Old Hackers, New Hackers : What's the Difference ?

Steve Mizrach

Apparently, to people enamored of the "old school" of hackers, like Steven Levy or Clifford Stoll, there is a big difference. Indeed, to the "old style" MIT/Stanford hackers, they resent the bestowal of their honored title on "those people" by the media... To many people, "hacker" is reserved for a class of people in the 60s, a certain "breed" of programmer who launched the "computer revolution", but just can't seem to be found around any more... According to these "old school" hackers, hacking meant a willingness to make technology accessible and open, a certain "love affair" with the computer which meant "they would rather code than sleep". It meant a desire to create beauty with computers, to liberate information, to decentralize access to communication...

But what about the "new" hackers ? Many of the "old" hackers think they don't deserve the name, preferring to call them "computer criminals", "vandals", "crackers", "miscreants", or in a purely generational swipe, "juvenile delinquents". The media uses the word "hacker" to refer to young, clever computer users who use their modems to break into systems without authorization, much as depicted in the movie *WarGames*. And the old school hackers resent this. Many of the new hackers aren't good programmers; they are just people without ethics who have no reservations about swiping passwords, codes, software, and other information and trading them with their friends. They may be good at exploiting security holes in systems, but all they succeed in doing (say people like Stoll) is destroying the trust on which open networks are built.

I am interested, needless to say, in the generational aspect to this battle over the name "hacker". Most of the old hackers of the 60s are of course now living in the 90s - Baby Boomers who, like their ex-hippie friends, went from "freak" to "straight", finding jobs in computer security firms and corporate software conglomerates. And like other counterculturalists from the 60s, they just can't seem to figure out this Generation X forming the counterculture of the 90s... where's the openness ? The idealism ? These "juvenile delinquents" just don't live up to the high moral standards of the 60s nostalgiacs like Levy and Stoll. But then, Levy rants about those great hackers who founded Apple Computer and launched the PC revolution - those same ex-phreaks, Jobs and Wozniak, who actually allowed their company to patent their system hardware and software !

The "cyberpunks" of the 90s, it seems, just don't live up to what people like Stoll and Levy expect of them. And all the old "hackers" go to great pains to define themselves apart from the new breed of "hackers", always groaning in angst when the label continues to be applied to them. I would argue that the hackers of the 90s are not so different from the hackers of the 60s, that indeed, the same exploratory, antiauthoritarian, liberatory impulses are at work; it is simply that the hackers of the 60s do not understand the situation in which we live, and this is probably because they read 60s hippie lit rather than 90s cyberpunk SF... The "old hackers" are simply too comfortable to be afflicted... They don't understand why the new "hacker" does what he does.

According to Levy, the differences between the old and new hackers are stark and clear. The first group strove to create, the second strives to destroy and tamper, he says. The first group loved control over their computers, but the second group loves the power computers gives them over people. The first group was always seeking to improve and simplify; the second group only exploits and manipulates. The first group did what they did because of a feeling of truth and beauty in their activities; the second group hacks for profit and status. The first group was communal and closely knit, always sharing openly their new hacks and discoveries; the second, he says, is paranoid, isolated, and secretive. For Levy, the old hackers were computer wizards, but the new hackers are computer terrorists, always searching for new forms of electronic vandalism or maliciousness without thought of the consequences.

But where Levy sees differences, I see some curious similarities. Old-style MIT "hackers" were rather well-known for getting around locks of both the physical and electronic variety. Is there such a difference between the righteous anger of the MIT hacker toward the IBM "priesthood" who kept him away from the massive mainframe, and the 90s hacker who feels righteous anger over being prevented access from huge commercial databases without an expensive account ? The old MIT hackers were also known for their exploration of the phone system, and exploring "hacks" to make calls to unsuspecting places for free. Indeed, many of the early hackers were phone phreaks, plain and simple, ripping off service from the phone company (THE company, AT&T, alias Ma Bell, back then), which they resented for its refusal to share the technical information about telephony.

The 60s hackers were known for their desire for liberating information. They openly shared source code; members of the Homebrew Computer Club also openly shared with each other the flaws of various machines, and "hacks" to get around their lack of performance. Since Levy seems to think that software piracy should not be a crime (since he thinks source code should not be copyrighted), his problem with the "new hackers" does not appear to be piracy. Neither does it appear to be the open sharing of some admittedly dangerous "real-world" information taken straight from books like the *Anarchist Cookbook* on how to make bombs and drugs. Rather, it seems to focus around the malicious misdeeds of a small minority, dedicated to spreading Trojan horses, logic bombs, viruses, worms, and other destructive programs...

In actuality, the majority of viruses (such as the Christmas virus) are harmless. They eat up small fractions of CPU space and are designed, rather than to wipe clean someone's hard drive, to just display a message at a given time. They are, in short, pranks - something that Levy also points out the old MIT hackers were overfond of. They were known for playing complex tricks on people, and were masters of "social engineering" - the art of manipulating technocrats by being a good bullshit artist - just as the 90s hackers are... their elaborate games and pranks often being ways to demonstrate their superiority to the faculty, administrators, or other "know-it-alls" who they felt got in their way of their access to computers...

In "invading" corporate voicemail systems, the modern 90s hackers are no different than the 60s MIT hackers mapping out the labyrinths of the MIT underground tunnel system. They do it for the same reasons : because they are told not to, because the conduits often lead to surprising places, because the activity is basically harmless even though it is declared unauthorized or even illegal, and because it gives them a feeling of mastery and control over a complex problem. The simple fact is, most of the 90s hackers are not wantonly malicious or destructive. Indeed, many subscribe to an updated 90s Hacker Ethic, declaring that they will not "hack" personal privacy or the personal computer user, instead declaring that their "targets" will be large, unresponsive corporations or bureaucratic government organizations...

But the main reason for the difference between the 60s and 90s hackers is that the GenXers are a "post-punk" generation, hence the term, "cyberpunk". Their music has a little more edge and anger and a little less idealism. They've seen the death of rock n'roll, and watched Michael Bolton and Whitney Houston try and revive its corpse. Their world is a little more multicultural and complicated, and less black-and-white. And it is one in which, while computers can be used to create beauty, they are also being used to destroy freedom and autonomy... hence control over computers is an act of self-defense, not just power-hunger. Hacking, for some of the new "hackers", is more than just a game, or a means to get goodies without paying for them. As with the older generation, it has become a way of life, a means of defining themselves as a subculture...

Many of them are quite deliberately "nonviolent" in their ambitions. They will not lock others out from their accounts, damage or change data without permission, or do anything to jeopardize system viability. Instead, they enter computer systems to 1) look around and see what's there (if someone breaks into your house, looks at the posters on your wall, then locks the door on the way out, have they committed a crime ?) 2) see where else they can go from where they are (what connections can be pursued ?) and 3) take advantage of any unique abilities of the machine that they've accessed. MIT's hackers did all of these things and more with the various mainframes they were "forbidden" to access and explore... They questioned the right of technocrats to limit access, and openly transgressed their arbitrary limitations based on invoked mantras of the preciousness of computer time.

Indeed, the 90s hackers pay a lot of homage to the first generation. They have borrowed much of their jargon and certainly many of their ideas. Their modus operandi, the PC, would not be available to them were it not for the way the 60s hackers challenged the IBM/corporate computer model and made personal computing a reality... Their style, their use of handles, their love for late-night junk food, are all testaments to the durability and transmission of 60s Hacker culture. So why are the biographers of the 60s hackers so antagonistic and hostile to the new 90s hackers ? Do they sense some sort of betrayal of the original Hacker Ethic and its imperatives ? Is it just the classic refusal to pass a torch onto a new generation ?

Breaking into the root node of a UNIX network or the system manager account of a VAX network takes nimble thinking and clever programming. It often takes a knowledge of various loopholes in the system, and clever tricks that can be done with its coding. It often requires unorthodox uses of standard applications. In short, it requires hacking in the oldest and best senses of the term. In doing it, many 90s hackers seek to expand their knowledge of the system and its capabilities, not to sabotage the efforts of others or wreck the system. Phreaks, in "hacking" the phone system, are simply acting in the centuries-old tradition of American radicals who have always challenged the ways in which corporate and governmental structures prevent people from free association with their peers... Challenging the notion that "to reach out and touch someone" should be a costly privilege rather than a right.

Someday, the old and new "hackers" may sit down, and discuss their commonalities rather than their differences. They may realize that they share an alienation from the existing system. They might find out that they have motivations and principles in common. Most importantly, they might stop competing with each other for a mantle or title. The old hackers might see the ways in which their countercultural visions failed to take account of new realities, and they might provide a sense of communal vision and purpose for the often backstabbing and self-aggrandizing new hackers. If they were to actually team up, it might be mean what Bruce Sterling calls "the End of the Amateurs". And the beginning of "Computer Lib" ?