

the Internet Society (ISOC) and the Internet Assigned Numbers Authority (IANA) to provide a new structure, free enterprise, and competition to the **domain name system** (DNS) when the monopoly on .com, .org and .net was due to end in 1998. CORE was created in October 1997 and is based in Geneva, Switzerland.

In October 1998, the U.S. Department of Commerce (DoC) and the private company Network Solutions, Inc. (NSI) amended their cooperative agreement, under which NSI had been the sole registrar and administrator for top-level domains “.com,” “.net,” and “.org.” (The other top-level domains, “.gov,” “.mil,” and “.edu,” are reserved for government, military, and educational bodies only.) In November 1998, the DoC identified the **Internet Corporation for Assigned Names and Numbers** (ICANN) as the entity that would oversee the transition to competition under the Shared Registration System (SRS). Part of ICANN's responsibilities included establishing and implementing a procedure for registrar accreditation that would ensure a transition to a registration system that would introduce competition to domain names while ensuring Internet stability and domain-name durability.

On 4 March 1999, the ICANN Board of Directors adopted a Statement of Registrar Accreditation Policy. Between 11 March and 8 April 1999, ICANN accepted applications from entities seeking accreditation to participate as one of the five domain-name registrars in the SRS Testbed Program. The five testbed selected registrars were **America Online**, CORE, France Telecom/Oléane, Melbourne IT, and register.com.

Since 8 April 1999, ICANN has continued to accept applications for registrar accreditation for the post-testbed period of the SRS and has accredited over 90 businesses in addition to the original five testbed program participants. Many of these new registrars were allowed to participate in the final months of the testbed program, and some of them have joined CORE since then.

CORE has more than 60 members in some 20 countries in four continents. To register domains, CORE members compete in an open environment. There are no territorial assignments: Customers can freely choose the CORE member with whom they want to do business. Moreover, after registering a name, the registrant can change the CORE member.

#### FURTHER READING

Moschovitis, Christos J. P., Hilary Poole, Tami Schuyler, and Theresa M. Senft. *History of the Internet: A Chronology, 1843 to the Present*. Santa Barbara, Calif.: ABC-CLIO, 1999.

—*Manuel Sanromà*

## CP/M

**CP/M** (Control Program for Microcomputers) is an **operating system** for 8-bit computers developed by **Gary Kildall** (1942–94) while working at the Naval Postgraduate School in Monterey, California.

In 1972, Kildall saw an advertisement describing the first **microprocessor**, the 4004 chip built by **Intel**. He bought one for U.S.\$25 and started experimenting with it. He soon moved up to the new Intel 8008 processor and wrote several programs, which he also used for his computing classes. Looking for a safe way to store his programs, Kildall connected a hard disk drive to his small computer and wrote the software to control it. The result was a disk operating system which Kildall called CP/M. He offered Intel the software for U.S.\$20,000, but Intel declined, because at the time there was no market for microcomputers. Kildall then decided to start his own company, Intergalactic Digital Research Inc. (later shortened to Digital Research).

CP/M was a remarkable operating system for its reduced size. It allowed a programmer to store files in floppies or on the hard disk, view directories, and edit and start the programs. It was much more comfortable than anything else available for microcomputers at the time, which still stored programs in audiotapes or used hexadecimal keyboards. CP/M had a set of commands very similar to the ones used later in DOS, the operating system for the **IBM PC**, or those used in the Decsystem-10 time-sharing system of **Digital Equipment Corporation**.

One important feature of CP/M was its expandability. There was a clean interface to the operating system that allowed programmers to write their own code and link it to the rest of the system. Since CP/M also included an assembler and editor, the programmer could start working with the system right away. It was possible to add new peripherals as they became available. CP/M gave the user total control of the

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

Cringley, 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*.