programming languages, networks, and cryptography. But, I am not challenging a policy to hire competent people of sound character. Rather, I am challenging a strict policy that uses economic pressure to close a field of activity to all persons convicted of breaking into systems. It is enough that a company is responsible for the behavior of its employees. Each hacker can be considered for employment based on his or her own competency and character.

Some people have called for stricter penalties for hackers, including prison terms, in order to send a strong deterrent message to hackers. John Draper, who was incarcerated for his activities in the 1970's, argues that in practice this will only make the problem worse. He told that he was forced under threat to teach other inmates his knowledge of communications systems. He believes that prison sentences will serve only to spread hacker's knowledge to career criminals. He said criminals outside the prison never approached him, but that inside the prison they had control over him.

One hacker said that by clamping down on the hobbyist underground, we will only be left with the criminal underground. He said that without hackers to uncover system vulnerabilities, the holes will be left undiscovered, to be utilized by those likely to cause real damage.

Goldstein argues that the existing penalties are already way out of proportion to the acts committed, and that the reason is because of computers. He says that if Kevin Mitnick had committed crimes similar to those he committed but without a computer, he would have been classified as a mischief-maker and maybe fined $100 for trespassing; instead, he was put in jail without bail. Craig Neidorf, a publisher and editor of the electronic newsletter ``Phrack,'' faces up to 31 years and a fine of $122,000 for receiving, editing, and transmitting the downloaded text file on the 911 system.

Conclusion

Hackers say that it is our social responsibility to share information, and that it is information hoarding and disinformation that are the crimes. This ethic of resource and information sharing contrasts sharply with computer security policies that are based on authorization and ``need to know.'' This discrepancy raises an interesting question: Does the hacker ethic reflect a growing force in society that stands for greater sharing of resources and information -- a reaffirmation of basic values in our constitution and laws? It is important that we examine the differences between the standards of hackers, systems managers, users, and the public. These differences may represent breakdowns in current practices, and may present new opportunities to design better policies and mechanisms for making computer resources and information more widely available.

The sentiment for greater information sharing is not restricted to hackers. In the best seller ``Thriving on Chaos,'' Tom Peters writes about sharing within organizations: ``Information hoarding, especially by politically motivated, power seeking staffs, has been commonplace throughout IT industry, service and manufacturing alike. It will be an impossible millstone around the neck of tomorrow's organizations. Sharing is a must.'' Peters argues that information flow and sharing is fundamental to innovation and competitiveness. On a broader scale, Peter Drucker says that the ``control of information by government is no longer possible. Indeed, information is now transnational. Like money, it has no `fatherland.' ''

Nor is the sentiment restricted to people outside the computer security field. Harry DeMaio says that our natural urge is to share information, and that we are suspicious of organizations and individuals who are secretive. He says that information is exchanged out of ``want to know'' and mutual accommodation rather than ``need to know.'' If this is so, then some of our security policies are out of step with the way people work. Peter Denning says that information sharing will be widespread in the emerging worldwide networks of computers and that we need to focus on ``immune systems'' that protect against mistakes in our designs and recover from damage.

I began my investigation of hackers with the question: who are they and what is their culture and discourse? My investigation uncovered some of their concerns, which provided the organizational structure to this report, and several

suggestions for new actions that might be taken. My investigation also opened up a broader question: What are the clashing discourses that the hackers stand at the battle lines of? Is it owning or restricting information vs. sharing information -- a tension between an age-old tradition of controlling information as property and the Enlightenment tradition of sharing and disseminating information? Is it controlling access based on ``need to know,'' as determined by the information provider, vs. ``want to know,'' as determined by the person desiring access? The answers to these questions, as well as those raised by Barlow on the nature of information and free speech, are important because they tell us whether our policies and practices serve us as well as they might. The issue is not simply hackers vs. system managers or law enforcers; it is a much larger question about values and practices in an information society. But the things to remember from the hackers point of view is the difference between a hacker and a Cracker, for most of us the word cracker doesn't have to do anything with the word hackers. Hackers are the builder, the innovators and in my opinion they deserve the credit because of their tireless efforts for making the seem to be a dream digital into a real digital world a world. They don't hack websites just because of some credit card numbers; these kind of acts only belong to the cracker family. So we should remember that crackers are not hackers. Hackers only want that information should be freely available because:

> *"Information is the key to success, power and wealth. Success leads to wealth which gives you the power to hold the information which is vital".*

-Sign off-

Text References

[1]	A well-known hacker of 80’s, he wrote these words in jail after FBI caught him for bank tampering.
[2]	Hacker group Cult of the Dead Cow (cDC), they are the creator of deadly Trojan “Back Orfice”.

Internet Sites

[3]	http://www.zone-h.org
[4]	http://www.hacktivism.com
[5]	http://www.phrack.org
[6]	http://www.indiacracked.com
[7]	http://www.attrition.org
[8]	http://www.hackersdigest.com