machine. This guaranteed its success in the emerging hacker community.

When in the early 1980s IBM started a program to build its own personal computer, they decided to buy the operating system from an outside source rather than develop their own. IBM representatives visited Digital Research to investigate CP/M, but apparently Kildall did not agree to certain demands. IBM turned instead to **Microsoft**, which in turn bought QDOS from Seattle Computer Products and turned it into PC-DOS and MS-DOS. Ironically, QDOS (Quick and Dirty Operating System) had been written by Tim Paterson as a clone of CP/M for 16-bit machines. The partnership with IBM turned Microsoft's **DOS** into the dominating operating system of the 1980s, while Digital Research lost ground. The company was later acquired by Novell and then Caldera. CP/M later evolved into 16-bit versions for different processors and even a version for the IBM PC, but in the 16-bit world it never had the dominance that it once had in the eight-bit arena.

FURTHER READING

Cringely, Robert X. *Accidental Empires: How the Boys of Silicon Valley Make Their Millions, Battle Foreign Competition, and Still Can't Get a Date.* New York: Harper Business, 1996.

Erickson, Jonathan. "Dr. Dobb's Journal: Excellence in Programming Awards." *Dr. Dobb's Journal,* May 1997, p. 18.

Swaine, Michael. "Gary Kildall and Collegial Entrepreneurship." *Dr. Dobb's Special Report,* Spring 1997.

—*Raúl Rojas*

CPU See Central Processing Unit.

Cracker

A cracker is a person who breaks into a computer system by appropriating passwords from registered users or by bypassing the log-in process altogether. Related to the more common term **hacker**, cracker was coined by programmers who are proud of being hackers in the good sense of the word and who do not want to be associated with illegal break-ins. The press, however, misleadingly refers regularly to persons who break into computer systems as hackers.

Crackers usually exploit little-known security holes in operating systems. For example, the Internet Worm, which was set on the loose in 1988 by Robert Morris, a student at Cornell University, exploited a nondocumented feature of the **electronic mail** handling utility, **Sendmail**. Through this security hole he could appropriate passwords of sites and continue sending the Worm to other sites. Cracking into a system does not involve superior programming capabilities, only perseverance at trying all known security holes. Crackers usually leave a **back door** in systems they have cracked in order to visit them later, maybe months after the initial break-in.

Related to cracking is *phreaking*, which describes the act of breaking into the telephone system and manipulating the telephone signals in order to, for example, make free long-distance calls. This was a respectable activity among electronic hobbyists in the 1970s; for example, **Steve Jobs** (1955–) and **Steve Wozniak** (1950–), the future founders of **Apple Computer**, sold so-called "blue boxes" for this purpose. Phreaking was even advocated by some U.S. political activists as a method of protesting the Vietnam War.

That was not the only time that crackers have been involved in politics. A classic case was that of some German crackers who were paid by the Soviet KGB to steal documents from computers in the United States. Clifford Stoll, a system manager for the computer at Lawrence Berkeley Laboratory, noticed a 75-cent deficit in the computer accounts. The error was due to inconsistencies in the accounting file caused by a cracker who had broken into the system and altered the file to conceal his tracks. Stoll managed to identify the account that the cracker was using and could later observe all his keystrokes on a screen. Noticing that the cracker was interested in military information about the SDI program of the Reagan administration, one day he lured the cracker into maintaining his network connection for a long time in order to copy files that were used as decoy. The cracker took the bait, and his connection was eventually traced back to Hannover, Germany, where the police caught him and his collaborators. Stoll has told the story of the discovery of the cracker ring and how they get caught in *The Cuckoo's Egg*.

It should not be surprising that the militaries are interested in techniques for breaking into computer systems, and not only for defensive reasons. In 1994 the School for Information Warfare and Strategy was founded at the National Defense University in the United States. When a cracker is paid to break into computers of political parties or other companies, he or she is referred to as a *samurai*.

As dependence on computer networks has increased, so has interest in programs that can thwart crackers. The release of anticracker software SATAN (Security Tool for Analyzing Networks) received large amounts of media attention in 1995. SATAN is a utility for automatically testing and detection of the security holes in computer systems usually exploited by crackers. There was speculation at the time that SATAN could also be used by crackers to find security holes and that it would increase the number of illegal break-ins, but the creators of SATAN (Wietse Venema and Dan Farmer) argued that this tool would, on the contrary, make system administrators aware of security problems. The day the package was released, so many Internet users tried to download SATAN that the connection to the sites distributing the software almost broke down. The availability of SATAN has not led to an increase in cracking, as some had feared.

FURTHER READING

Hafner, Katie, and John Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster, 1995.

Stoll, Clifford. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Pocket Books, 2000.

Schwartau, Winn, ed. *Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age*. New York: Thunder Press, 1996.

—Raúl Rojas

Cray 1

Introduced in 1976, the Cray 1 vector computer represented such a marked increase in performance over other machines of its era that it defined the term *supercomputer* for many years thereafter. It was designed by **Seymour Cray** (1925–96) following his departure from **Control Data Corporation** (CDC), as the first product of **Cray Research**. It can be considered the successor to the CDC 6600 and CDC 7600, also developed by Seymour Cray.

The Cray-1 was a physically impressive and demanding piece of equipment. It weighed 5 tons, not counting the motor-generators and external heat-exchange apparatus. Its power requirement was over 100 kilowatts and Freon refrigeration was used to remove the enormous amount of heat produced by its emitter-coupled logic (ECL) circuits. At the time, ECL was faster than complementary metal-oxide-semiconductor (CMOS) technology and several times faster than transistor–transistor logic (TTL). Low-scale integration was used, with circuits supplied by **Fairchild Semiconductor** and **Motorola**. Only four distinct chip types were used in the machine.

The clock speed, 80 megahertz (MHz), does not seem high by present-day microprocessor standards, but it was a technical achievement because the physical size of the processor was about 2 meters. The wire lengths play a significant role in the clock timing and the interaction with the ECL, so it was the first computer designed with close attention to speed-of-light limitations. The machine backplane was hand-wired and contained about 8 kilometers of wiring.

The logic and memory were arranged in a C shape, with power supplies around the base of the C concealed under the "seats." Plumbing and power cables were routed through the floor. The Cray 1 itself was silent in operation. Motor-generators supplied power from a distance away, adding to the already considerable facility requirements for maintaining operation of the Cray 1. The motor-generators were necessary to supply the very stable power demanded by the computer.

The memory of the Cray 1 was static, or bipolar memory. Since static memory requires five transistors per bit, compared with one transistor per bit for (slower) dynamic memory, it was much more expensive than conventional designs. Depending on memory configuration, the price of the Cray 1 when initially marketed was about U.S.$10 million. Additional memory was priced at about U.S.$1 million per megaword.

Like its CDC 7600 predecessor, the Cray 1 had separate functional units for **floating-point** addition, float-