

STEVEN ALEXANDER

why teenagers hack: a personal memoir



Steven is a programmer for Merced College. He manages the college's intrusion detection system.

alexander.s@mccd.edu

BROWSING THROUGH SOME OLD

issues of *;login*: online, I came across the “Point/Counterpoint” that Tina Darmohray and Rob Kolstad wrote in April of 2002 about the possible culpability of the security community in the hacking career of Ben Breuninger, a.k.a. konceptor. (The young man was invited to represent the “black hats” at a computer conference in Orlando, Florida.) Both their points of view are interesting. I do agree with Rob that a twenty-one-year-old ought to have known better. But sometimes growing up is hard to do.

I don't think anyone intended the 1998 conference to be exploitative, but I can imagine the unintended consequences it may have had. While the “good” attendees may have encouraged Ben to pursue computers in other ways, being funded to appear at the conference must have stroked his ego fiercely.

I understand this because, unfortunately, I myself did not start out on the right side. I straightened myself out a long time ago, but for a while things were a little different from the way they are now.

The dark side was very tempting because it offered numerous benefits, both perceived and real, for a teenager. It was rebellious and cool. It was empowering to know more about computers and networks than the adults around me; break-ins were a way of proving this. Nobody my age cared that I could write neat programs in assembly language or even cared to know what the hell assembly language was.

Quake skills would win you a few friends, but my computer couldn't run the game, and I wasn't particularly interested in playing video games anyway. Hacking?¹ That was cool. Almost none of my peers understood anything about the mechanics of it—what they did understand was picked up from movies like *Wargames* and (shudder) *Hackers*—but damned if I wasn't sticking a finger up at the authorities and the system.

One of the worst aspects was the wild myths that surrounded hacking. I once heard the insane assertion that anyone who was able to hack MIT's network would be admitted into the MIT CS program. Stories of companies hiring hackers for six-figure salaries floated around here and there. Most unfortunately, there is truth to some of the stories.

I think that it is important for adults to reach out to young black hats and try to convince them to pursue their interest in security through other means. One of

my high school teachers was instrumental in bringing me around. Sadly, many adults are quite unhelpful.

I became interested in computers at 13, started hacking by 14, and gave hacking up at 16; I had finally grown up enough to join the mainstream. I had skated through my first two years of high school not trying to do particularly well. By the time I was a junior, I knew that I wanted to go to college (yay!), major in computer science, etc., and I knew what I needed to do to get there. The major reasons that I quit hacking are that I no longer valued the popularity that it brought me, I realized the consequences it might bring upon me, I came to understand the stress and problems it was causing admins worldwide, and I figured out that I wasn't really respected, just feared. In other words, I grew up.

The problem was that in about the second or third week of my sophomore year, I had hacked my high school's Web site. I got away with it—barely. My IP address was logged. The school contacted my ISP. The ISP thought it was me but said they couldn't swear to it (I don't know why; maybe the log times were sketchy). They knew, I knew they knew, and I knew they couldn't prove it.

Fast-forward a couple of years. I'm a high school senior. I'm assembling applications for various colleges. I'm pulling straight As, have strong SAT scores, AP classes, etc. Two Windows NT servers crash in the middle of a Service Pack 3 install and someone decides to blame me. I'm pulled out of class, searched, have a floppy disk confiscated, and am interrogated for three hours by three vice principals. The computer I use at school is searched, but the only "bad" thing on it is mIRC.

My stepdad and I met with three vice principals, two network admins, and a police officer. One of the network admins explained that they knew that I had been responsible, because the IP address of the computer I used in my programming class was displayed on the trademark Blue Screen of Death when the servers crashed (no, I'm not kidding). I wasn't in the class with the suspect computer when the "attack" occurred, but the theory was that I had written a program to crash the servers at a certain time, then erase itself.

They never did settle on a technical explanation for the crash. The last I heard, they suspected it was a one-megabyte IP packet (I'm still not kidding, and, no, I have no idea who came up with the notion). Since I was officially in violation of the school's acceptable-use policy by having mIRC installed, I was banned from using any school computer. Since I couldn't use school computers, I was dropped from my programming class and my networking class. My stepdad bought the administrators' reasoning, of course.

The networking class was a work-study class that had me working at a local ISP (my ISP, the one that almost caught me!). Someone (one of the vice principals, most likely) called the ISP and talked to my boss, the network admin. They explained everything and laid out the "evidence" for him. The school suggested that the ISP fire me. My boss, thank Joe Pesci,² told them basically to go to hell. As he put it, in rather unkind language, their admins were liars and idiots to boot.

My point is that, while some professionals try to help talented youths apply their skills in positive ways, other adults are not so reasoned in their approach.

These days I look at what happened as having been, for the most part, a karmic kick in the ass. The whole situation did, after all, start with me doing things I shouldn't have been doing. But at the time, I was not encouraged to move over to the right side. If it had not been for some very supportive people, primarily my boss and my girlfriend (who is now my wife), I don't think I would have changed. My gut reaction was to grab my assembly manuals and write an implacable, firmware-flashing bit of madness to wreak havoc throughout my school district. It was hard to walk away.

It is unbelievably empowering to know that you don't have to play by the same rules as everyone else. I understand from the "Point/Counterpoint" article that Ben Breuninger didn't have a grudge against LLNL. I don't think that mattered. Hacking gives you the ability to exist outside the law (for a while). The risk is relatively low, and you're aren't hurting other people in a way that is tangible, as it is with other crimes. (Of course, those in the DoS business are looking to cause tangible losses.)

I felt spurned by "the system" when I got into trouble. Before that, I felt empowered. I think others also feel empowered by the respect and awe they are handed and believe that they are placed above or outside the system because of it. Some feel that the system will actually reward their transgressions if they prove themselves skillful enough.

I don't think there is a lot that can be done once people who should have grown up already act out and find themselves on the wrong side of the law. I am very glad that I grew up before I met the fate others, like Ben, have suffered.

I think that hiring convicted or active hackers sets a terrible precedent. It reinforces the myths that make the dark side alluring. I don't think that learning from a teenage hacker or respecting his knowledge on technical matters is bad. I do think these kids should be encouraged to do more productive things (kudos to Rob on USACO in this context). Those who are caught young enough should be both punished and steered in new directions.

The bottom line is, however, that some kids will not grow up. They will continue to make poor choices and to break the law. They will continue to value the adulation of their peers and the myths of idiots over the well-reasoned advice of adults and professionals, and there really isn't a thing anybody can do about it.

1. Forgive me for using this in the media-driven rather than kernel-hacking sense.
2. See George Carlin's *You Are All Diseased*.