United States Patent [19]

Chandra et al.

[11] **Patent Number: 4,817,140**

[45] **Date of Patent: Mar. 28, 1989**

[54] **SOFTWARE PROTECTION SYSTEM USING A SINGLE-KEY CRYPTOSYSTEM, A HARDWARE-BASED AUTHORIZATION SYSTEM AND A SECURE COPROCESSOR**

[75] Inventors: **Ashileshwari N. Chandra,** Mahopac; **Liam D. Comerford,** Carmel; **Steve R. White,** New York, all of N.Y.

[73] Assignee: **International Business Machines Corp.,** Armonk, N.Y.

[21] Appl. No.: **927,629**

[22] Filed: **Nov. 5, 1986**

[51] **Int. Cl.**[4] **H04L 9/00**

[52] **U.S. Cl.** **380/4;** 380/25

[58] **Field of Search** 364/200, 900; 380/4, 380/25, 23

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,996,449	12/1976	Attanasio	235/61.7 R
4,104,721	8/1978	Markstein	364/200
4,120,030	10/1978	Johnstone	364/200
4,168,396	9/1979	Best	178/22
4,183,085	1/1980	Roberts	364/200
4,246,638	1/1981	Thomas	364/200
4,278,837	7/1981	Best	178/22.09
4,433,207	2/1984	Best	178/22.09
4,442,484	4/1984	Childs, Jr.	364/200
4,446,519	5/1984	Thomas	364/300
4,458,315	7/1984	Uchenick	364/200
4,462,078	7/1984	Ross	364/300
4,465,901	8/1984	Best	178/22.08
4,471,163	9/1984	Donald et al.	364/200
4,471,216	9/1984	Herve	235/380
4,513,174	4/1985	Herman	178/22.08
4,523,271	6/1985	Levien	364/200
4,525,599	6/1985	Curran et al.	364/200
4,558,176	12/1985	Arnold et al.	178/22.08
4,562,305	12/1985	Gaffney, Jr.	178/22.08
4,562,306	12/1985	Chou	178/22.08

(List continued on next page.)

OTHER PUBLICATIONS

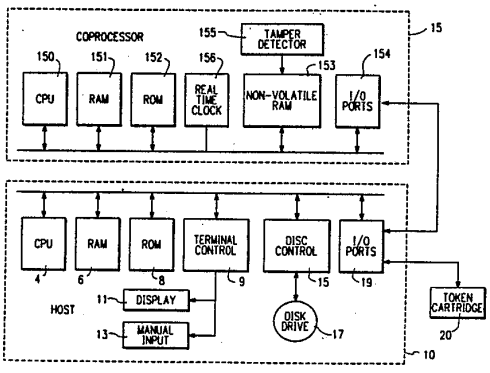
Best, Preventing Software Piracy with Crypto-Microprocessors, IEEE, 1980.

(List continued on next page.)

[57] **ABSTRACT**

The invention provides a software asset protection mechanism which is based on the separation of the software to be protected from the right to execute that software. Protected software can only be executed on composite computing systems in which a physically and logically secure coprocessor is associated with a host computer. The software to be protected is broken down into a protected (encrypted) portion and an (optional) unprotected or plain text portion. The software is distributed by any conventional software distribution mechanism (for example a floppy disk) including the files already identified along with an encrypted software decryption key. The coprocessor is capable of decrypting the software decryption key so it can thereafter decrypt the software, for execution purposes. However, the coprocessor will not perform these functions unless and until the user's right to execute is evidenced by presentation of a physically secure token. The physically secure token provides to the coprocessor token data in plain text form (the physical security of the plain text token data is provided by the cartridge within which token data is stored). The physical properties of that cartridge taken together with the correspondence between the token data provided by the cartridge and the encrypted token data evidence the user's right to execute. While the coprocessor can, thereafter, decrypt and execute the protected portion of the software, access to that software is denied the user by the physical and logical features of the coprocessor. Other properties of the cartridge (specifically a destructive read property) ensure that the act of transferring token data to the coprocessor obliterates that data from the cartridge so it cannot be revised. Further, the protocol for the coprocessor/cartridge exchange is arranged so that observation of even the entire exchange provides inadequate information with which to simulate or spoof the effect of an authentic, unused cartridge.

35 Claims, 8 Drawing Sheets



U.S. PATENT DOCUMENTS

4,577,289	3/1986	Comerford	364/900
4,598,288	7/1986	Yarbrough	340/825.34
4,599,489	7/1986	Cargile	178/22.08
4,609,777	9/1986	Cargile	178/22.08
4,609,985	9/1986	Dozier	364/200
4,621,321	11/1986	Boebert et al.	364/200
4,621,334	11/1986	Garcia	364/550
4,633,388	12/1986	Chiu	364/200
4,644,493	2/1987	Chandra et al.	364/900
4,652,990	3/1987	Pailen et al.	364/200

OTHER PUBLICATIONS

Everett, "Padlock", Computer Bulletin, Mar. 1985, pp. 16–17 + Padlock Public Key Software Protection System.

Goldschmitt, "Thou Shall Not Dupe", Computerworld, Jan. 28, 1985.

Herzberg, "Public Protection of Software", Lecture Notes in Computer Science, vol. 218, 1986 (Proc. Crypto 85), pp. 158–178.

Kent, Protecting Externally Supplied Software in Small Computers, Phd. thesis, M.I.T., Sep. 1980.

Lipson, "Little Black Box 'Blocks' Illicit Software Copying", Stamford Advocate, Sep. 14, 1986, pp. E1–E2.

Maude, "Hardware Protection Against Software Piracy", Communications of the ACM, vol. 27, No. 9, Sep. 1984, pp. 950–959.

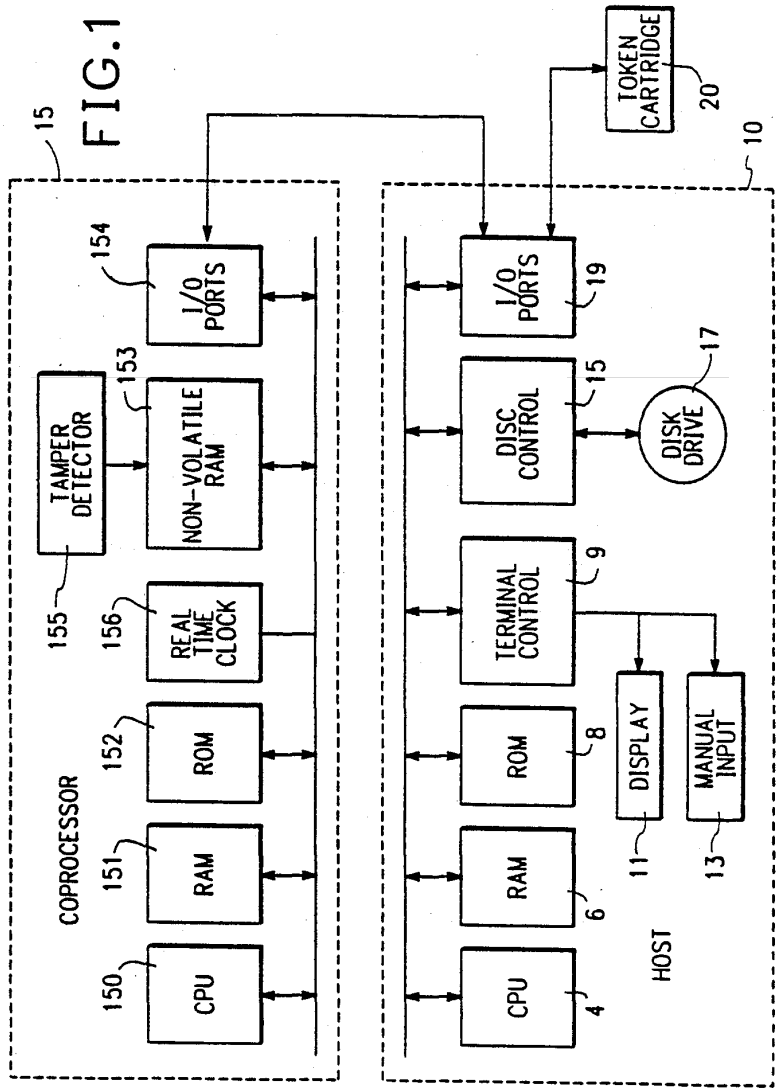
Purdy, "A Software Protection Scheme", IEEE, 1982.

Simmons, "How to (Selectively) Broadcast a Secret", IEEE, 1985.

Winslow, "For Software Firms, Questions is How to Cope with Piracy", Wall Street Journal, Apr. 12, 1985.

Primary Examiner—Gareth D. Shaw
Assistant Examiner—John G. Mills
Attorney, Agent, or Firm—Pollock, Vande Sande & Priddy

FIG. 1



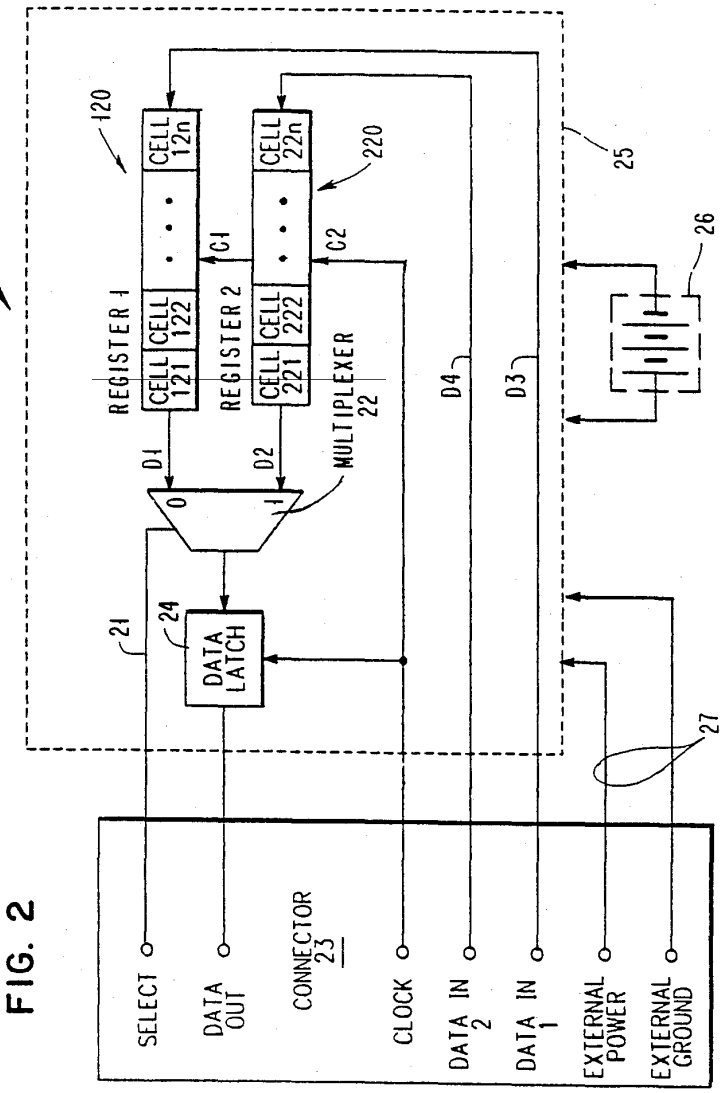


FIG. 2

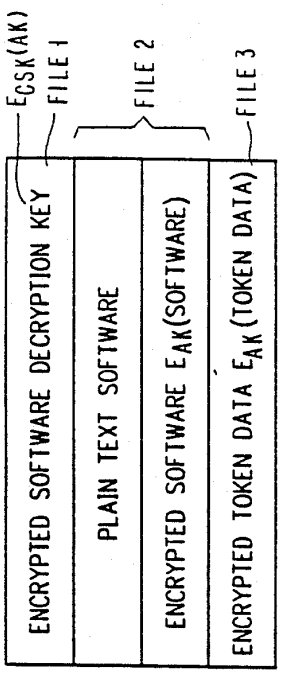


FIG.3

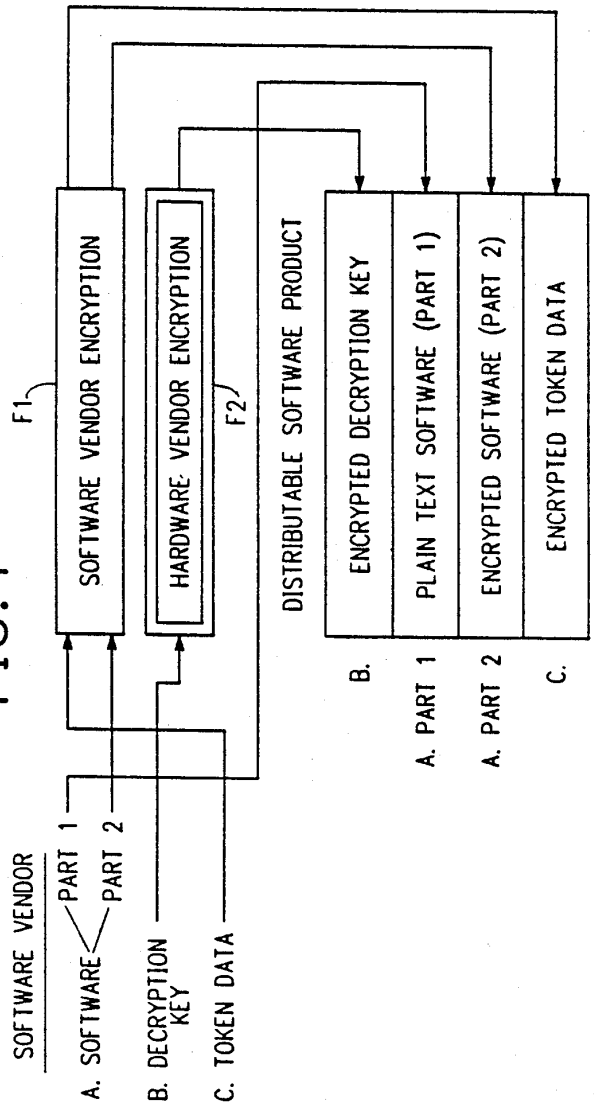


FIG.4

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.