William A Hawkes-Robinson
5 June 2007

Today’s Hacker Culture, Developing Innovators or Criminals?

Audience: Anyone interested in privacy, security, civil rights, or hacker culture.

The term hacker has changed considerably since its inception in the 1960’s and 1970’s. Hackers were once considered by many in the scientific community as heroes, but since the late 1970’s and early 1980’s onward, have continued to be synonymous with cracker, computer criminal or anarchist, and more recently even terrorist. Hacker culture varies broadly in many areas from demographics to goals, but has a number of common themes. Many argue that all hackers should be locked up and the key thrown away. Corporations, governments and citizens have had an increasing misunderstanding based on ignorance about hackers that has led to an escalation of fear and increasingly, the abuse of human rights that is gaining a dangerous momentum.

In the 1950’s, 60’s and 70’s, the terms “hacker” and “hacking” had considerably different meanings than today’s popular use of the term. Hacking originally had two different applications of the term, but with over-arching similar meanings. One definition was hacking at software code. That is the process of revising the computer language for a program, over and over to get it to become the most efficient in speed, memory allocation, function and clarity. In the days of early computing, even mainframes such as the Digital PDP’s, had very limited memory available to run programs, so even one line of inefficient programming code had a significant impact on the utility of the programs execution. The other definition of the term had a broader usage, that of modifying existing technology to meet functions other than originally intended. This would include modifying computer hardware, model railroads, solid-state electronics such as appliances, and generally innovating and inventing.

Technology “heroes” such as Steve Wozniak “The Woz” (creator of the Apple computer system), Steve Jobs (founder of the company Apple), and Bill Gates (founder of Microsoft) just to name a few, were considered hackers in those days. These “Heroes of the Computer Revolution” (Hackers, Levy) were mostly college students or graduates (or in the case of Bill Gates a Harvard drop out) such as MIT (Massachusetts Institute of Technology), U of Ca Berkeley, Harvard, Princeton, etc. Though many came from diverse backgrounds, personalities and interests initially, they were united by their love of technology and innovation. Some originally met because of joining hobby groups such as “Tech Model Railroad Club” (Hackers, Levy). They usually met in person, face to face with close relationships built between them, some to become lifelong friendships, others to become if not outright enemies, at least strongly competitive arch rivals such as Steve Jobs and Bill Gates.

Today’s so-called “Hackers” are of a very different breed and means of interaction. There are several types in today’s hacker culture. There are still many of the well educated – some more informally educated than others – scientists in the culture from the old days and some new blood, but other groups have since developed and incurred some of the cliché’s that layman now associate with the term “hacker”. Within the Hacker community they have developed many subtitles such as script kiddies, white hats, gray hats, and the notorious black hats. A new label has been added in recent years by the government and media, that of the “cyber terrorist”.

Scripts kiddies are actually what most people associate with hacking. That is the anti-social pencil-necked pimply-faced, usually male, juvenile “geek”. Script kiddies do not actually have much in the way of talent or knowledge. They simply run programs that others have written, without really having a clue as to how they work and why.

The “Red Button” program is such an example of a simple program that pops up with a text field for the user to enter the address of a computer or website you want to attack, something like http://www.ebay.com. The user then just clicks the big red button. At this point everything runs in automatic to take over computers and then attack the target site. The script kiddie has no idea how it really works, but they think they are very “cool” when they cause a temporary disruption of service for a website. They tend to be very obvious and brag a lot about their mostly imaginary hacking successes. This is now the majority of so-called hackers. Most true hackers do not consider script kiddies to be in the same league, and look down on them with disdain. Many frequently manipulate the “kiddies” fragile egos to perform deeds for the more experienced and actually talented hackers, especially the black hats. Recognition, public ego-stroking and “ranking” in the hacker culture are the main goals for the “script kiddie” individuals.

Enter the Black Hat. Black hats are the ones with the help of the typically misguided and misinformed public media, who have given hacking the bad name it now has. These people are nothing more than criminals. Some are brighter than others, but almost all have an all-consuming need for power, recognition, ranking, and to top it off many try to make significant sums of money, either directly or indirectly at the cost of others. Many of the world’s top 20 spammers from the Spamhaus’s ROKSO database of spam gangs are on the FBI’s most wanted list. These people do usually have the know-how to create new programs, known as zero day exploits, perform social engineering, physical and virtual breaking and entering, armed robbery, and any other means of accomplishing their goals. If they do not have the skills themselves, they are able to recruit many others to perform the development and tasks for them, leaving these “minions” to take the fall if they get caught, while the Black Hat disappears.

Some black hats hack in the name of professing a “greater good” such as a fight against abusive mega-corporations or oppressive governments. Others have philosophies of fighting for freedom of speech and civil rights, but cross the line, not only beyond the law, but beyond most peoples’ morality. Some are just downright anarchists, while others have no moral guide except their own greed and feeding of their impulses.

Enter the White Hats. These are the “good guys”. The information security specialists who fight off attacks from the black hats and their unwitting dupes the script kiddies. The white hats try to learn and keep up with the hacker culture, and setup many traps such as “honeypots” and “The Honeynet Project” (Know Your Enemy, 2002) to monitor them, all the while using the skills acquired to help a company, government agency or individual fight off attacks, perform forensics, hunt down and assist law enforcement in arresting the computer criminals.

Gray hats walk the middle path. They do break laws, but only out of curiosity not malignancy or financial gain. They try to follow a fairly strong moral code. They will break into systems, trying to “do no harm” in the process and as unobtrusively as possible, just for the challenge of solving the puzzles. They may leave little harmless text files saying things like “Killroy was here”. They do not mean to do harm, though sometimes they may inadvertently do so. They like to leave some evidence for “bragging rights” about having defeated a supposedly secure system.

A fairly new term assigned to hackers has been “Terrorist” or “cyber-terrorist”. This is generally a more subjective labeling currently, though clearer definitions are developing, and some individuals and groups are starting to wear the label with pride. Most of those who have been labeled as cyber-terrorists however, are generally not considered terrorists by their peers, and find the labeling completely inappropriate in most cases.

The hats orientation is usually clearly defined and self-professed, but sometimes it is more subjective. Some are called black hats by one group, and white hats by another, and believe themselves to be white hats, or at worst gray hats. As an example the US and China have been involved in cyber-warfare for many years now. Some of the more public battles epitomized with the “Code Red” worm and other attacks. Some of these attacks have been more officially sanctioned than others. The US would call those Chinese government computer security specialists that hacked the US government agencies’ websites, black hats. Whereas the Chinese government would call them white hats in retaliation to the attacks by US hackers against the Chinese government sites.

Another example of subjective labeling would be Mark A. Ludwig’s attempts at publishing “The Little Black Book of Email Viruses”. He fought censorship from publishers, government agencies and professional associations for years because they were afraid of his making the information publicly available. He felt it important to get the book published because he believed:

“When knowledge is restricted, be it by government edict or by a group of self-proclaimed experts, everyone suffers.”(Ludwig, 2002).

The fact that governments and companies feel they do not know what to do with “these people” or the related information does not warrant the outright abuses of supposed hackers' civil rights. Some people have spent days, weeks, months and even years being incarcerated without being properly charged with a crime, so as to allow the prisoner the beginnings of due process and a chance for a legal defense. Some of the more famous cases, such as Kevin Mitnick of the “Free Kevin” campaign, deserved criminal conviction after due process, but never deserved to rot in solitary confinement for years before finally receiving charges defining his crimes.

Another example of abuse and subjective mislabeling of “hackers” is the case of the Russian programmer Skylarov. He was a software developer for a legitimate Russian software development company. He came to the US to give a talk at a large technology convention in Las Vegas about his company’s products, and was promptly arrested by the FBI as he walked off the plane. Adobe Software had complained that Skylarov was a hacker and was making and distributing a software program that allowed the removal of their PDF copy protection, in violation of the US DMCA (Digital Millennium Copyright Act). The software he developed for his employer was completely legal in his country of origin, and was meant as an aide to PDF users who wished to make archival backups and the ability to move their files to their other devices, to make full use of their legitimately acquired digital documents. He was held for months without any hearings. It took the rallying of huge public protests and a growing boycott by computer developers and engineers nationwide, to pressure Adobe to drop the charges, with the government following suit shortly thereafter. Skylarov was allowed to return to his country, obviously with a reduced view of the freedoms of the USA.

Year after year since the latter 1990’s, and continuing to this day, new legislation is being passed that is taking away everyone’s civil rights, in the government's fear and ignorance motivated attempts at trying to deal with cybercrimes. The 2002 changes to the (FOIA) *Freedom of Information Act* allow “attacks, incidents and vulnerabilities on ‘critical infrastructure’” to be more easily withheld from the public (Rasmussen, Homeland Security and InfoSec, 2003), significantly reducing the effectiveness of the FOIA and leaving the general public and businesses much more vulnerable to what would otherwise be known attacks that the public could then use to defend themselves. *The Cyber Security Enhancement Act of 2002* stiffens penalties for cyber crimes to be far worse in conviction penalties (Rasmussen, Homeland Security and InfoSec, 2003) than those receiving convictions for acts of murder or rape.

It is important that technologists and layman alike have a better understanding of the hacker culture, and the differences between hacking and computer crime. The current growing ignorance and misunderstandings will lead to further inappropriate arrests and violations of civil rights, unless there is an increased awareness that “hackers are people too”. The hacker community, as with any other culture, have variances in the populace between “good” and “bad” individuals, and should not all be labeled as criminals as a whole, just because of their affinity or interest in “how things work”. The continuing revoking of civil rights in reaction to fear of the unknown and what to do about it, impact everyone, not just the hacker community, and everyone who has an appreciation for privacy, security and civil rights should take notice and realize that this affects everyone’s rights.

Works Cited

Levy, Steven. Hackers, Heroes of the Computer Revolution. Harmondsworth, Middlesex, England: Penguin Books Ltd., 2001.

Ludwig, Mark A. The Little Black Book of Email Viruses. Show Low, Arizona: American Eagle Publications, 2002.

The Honeynet Project. Know Your Enemey, Revealing the Security Tools, Tactics, and Motives of the Blackhat Community. Boston, MA: Addison-Wesley, 2002.

Rasmussen, Michael. Password, The ISSA Journal. January 2003. p 17. Homeland Security and InfoSec.