A Short History of Hacking in America

Steve Steinberg
1998

> Big Science. Hallelujah.
> Big Science. Yodellayheehoo.
> -- Laurie Anderson

Big science is dead. Forget the huge research labs bustling with bearded scientists in white lab coats -- we tried that route and all we got was overpriced space junk. Cheap technology means that we can all explore the electronic frontier instead of getting handouts from the scientific establishment. Bruce Sterling says it best : "Science in this world is not a source of Mr. Wizard marvels, but an omnipresent, all-permeating, definitive force. It is a sheet of mutating radiation pouring through a crowd, a jam-packed Global Bus roaring wildly up an exponential slope". OK, so Sterling was talking about the world in William Gibson's Sprawl series (it rings just as true for the US in 1991). Underground bands such as "Non Serviam" and "Consolidated" are using state-of-the-art technology to create sounds that the machine's inventors never thought possible, while fringe graphic artists have the equivalent of a $100,000 color studio on their desktop. People on the street, the formerly disfranchised, have wrested technology from the capital-S Scientists and are stretching and warping it into their own image.

It's not just artists who are using technology in unintended ways. A movement that is just as important are the youths who use computers to illegally joyride through the global communications network. The hackers. Over the last few years, the publicity about hackers has been fast and furious, to the point where hacking may even seem passe. Many people now believe that hackers are just middle class male teenagers who break a minor law or two. This is missing the point. Hackers are important because they are at the front. They're spelunking cyberspace, exploring the parts of the network few of us can see. They're not happy with just their IBM PC and a local bulletin board. They want it all, the whole god damn global network -- even if it means breaking a few laws. If you don't think this is important, listen to cyber-sage John Perry Barlow :

> "What crackers are doing is learning about a new place, exploring in a very open ended fashion, a place that no one knows very well. If you work for a telco you know that place exists but you are only familiar with your little precinct of it. You don't have a broad spectrum sense of it. And I think its culturally important to develop such a sense".

The Early Days (1970-1983)

It all started with phone phreaks. These were people fascinated with the phone system -- what it was made of, how it worked -- and how you could avoid paying for your calls. In the early 1970's, Abbie Hoffman put up the money to start a newsletter called *YIPL* (the name was later changed to *TAP*). It was a place where all those people who loved to dial random numbers just to see if they could find a special Bell test number could get together and share their discoveries. The magazine was started just in time to catch the first major phreaker

discovery : the blue box.

In perhaps one of the biggest mistakes in publishing history, the Bell Technical Journal had published an article giving the special tone frequencies that were used to route calls and to control the telephone network. It didn't take long before some bright college engineering students realized what this meant : any person with a device that could make those tones would have the capabilities of a telephone operator. The tone devices, which soon came to be called blue boxes, launched the phreaking career of many luminaries from the outlaw Captain Crunch to Apple Computer co-founder Steve Wozniak. A whole community quickly formed, connected by the soft beeps of their boxes. Phreaks would set up illegal teleconferences where they would hang out and trade tips on how to build and use boxes. Because phone phreaks could make calls for free by using their blue box, physical location (and physical appearance) were unimportant. It didn't matter if you lived in Tennessee, when you **really** lived in cyberspace.

But by 1980, blue boxing had become difficult to do without being caught, so a new activity, hacking, began to supplant boxing. Computers were now available at prices affordable by many people and phone phreaks discovered that from home they could call up and connect to mainframe computers owned by large corporations and universities. Security was very minimal at this time, many mainframe computers didn't even require a password to gain entry. The exciting thing about hacking was not only the challenge but that there was so much to learn. Many computer enthusiasts had quickly grown bored with their simple home computer and its slow BASIC language. By hacking into mainframes these computer enthusiasts could access real computing power and learn about things like JCL, VMS and Unix. Hacking was getting more and more popular -- and then, along came the explosion.

The Renaissance (1983-1988)

The hacking community always had high turn-over. Every January there would be an influx of young hackers who had received modems for Christmas, and every September some of the older hackers would leave for college and "go legit". But when the movie *WarGames* came out, with Matthew Broderick making hacking look fun and easy (and heck, it even got him the girl), every 15 year old in the country begged their parents for a modem. And then they called the local bulletin boards. And then they discovered code abuse. The well-known UNIX hacker Shooting Shark recently declared, "I'll admit it, my interest in hacking was largely influenced by that film".

Codes were what replaced blue boxes in allowing hackers to make free calls, and in the process, keep a national (and increasingly, international) underground together. Codes were simply telephone calling card numbers, usually 5 or 6 digits that allowed someone to use a carrier other than AT&T. Remember : this was before "equal access" and 10XXX dialing. Shooting Shark was one of the thousands who discovered, and fell in love with, code abuse. "Elric of Imrryr explained that all I needed to do was dial an 800 number, enter a six-digit code, and then I could call anywhere I wanted for FREE! It was the most amazing thing". It would be hard to overemphasize the importance of codes to the computer underground. Although it quickly became unfashionable to be too interested in acquiring codes (or else you would find yourself labeled a "Codez Kid") they were a crucial tool. Not only did codes allow hackers to stay in contact and to call electronic bulletin boards no matter where the board was located, it also allowed people to make the many calls it took to successfully hack a distant computer site.

These were exciting times. A number of legendary boards and hackers emerged during this period. "Plovernet", "Metal Shop Private" and "Catch-22" were datahavens in the net where notorious hackers and phone phreaks

could freely share secret, arcane information. Here, the incredible talents of hackers like King Blotto, Sharp Razor and Mark Tabas were displayed. Things moved at lightspeed -- a hacker could make or lose their reputation in a week. Many hackers dedicated every waking moment to their illicit pursuits. The now infamous Legion of Doom group was formed by Lex Luthor around this time. Membership in LoD, as in most other hacking groups, was by invitation only. LoD was able to attract some of the best people and got a reputation for being very, very heavy. Of course, there were plenty of hackers who thought the LoD's reputation was undeserved and they would get into fights with the LoD. Hacker wars could get vicious with people trying to find out their enemy's real name and phone number so they could disconnect the line, or even listen in on enemy hacker conversations.

By 1988, things were beginning to slow down. A number of prominent members of the computer underground including Knight Lightning and The Prophet were leaving for college. Furthermore, a large bust occurred that year which netted a number of talented hackers including Bill From RNOC and Lock Lifter. And things were about to get much worse. Hacker Erik Bloodaxe remembers this renaissance period and lamented : "I don't think it's ever going to be the same. There will never be this wild, rampant, trading of information and just...it was like sex in the streets. Stuff going around left and right. It will never be like that again".

End of an Era (1988-1990)

What really broke up the party was the cops. The Secret Service to be exact. Although known primarily for its protection of the US president, in 1990, over one-third of all Secret Service agents were busy tracking down and arresting hackers. In January the SS busted Phiber Optik and Acid Phreak, two prominent East Cost phone phreaks. Then in February, stemming from an innocuous (but admittedly pilfered) Bell South document that was published in the electronic underground magazine *Phrack*, three of the top US hackers were busted : The Prophet, The Leftist and The Urville. Craig Neidorf, co-editor of *Phrack* and known as Knight Lightning, was also charged with illegally publishing the purloined document. Things just got more ridiculous. In March the Secret Service raided Steve Jackson Games, a publisher of role playing games, calling one of the companies game books a "handbook for computer crime". During all this Gail Thackeray, a district attorney in Arizona, was coordinating Operation Sun Devil which culminated in 28 raids in May. The investigations reeked of Keystone Kop-style tactics due to the Secret Service's ignorance of computer technology and their general heavy handed manner. In one effort to get something on these "dirty hackers" the Secret Service videotaped a bunch of hackers drinking beer from behind a one-way mirror.

Although many of the arrests and charges detailed above were later dropped (most notably the case against Neidorf) the large number of busts and resulting details about police infiltration into the computer underground raised hacker's paranoia to a fever pitch. Bloodaxe pointed out to me last year that "even on the elite private boards that still kinda float around, there still isn't much camaraderie. You're not going to see, 'here's the password for Telenet's PRIME's so you can use TDT'. Maybe two hackers know it, but they're not going to tell anybody, not even on the most elite board. Because, as far as everyone is concerned, there are leaks. No matter how secure it seems, people are convinced there is a leak".

In reaction to the governments witch hunt against hackers, Mitch Kapor (founder of Lotus Corporation), John Perry Barlow (Grateful Dead lyricist), and John Gilmore (generalist) founded the Electronic Frontier Foundation. While the EFF is not the "hacker defense fund" it was accused of being by early media reports, it is interested in curbing the government's excess zeal in busting hackers. The EFF has made some significant strides towards this goal of treating computer crime rationally, but interestingly, the EFF has also had a deleterious effect on the computer underground. With the increase in favorable publicity, many hackers have

become less feral -- more interested in talking to reporters than breaking into computers. This was typified by Eric Bloodaxe's highly publicized announcement in June of 1991 that he and several other hackers from the Legion of Doom group were forming a computer security firm called COMSEC. Many in the computer underground saw this as selling out, while others saw it as simply survival.

Hackers are beginning to regroup now. They often have to relearn information which was known during the renaissance of the computer underground, but which was not passed down. More and more hack/phreak bulletin boards are springing back up across the country. Hackers are being more careful this time around -- and that's a good thing.

Future

Hacking will never be obsolete. There will always be kids who want to explore, and the terrain of cyberspace is only going to get more alluring. Technology reporter John Markoff points out "I mean, think about being a high school kid... what can you do in the world ? You can go hang out at the mall, or... from your room, you can travel all over the world. It's very compelling". Hacking will continue to get harder, as security gets smarter. But, that's what street tech is all about : exploiting technological loop holes for education, fun, and profit. If there isn't just a little part of you that wants to be a hacker, an electronic rat furrowing through the network, you don't belong in cyberspace.