
GUIDE TO (mostly) HARMLESS HACKING

Beginners' Series Number 5

Computer hacking. Where did it begin and how did it grow?

If you wonder what it was like in days of yore, ten, twenty, thirty years ago, how about letting and old lady tell you the way it used to be.

Where shall we start? Seventeen years ago and the World Science Fiction Convention in Boston, Massachusetts? Back then the World Cons were the closest thing we had to hacker conventions.

Picture 1980. Ted Nelson is running around with his Xanadu guys: Roger Gregory, H. Keith Henson (now waging war against the Scientologists) and K. Eric Drexler, later to build the Foresight Institute. They dream of creating what is to become the World Wide Web. Nowadays guys at hacker cons might dress like vampires. In 1980 they wear identical black baseball caps with silver wings and the slogan: "Xanadu: wings of the mind." Others at World Con are a bit more underground: doing dope, selling massages, blue boxing the phone lines. The hotel staff has to close the swimming pool in order to halt the sex orgies.

Oh, but this is hardly the dawn of hacking. Let's look at the Boston area yet another seventeen years further back, the early 60s. MIT students are warring for control of the school's mainframe computers. They use machine language programs that each strive to delete all other programs and seize control of the central processing unit. Back then there were no personal computers.

In 1965, Ted Nelson, later to become leader of the silver wing-headed Xanadu gang at the 1980 Worldcon, first coins the word "hypertext" to describe what will someday become the World Wide Web. Nelson later spreads the gospel in his book Literacy Online.

But in 1965 the computer is widely feared as a source of Orwellian powers. Yes, as in George Orwell's ominous novel , "1984," that predicted a future in which technology would squash all human freedom. Few are listening to Nelson. Few see the wave of free-spirited anarchy the hacker culture is already unleashing. But LSD guru Timothy Leary's daughter Susan begins to study computer programming.

Around 1966, Robert Morris Sr., the future NSA chief scientist, decides to mutate these early hacker wars into the first "safe hacking" environment. He and the two friends who code it call their game "Darwin." Later "Darwin" becomes "Core War," a free-form computer game played to this day by some of the uberest of uberhackers.

Let's jump to 1968 and the scent of tear gas. Wow, look at those rocks hurling through the windows of the computer science building at the University of Illinois at Urbana-Champaign! Outside are 60s antiwar protesters. Their enemy, they believe, are the campus' ARPA-funded computers. Inside are nerdz high on caffeine and nitrous oxide. Under the direction of the young Roger Johnson, they gang together four CDC 6400s and link them to 1024 dumb vector graphics terminals. This becomes the first realization of cyberspace: Plato.

1969 turns out to be the most portent-filled year yet for hacking.

In that year the Defense Department's Advanced Research Projects Agency funds a second project to hook up four mainframe computers so researchers can share their resources. This system doesn't boast the vector graphics of the Plato system. Its terminals just show ASCII characters: letters and numbers. Boring, huh?

But this ARPAnet is eminently hackable. Within a year, its users hack together a new way to ship text files around. They call their unauthorized, unplanned invention "email." ARPAnet has developed a life independent of its creators. It's a story that will later repeat itself in many forms. No one can control cyberspace. They can't even control it when it is just four computers big.

Also in 1969 John Goltz teams up with a money man to found Compuserve using the new packet switched technology being pioneered by ARPAnet. Also in 1969 we see a remarkable birth at Bell Labs as Ken Thompson invents a new operating system: Unix. It is to become the gold standard of hacking and the Internet, the operating system with the power to form miracles of computer legerdemain.

In 1971, Abbie Hoffman and the Yippies found the first hacker/phreaker magazine, YIPL/TAP (Youth International Party -- Technical Assistance Program). YIPL/TAP essentially invents phreaking -- the sport of playing with phone systems in ways the owners never intended. They are motivated by the Bell Telephone monopoly with its high long distance rates, and a hefty tax that Hoffman and many others refuse to pay as their protest against the Vietnam War. What better way to pay no phone taxes than to pay no phone bill at all?

Blue boxes burst onto the scene. Their oscillators automate the whistling sounds that had already enabled people like Captain Crunch (John Draper) to become the pirate captains of the Bell Telephone megamonopoly. Suddenly phreakers are able to actually make money at their hobby. Hans and Gribble peddle blue boxes on the Stanford campus.

In June 1972, the radical left magazine Ramparts, in the article "Regulating the Phone Company In Your Home" publishes the schematics for a variant on the blue box known as the "mute box." This article violates Californian State Penal Code section 502.7, which outlaws the selling of "plans or instructions for any instrument, apparatus, or device intended to avoid telephone toll charges." California police, aided by Pacific Bell officials, seize copies of the magazine from newsstands and the magazine's offices. The financial stress leads quickly to bankruptcy.

As the Vietnam War winds down, the first flight simulator programs in history unfold on the Plato network. Computer graphics, almost unheard of in that day, are displayed by touch-sensitive vector graphics terminals. Cyberpilots all over the US pick out their crafts: Phantoms, MIGs, F-104s, the X-15, Sopwith Camels. Virtual pilots fly out of digital airports and try to shoot each other down and bomb each others' airports. While flying a Phantom, I see a chat message on the bottom of my screen. "I'm about to shoot you down." Oh, no, a MIG on my tail. I dive and turn hoping to get my tormentor into my sights. The screen goes black. My terminal displays the message "You just pulled 37 Gs. You now look more like a pizza than a human being as you slowly flutter to Earth."

One day the Starship Enterprise barges in on our simulator, shoots everyone down and vanishes back into cyberspace. Plato has been hacked! Even in 1973 multiuser game players have to worry about getting "smurfed"! (When a hacker breaks into a multiuser game on the Internet and kills players with techniques that are not rules of the game, this is called "smurfing.")

1975. Oh blessed year! Under a Air Force contract, in the city of Albuquerque, New Mexico, the Altair is born. Altair. The first microcomputer. Bill Gates writes the operating system. Then Bill's mom persuades him to move to Redmond, CA where she has some money men who want to see what this operating system business is all about.

Remember Hans and Gribble? They join the Home Brew Computer club and choose Motorola microprocessors to build their own. They begin selling their computers, which they brand name the Apple, under their real names of Steve Wozniak and Steve Jobs. A computer religion is born.

The great Apple/Microsoft battle is joined. Us hackers suddenly have boxes that beat the heck out of Tektronix terminals.

In 1978, Ward Christenson and Randy Suess create the first personal computer bulletin board system. Soon, linked by nothing more than the long distance telephone network and these bulletin board nodes, hackers create a new, private cyberspace. Phreaking becomes more important than ever to connect to distant BBSs.

Also in 1978, The Source and Compuserve computer networks both begin to cater to individual users. "Naked Lady" runs rampant on Compuserve. The first cybercafe, Planet Earth, opens in Washington, DC. X.25 networks reign supreme.

Then there is the great ARPAnet mutation of 1980. In a giant leap it moves from Network Control Protocol to Transmission Control Protocol/Internet Protocol (TCP/IP). Now ARPAnet is no longer limited to 256 computers -- it can span tens of millions of hosts! Thus the Internet is conceived within the womb of the DoD's ARPAnet. The framework that would someday unite hackers around the world was now, ever so quietly, growing. Plato fades, forever limited to 1024 terminals.

Famed science fiction author Jerry Pournelle discovers ARPAnet. Soon his fans are swarming to find excuses -- or whatever -- to get onto ARPAnet. ARPAnet's administrators are surprisingly easygoing about granting accounts, especially to people in the academic world.

ARPAnet is a pain in the rear to use, and doesn't transmit visuals of fighter planes mixing it up. But unlike the glitzy Plato, ARPAnet is really hackable and now has what it takes to grow. Unlike the network of hacker bulletin boards, people don't need to choose between expensive long distance phone calls or phreaking to make their connections. It's all local and it's all free.

That same year, 1980, the "414 Gang" is raided. Phreaking is more hazardous than ever.

In the early 80s hackers love to pull pranks. Joe College sits down at his dumb terminal to the University DEC 10 and decides to poke around the campus network. Here's Star Trek! Here's Adventure! Zork! Hmm, what's this program called Sex? He runs it. A message pops up: "Warning: playing with sex is hazardous. Are you sure you want to play? Y/N" Who can resist? With that "Y" the screen bursts into a display of ASCII characters, then up comes the message: "Proceeding to delete all files in this account." Joe is weeping, cursing, jumping up and down. He gives the list files command. Nothing! Zilch! Nada! He runs to the sysadmin. They log back into his account but his files are all still there. A prank.

In 1983 hackers are almost all harmless pranksters, folks who keep their distance from the guys who break the law. MITs "Jargon file" defines hacker as merely "a person who enjoys learning about computer systems and how to stretch their capabilities; a person who programs enthusiastically and

enjoys dedicating a great deal of time with computers."

1983 the IBM Personal Computer enters the stage powered by Bill Gates' MS-DOS operating system. The empire of the CP/M operating system falls. Within the next two years essentially all microcomputer operating systems except MS-DOS and those offered by Apple will be dead, and a thousand Silicon Valley fortunes shipwrecked. The Amiga hangs on by a thread. Prices plunge, and soon all self-respecting hackers own their own computers. Sneaking around college labs at night fades from the scene.

In 1984 Emmanuel Goldstein launches 2600: The Hacker Quarterly and the Legion of Doom hacker gang forms. Congress passes the Comprehensive Crime Control Act giving the US Secret Service jurisdiction over computer fraud. Fred Cohen, at Carnegie Melon University writes his PhD thesis on the brand new, never heard of thing called computer viruses.

1984. It was to be the year, thought millions of Orwell fans, that the government would finally get its hands on enough high technology to become Big Brother. Instead, science fiction author William Gibson, writing Neuromancer on a manual typewriter, coins the term and paints the picture of "cyberspace." "Case was the best... who ever ran in Earth's computer matrix. Then he doublecrossed the wrong people..."

In 1984 the first US police "sting" bulletin board systems appear.

The 80s are the war dialer era. Despite ARPAnet and the X.25 networks, the vast majority of computers can only be accessed by discovering their individual phone lines. Thus one of the most treasured prizes of the 80s hacker is a phone number to some mystery computer.

Computers of this era might be running any of dozens of arcane operating systems and using many communications protocols. Manuals for these systems are often secret. The hacker scene operates on the mentor principle. Unless you can find someone who will induct you into the inner circle of a hacker gang that has accumulated documents salvaged from dumpsters or stolen in burglaries, you are way behind the pack. Kevin Poulson makes a name for himself through many daring burglaries of Pacific Bell.

Despite these barriers, by 1988 hacking has entered the big time. According to a list of hacker groups compiled by the editors of Phrack on August 8, 1988, the US hosts hundreds of them.

The Secret Service covertly videotapes the 1988 SummerCon convention.

In 1988 Robert Tappan Morris, son of NSA chief scientist Robert Morris Sr., writes an exploit that will forever be known as the Morris Worm. It uses a combination of finger and sendmail exploits to break into a computer, copy itself and then send copy after copy on to other computers. Morris, with little comprehension of the power of this exponential replication, releases it onto the Internet. Soon vulnerable computers are filled to their digital gills with worms and clogging communications links as they send copies of the worms out to hunt other computers. The young Internet, then only a few thousand computers strong, crashes. Morris is arrested, but gets off with probation.

1990 is the next pivotal year for the Internet, as significant as 1980 and the launch of TCP/IP. Inspired by Nelson's Xanadu, Tim Berners-Lee of the European Laboratory for Particle Physics (CERN) conceives of a new way to implement hypertext. He calls it the World Wide Web. In 1991 he quietly unleashes it on the world. Cyberspace will never be the same. Nelson's Xanadu, like Plato, like CP/M, fades.

1990 is also a year of unprecedented numbers of hacker raids and arrests.

The US Secret Service and New York State Police raid Phiber Optik, Acid Phreak, and Scorpion in New York City, and arrest Terminus, Prophet, Leftist, and Urvile.

The Chicago Task Force arrests Knight Lightning and raids Robert Izenberg, Mentor, and Erik Bloodaxe. It raids both Richard Andrews' home and business. The US Secret Service and Arizona Organized Crime and Racketeering Bureau conduct Operation Sundevil raids in Cincinnatti, Detroit, Los Angeles, Miami, Newark, Phoenix, Pittsburgh, Richmond, Tucson, San Diego, San Jose, and San Francisco. A famous unreasonable raid that year was the Chicago Task Force invasion of Steve Jackson Games, Inc.

June 1990 Mitch Kapor and John Perry Barlow react to the excesses of all these raids to found the Electronic Frontier Foundation. Its initial purpose is to protect hackers. They succeed in getting law enforcement to back off the hacker community.

In 1993, Marc Andreesson and Eric Bina of the National Center for Supercomputing Applications release Mosaic, the first WWW browser that can show graphics. Finally, after the fade out of the Plato of twenty years past, we have decent graphics! This time, however, these graphics are here to stay. Soon the Web becomes the number one way that hackers boast and spread the codes for their exploits. Bulletin boards, with their tightly held secrets, fade from the scene.

In 1993, the first Def Con invades Las Vegas. The era of hacker cons moves into full swing with the Beyond Hope series, HoHocon and more.

1996 Aleph One takes over the Bugtaq email list and turns it into the first public "full disclosure" computer security list. For the first time in history, security flaws that can be used to break into computers are being discussed openly and with the complete exploit codes. Bugtraq archives are placed on the Web.

In August 1996 I start mailing out Guides to (mostly) Harmless Hacking. They are full of simple instructions designed to help novices understand hacking. A number of hackers come forward to help run what becomes the Happy Hacker Digest.

1996 is also the year when documentation for routers, operating systems, TCP/IP protocols and much, much more begins to proliferate on the Web. The era of daring burglaries of technical manuals fades.

In early 1997 the readers of Bugtraq begin to tear the Windows NT operating system to shreds. A new mail list, NT Bugtraq, is launched just to handle the high volume of NT security flaws discovered by its readers. Self-proclaimed hackers Mudge and Weld of The LOpht, in a tour de force of research, write and release a password cracker for WinNT that rocks the Internet. Many in the computer security community have come far enough along by now to realize that Mudge and Weld are doing the owners of NT networks a great service.

Thanks to the willingness of hackers to share their knowledge on the Web, and mail lists such as Bugtraq, NT Bugtraq and Happy Hacker, the days of people having to beg to be inducted into hacker gangs in order to learn hacking secrets are now fading.

Where next will the hacker world evolve? You hold the answer to that in your hands.

Want to see back issues of Guide to (mostly) Harmless Hacking? See:
http://www.geocities.com/TimesSquare/Arcade/4594

http://base.kinetik.org
http://www.anet-chi.com/~dsweir
http://www.tacd.com/zines/gtmhh/
http://ra.nilenet.com/~mjl/hacks/codez.htm
http://www.ilf.net/brotherhood/index2.html
http://www.magnum44.com/orion/entry.htm
http://www.geocities.com/NapaValley/1613/main.html

To subscribe to Happy Hacker Digests, moderated by Roger Prata and Strider, and receive more of these Guides to (mostly) Harmless Hacking, please email majordomo@happy-hacker.ml.org with message "subscribe happy-hacker" in the body of your message. To join out chat list, give the message "subscribe hh-chat." These mail lists are maintained by Jesse Brown.
Want to share some kewl stuph with the Happy Hacker list? Correct mistakes? Send your messages to hh@happy-hacker.ml.org. To send me confidential email (please, no discussions of illegal activities) use cmeinel@techbroker.com. Direct flames to dev/null@techbroker.com. Happy hacking!
Copyright 1997 Carolyn P. Meinel. You may forward or post this GUIDE TO (mostly) HARMLESS HACKING on your Web site as long as you leave this notice at the end.

Carolyn Meinel
M/B Research -- The Technology Brokers
http://techbroker.com