A brief history of hacking...

```
bsd 4.11> █
```

zuley clarke / james clawson / maria cordell

november 2003

LCC 6316: Historical Approaches to Digital Media

table of contents

the evolution of hacking

Though it wasn't yet called "hacking," the earliest known incidents of modern technological mischief date from 1878 and the early days of the Bell Telephone Company. Teenage boys hired by Bell as switchboard operators intentionally misdirected and disconnected telephone calls, eavesdropped on conversations, and played a variety of other pranks on unsuspecting customers (Slatalla 1).[1]

first hacks

The first bona fide appearance of a computer hacker occurs nearly 100 years later, in the 1960s. A "hack" has always been a kind of shortcut or modification—a way to bypass or rework the standard operation of an object or system. The term originated with model train enthusiasts at MIT who hacked their train sets in order to modify how they worked. Several of these same model train hackers later applied their curiosity and resourcefulness to the then new computer systems being deployed on the campus (CNN 1). These and other early computer hackers were devout programming enthusiasts, experts primarily interested in modifying programs to optimize them, customize them for specific applications, or just for the fun of learning how things worked. In many cases, the shortcuts and modifications produced by these hackers were even more elegant than the professional programs they replaced or circumvented. In fact, the most elegant—and enduring—hack from this period is the UNIX operating system, developed in the late 1960s by Dennis Ritchie and Keith Thompson of Bell Labs.

The 1970s produced another type of hacker, one focused on telephone systems. Known as "phreakers," these hackers discovered and exploited operational characteristics of the newly all-electronic telephone switching network that enabled them to make long distance calls free of charge. The phreaker movement is an important early example of anti-establishment subculture that spawns influential hackers and visionaries in the realm of the personal computer. [2]

the golden era

Hacking enjoyed a golden era of sorts in the 1980s. The introduction of turnkey "personal" computers by Radio Shack, IBM, Apple, and others is a turning point in hacker history.[3] Now computers were no longer limited to the realms of hardcore hobbyists and business users; anyone, including existing and yet-to-be-realized hackers, could acquire a computer for their own purposes. Modems, devices that enabled computers to communicate with each other over telephone lines, were also more widely available and significantly extended the hacker's reach.

It was just this sort of capability that was explored and popularized in a number of popular books and films at this time, beginning with 1983's movie, *War Games*. The central character, a young, suburban hacker, taps into a remote military computer by dialing into it from home using a personal computer and an acoustic coupler, an early type of modem. *War Games* was followed in 1984 by Steven Levy's publication of *Hackers: Heroes of the Computer Revolution*, in which he details early hacking history and summarizes the hacker credo of this and earlier eras: "Access to computers, and anything that might teach you something about the way the world works, should be unlimited and total."

a split forms

Although hacking expanded and enjoyed glorification during its golden years, a divide was forming within the hacking community by the late 1980s. An increasing number of hackers were no longer satisfied with benign exploration of systems merely to learn how they worked. The hacker principle of "freedom of technology" as described by Levy was changing, and a younger generation interested in individual gain emerged.

[1] Interestingly, this apparently is at least one factor for the Bell Telephone Company's decision to go to an all-female operator workforce early in its operation.

[2] Apple Computer founders Steve Jobs and Steve "Woz" Wozniak got their start by selling phone phreaking devices while still in college.

[3] Personal computers had been available for sometime before this, but they generally required assembly and more intimate hardware knowledge to assemble and maintain. They were also far less widely marketed and distributed.

This new breed of “hacker” directed its knowledge and tenacity toward distinctly criminal pursuits, including the distribution of pirated commercial software, games, and viruses and worms that could virtually shut down systems. The dark side fragmented even further as several groups formed “electronic gangs,” driven to tap into the sensitive information housed within large institutions, like government and educational research centers. As happens with conventional street gangs, it didn’t take long for these groups to begin fighting each other, and the early 1990s saw an escalation of infighting that jammed phone lines and networks, and ultimately led to the demise and criminal prosecution of several groups.

criminalization

Legislators and law enforcement began to get serious about criminalizing and prosecuting these activities in the mid-1980s. Congress passed its first hacking-related legislation, the Federal Computer Fraud and Abuse Act, in 1986. The act made computer tampering a felony crime punishable by significant jail time and monetary fines. By the mid-1990s several high-profile arrests had taken place and signaled the seriousness with which government and businesses were dealing with these activities. Kevin Mitnick, perhaps the best known hacker of this era, was arrested twice, served significant jail time, and was barred from touching a computer for several years after completing his sentence.

the newest frontier

One of the newest forms of hacking involves finding and connecting to unsecured Wireless Access Points (WAPs). Also called “whacking,” the practice has grown with the increasingly widespread use of wireless networks.[4] Whacking capitalizes on the relative ease with which many wireless networks can be accessed (generally because their owners haven’t taken steps to secure them). The wireless nature of these networks makes them easy to find and hack, and because they so often extend Internet access, wireless networks are especially enticing targets for unauthorized use.

the drive to hack

Even though computers and the software systems they run are fundamentally deterministic, their complexity can quickly exceed what their very designers are able to predict or simulate. And as complexity increases, predicting what someone else will be able to do with it increases as well. Any sufficiently complex technology can therefore exhibit unpredictable or surprising results. In part this is what the hacker exploits: using systems in ways that are not specifically part of their design or intended use. The other is the subversive aspect: breaking into systems with ultimately criminal goals, including operational disruption and data theft.

hacker good, cracker bad

Although the term “hacker” is in widespread use, the sense in which it is employed is generally incorrect. Popular media and entertainment providers have long used it to describe anyone who tampers with a system, particularly in connection to criminal activity. This journalistic misuse of the name upset many “traditional” hackers, who responded to the vilification of their good name by offering a new term for these individuals: “crackers.” Crackers are vandals and thieves whose sole purpose is unauthorized “cracking” into secure systems for personal gain.[5]

This darker side of hacking has three main motivations with varying degrees of harm. The most benign cracks are attempts to gain unauthorized access in order to satisfy a personal motive such as curiosity or pride. More malicious cracking seeks to gain unauthorized access in order to tamper with or destroy information. The goal of the most serious and professional crackers is unauthorized access to systems or computer services in order to steal data for criminal purposes. Systems commonly under attack are universities, government agencies, such as the Department of Defense and NASA, and large corporations such as electric

[4] Related practices are “wardriving,” or actively seeking usable WAPs, and “warchalking,” marking WAP locations and access parameters according to a well-defined symbol set, usually drawn in chalk on the street or sidewalk, to enable others to easily find and tap into the access points. For more on the symbol set, see http://www.warchalking.org.

[5] The term “cracker” may have been selected in part to recall “safecracker,” one who breaks into safes in order to steal their contents.

utilities and airlines. Many crackers are professional criminals involved in corporate or government espionage and have links to organized crime.

A relative newcomer to the “hacker” field, script kiddies are another break-off group mistakenly called hackers by the media. A lower form of crackers, script kiddies are not particularly knowledgeable about computer and networking details. Instead, they download ready-made tools to seek out weaknesses on systems accessible via the Internet. They do not target specific information or a specific company but rather scan for opportunities to disrupt and vandalize systems. Most “hackers” and “hacking” events reported on by the popular press are actually of this type.

hacker and cracker profiles

For the traditional hacker, then, hacking is about the thrill of exploration and about the excitement of learning how something works in order to modify or improve it. This generally benign activity is hardly different from that of any other aficionado who wants to learn more about his or her area of interest. It’s about the pursuit of knowledge for its own sake and the ability to create and customize the technological fabric that surrounds us.

For the cracker, everything is about *access* to information, especially if it is sensitive or protected. Moreover, crackers consider their illicit activities badges of honor to be worn with pride. Ironically, although most crackers are thought to live on the fringe of society, many have a tendency to downplay the consequences of their actions and generally rationalize their activities as being for the good of humanity.[6] In another twist, crackers blame their own criminal behavior on their victims, a characteristic found in other criminals (Quittner, Hacker Psych). Research into cracker activity shows that many of these individuals develop a flexible system of ethics in which concern about ramifications of this type of activity are easily discarded.

who cracks?

In the United States, crackers are predominately white, male, and young. Script kiddies and less serious crackers are thought to be between 12 and 30 years old. The primary driving force for these individuals is a combination of curiosity, voyeurism, and entertainment. Others are thought to start out with a benign technological interest but, possibly because of a predisposition for criminality, eventually find their way into shadier pursuits, including cracking and spreading viruses and worms.

Malicious hacking is no longer the sole realm of the young American male, however. Thanks in part to the substantial expansion of Internet access availability throughout the world since the late 1990s and in another to the increasing availability of inexpensive personal computers, crackers from many other parts of the world enjoy the same level of access to a growing pool of enticing targets. Asia and Europe, for example, have long had a significant number of crackers. More recently, Brazil has taken the lead in hacking and cracking activities, with nearly 96,000 overt Internet attacks (those that have been reported and traced) attributed to Brazil for January through September 2003 alone.[7] This high level of activity in Brazil and in other countries, is generally attributed to a lack of legal recourses to control the activity. The “hacker” subculture in Brazil and other countries is also fostered by the wide availability of magazines that glorify cracking and provide “how-to” articles.

Banking systems and U.S.-based companies and government systems appear to remain popular targets for crackers everywhere. In 2003, nearly 72,000 attacks had been recorded against U.S.-based systems; the next most popular target country, Germany, recorded only about 17,000 attacks during the same period.[8]

[6] The early phone phreakers exhibited early example of twisted technological morality when they treated the private telephone network as it if were a public domain resource. Phreakers felt their practices didn’t hurt anyone because phone calls came from an “unlimited reservoir.”

[7] Figures from mi2g (a digital risk consulting firm based in London) via cnet.com article.

[8] Ibid. Data is for January through September 2003.

cultural infiltration

Hacking's influence on popular, and not so popular, culture parallels the rapid growth of both the personal computer industry and the interconnection of personal computers into formalized networks. Society started becoming aware of hackers as computers became increasingly accessible and as computer networks grew in both size (number of terminals) and popularity (number of users) throughout the late seventies and early eighties.

Hacking begins to enter popular culture in the 1980s, when a slew of movies, novels, television commercials, magazines, newsletters, and even academic proceedings dealt with the rising incidence of hacking, cracking, phreaking, computer access, and associated technology. Media and entertainment vehicles in the 1980s also introduced and popularized hacking and the hacker's belief system. The two events credited with doing the most in this area were the release of the movie *War Games*, which depicted the existence of hacking and the potential power associated with it,[9] and the publication of William Gibson's first hacking-related novel, *Neuromancer* (which coined the term "cyberspace") in 1984.

The 1980s began by popularizing and glorifying the notion of the hacker and ended with the criminalization and vilification of the hacker. Hacking's rise to popularity is marked by many technological, and cybercultural markers that surface in the early 1980s, including the releases of the films *Bladerunner*[10] and *Tron* in 1982, the publication of *Cyberpunk*[11] by Bruce Bethke in 1983, Levy's *Hackers: Heroes of the Computer Movement* in 1984 and the release of *The Terminator* in 1984. Later in the decade, the movie *RoboCop*, released in 1987, further popularized the notion of man/technology blends in the form of cyborgs. In 1988, Bruce Sterling's *Islands in the Net* is published, as is William Gibson's *Mona Lisa Overdrive* novel and bOING bOING, a monthly technology/techno-cultural newsletter. The decade closes with the initial publications of *Mondo 2000,* a prominent Southern California technology periodical which bolstered yet again hacking's image, and the 1989 publication of Stoll's *The Cuckoo's Egg*, which casts a bit of a shadow on hacking. *The Cuckoo's Egg*, which traces the pursuit and capture of crackers attempting to break into classified government computer systems, spent over four months on the New York Times best seller list[12] and spawned two television shows, a NOVA special, "The KGB, CIA, Computer and Me," and "Spycatcher," produced in Britain.[13]

It was also during the 1980s that society became sufficiently aware of malicious hacking to begin guarding itself from these activities. After the U.S. Congress passed the first anti-hacking laws in 1986, the Electronic Frontier Foundation, a technology-oriented civil liberties protection group formed in 1990, posed the question, "Is Computer Hacking a Crime?"[14] That question was answered with the launch of the much publicized and largest hacker crackdown in history, Operation Sun Devil[15]. Operation Sun Devil, organized and launched by the United States Secret Service and the Arizona Organized Crime and Racketeering Bureau, was a twelve city hacker crackdown that spanned nine states. By 1992, Bruce Sterling publishes *The Hacker Crackdown*, in which he documents a mounting legal resistance to hackers, provides an in-depth look at several actual hacks, and discusses the civil liberties side of hacking. Sterling's book gives the public yet another glimpse into the underworld of hacking, cracking, and phreaking.[16] The combination of these events publicized the dark side of hacking and raised the public's awareness its consequences.

[9] *War Games* is now considered a cult piece among hackers, as much for its hacking theme as for the antiquated hardware and computer jargon it contains.
[10] Based on the 1968 Phillip K. Dick short story, *Do Androids Dream of Electronic Sheep*.
[11] This is the first use of the term "cyberpunk."
[12] Front cover photo on http://images.amazon.com/images/P/0671726889.01.LZZZZZZZ.gif.
[13] "Spycatcher" is mentioned on http://www.ocf.berkeley.edu/~stoll/nova_show.html.
[14] Harper's Magazine, March 1990.
[15] May 7 – 9, 1990.
[16] See http://www.lysator.liu.se/etexts/hacker/ for an online version of the book.
[17] Released less that a month before the arrest of Kevin Mitnick on February 15, 1995.

The books, films, and television programs of the 1980s also paved a cultural path for the wild speculation, hope, and hype that accompanied the “information superhighway,” the name given to the “Internet” in the early days of its expansion for mass consumption. At this time Hollywood was busy simultaneously romanticizing and criminalizing the hacker and his credo with such movies as *Terminator 2* (1991), *The Lawnmower Man* (1992), *The Net* (1995), *Hackers* (1995),[17] *Johnny Mnemonic* (1995), and *The Matrix* (1999).

Frequent coverage of high-profile “hacking” activity in the popular press during this time alerted computer users to their own susceptibility to attack. Users gradually began to realize that connecting an unprotected computer to the Internet was an open and enticing invitation for hackers to invade private files and financial lives. While personal computer sales increased dramatically in the 1990s, so did demand for tools to protect personal computers against the threat of malicious hackers.

Meanwhile, traditional hackers found a receptive medium for their messages about the free flow of information and antigovernment/anticorporate ideals in publications like *Mondo 2000* and *Wired*, the self-proclaimed monthly digest of all things technologically hip. By the late 1990s hacking had come full circle and was the subject of scholarly research and discussion. Major colleges and universities began teaching and establishing programs of study focused on cyberculture, digital culture, technofuturist and cyberpunk literature, the cyberpunk subculture, and online and virtual communities, and cyber security.

The hacker mystique has continuously grown and evolved since its early days as a benign activity carried out within obscure computer labs in the 1960s. Participants have played many different roles and have been popularized through many mediums. They have been everything from computer tourists and network voyeurs to dangerous criminals and nihilist anarchists; from computer nerds to cyberpunks; from public nuisance to catalysts for technology advancement. No matter how much new legislation passes or how many new security roadblocks are devised, hacking will be practiced as long as computers and technology-driven communication systems are with us.

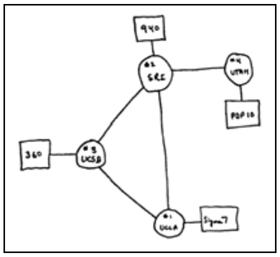
event timeline

1878 Teenage boys mischievously misdirect and disconnect telephone calls at Bell Telephone Company

1960 The term “hacker” is used by MIT train enthusiasts who hacked their train sets to change how they work. Later, these same enthusiasts emerge as the first computer hackers

1968 Dennis Ritchie and Keith Thompson develop the UNIX operating system, possibly the most elegant hack of all time

1969 The Advanced Research Projects Agency (ARPA) launches the first four nodes of ARPANET (the system that eventually morphs into the Internet) at UCLA, Santa Barbara, University of Utah, and Stanford



ARPANET 1969

1970 Phreakers, another type of hacker, exploits the newly all-electronic telephone network to make free long distance calls

Phreaker John Draper in 1970s

1971 Ray Tomlinson writes the first email program and uses it on ARPANET (now at 64 nodes)

1975 Bill Gates and Paul Allen form Microsoft

1976 Stephen Wozniak, Steve Jobs, and Ron Wayne form Apple Computer

1978 Randy Seuss and Ward Christiansen create first personal computer bulletin board system, still in operation today

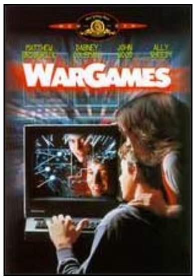
1980 Usenet is created by networking UNIX machines via telephone

1981 Ian Murphy is the first hacker tried and convicted as a felon

1983 ARPANET splits into military and civilian sectors; the civilian sector later evolves into the present-day Internet

The film *War Games* popularizes hacking

Richard Stallman makes the first GNU announcement via Usenet

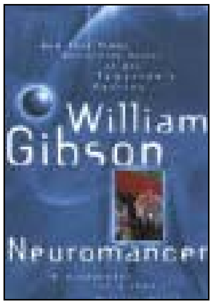


The film *War Games* released in 1983

1984 William Gibson coins the term “cyberspace” in his novel *Neuromancer*, the first hacking-related novel

The most famous hacker group, Legion of Doom, is formed

Steven Levy publishes *Hackers: Heroes of the Computer Revolution*, which summarizes the hacker credo of “freedom of technology”



Gibson’s *Neuromancer* published 1984

1986 The US Congress passes the Computer Fraud and Abuse Act, the first hacking-related legislation

A small accounting error alerts astronomer and computer manager Cliff Stoll to the presence of hackers using his computer system; a year-long investigation results in the arrests of five German hackers, and Stoll later recounts the events in his book, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*

Stoll publishes his account of tracking a hacker across multiple computer systems and countries

1988 Robert T. Morris, Jr. launches the first self-replicating worm on the government's ARPANET to test its effect on UNIX systems; he is the first person to be convicted under the Computer Fraud Act of 1986

1989 Herbert Zinn is the first juvenile convicted under the Computer Fraud Act

1990 The Electronic Frontier Foundation is formed, in part to defend the rights of those investigated for hacking

The United States Secret Service and the Arizona Organized Crime and Racketeering Bureau implement Operation Sun Devil, a twelve city multi-state crackdown and the largest hacker raid to date

Electronic Frontier Foundation founded 1990

1991 The federal ban barring business from the Internet is lifted

Justin Petersen, arrested three months earlier for hacking, is released from prison to help the FBI track hacker Kevin Mitnick

Linus Torvalds publicly releases Linux version 0.01

1992 Mark Abene (aka "Phiber Optik") and other members of the Masters of Deception, a gang of phreakers, are arrested from evidence obtained from wiretaps.

Mark Abene of Masters of Deception arrested 1992

1995 Kevin Mitnick, probably the world's most prolific and best known hacker, is arrested and charged with obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers, and educational institutions; and stealing, copying, and misappropriating proprietary computer software from Motorola, Fujitsu, Nokia, Sun, Novell, and NEC. Mitnick was also in possession of 20,000 credit card numbers.

Christopher Pile is the first person jailed for writing and distributing a computer virus.

WANTED

BY U.S. MARSHALS

Mitnick's Wanted Poster

1997 AOHell, a freeware application that allows script kiddies to wreak havoc on AOL, is released

1998 Two hackers, Hao Jinglong and Hao Jingwen (twin brothers) are sentenced to death by a court in China for stealing ~$87,000 from a bank in China; Hau Jingwen's sentence was upheld, while Hao Jinglong was acquitted in return for further testimony

1999 Napster begins to gain popularity; created by Shawn Fanning and Sean Parker (ages 19 and 20 at the time), Napster attracts 65 million registered users before being shut down in July of 2001

bibliography

All Movie Guide. Various entries. Online. <http://www.allmovie.com>.

CNN.com. “Timeline: A 40-year History of Hacking.” Online. 22 Oct. 2003. <http://www.cnn.com/2001/TECH/internet/11/19/hack.history.idg/?related>.

Levy, Steven. Hacking: Heroes of the Computer Revolution. Garden City, N.Y.: Anchor/Doubleday, 1984.

Slatalla, Michelle. A Brief History of Hacking. Online. Discovery Communications, 28 Oct. 2003. <http://tlc.discovery.com/convergence/hackers/articles/history.html>.

Stallman, Richard. “The GNU Manifesto.” The New Media Reader. Eds. Noah Wardrip-Fruin and Nick Monfort. Cambridge: MIT Press, 2003.

Sterling, Bruce. Encyclopædia Britannica. 2003. Encyclopædia Britannica Premium Service. 28 Oct, 2003 <http://www.britannica.com/eb/article?eu=102011>.

Stoll, Cliff. The Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage. New York: Doubleday, 1989.

Quinlan, Heather. Cyber Terrorism. Online. Discovery Communications. 28 Oct. 2003. < http://tlc.discovery.com/convergence/hackers/articles/cyberterror.html>

Quittner, Jeremy. Hacker Psych 101. Online. Discovery Communications. 28 Oct. 2003. <http://tlc.discovery.com/convergence/hackers/articles/psych.html>.

- - -. Hackers: Methods of Attack and Defense. Online. Discovery Communications. 28 Oct. 2003. <http://tlc.discovery.com/convergence/hackers/articles/method.html>.