United States Patent [19]

Bosen et al.

[11] **Patent Number:** **5,060,263**

[45] **Date of Patent:** **Oct. 22, 1991**

[54] **COMPUTER ACCESS CONTROL SYSTEM AND METHOD**

[75] Inventors: **Robert J. Bosen**, Pittsburg; **John R. Muir**, Antioch, both of Calif.

[73] Assignee: **Enigma Logic, Inc.**, Concord, Calif.

[21] Appl. No.: **165,868**

[22] Filed: **Mar. 9, 1988**

[51] Int. Cl.⁵ H04L 9/00

[52] U.S. Cl. 380/25; 380/23; 340/825.31

[58] **Field of Search** 364/918.7, 943.7, 949.7, 364/922.5, 222.5, 260.6, 225.2; 340/825.31, 825.34, 825.56, 825.3; 235/382, 382.5, 380; 380/23, 24, 25

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,310,720	1/1982	Check	340/825.31
4,396,914	8/1983	Aston	340/825.31
4,697,072	9/1987	Kawana	235/380
4,847,614	7/1989	Keller	340/825.31

FOREIGN PATENT DOCUMENTS

8503785	8/1985	PCT Int'l Appl.	340/825.31
0225010	6/1987	United Kingdom	380/23

Primary Examiner—Thomas H. Tarcza
Assistant Examiner—David Cain

Attorney, Agent, or Firm—Flehr, Hohbach, Test, Albritton & Herbert

[57] **ABSTRACT**

An access control system is disclosed in which protected systems and corresponding portable password issuing devices both generate new authentic passwords by successively encrypting a stored password with a selected sequence of predefined encryption steps. The protected system generates and displays one or more random digits, selects an encryption sequence by appending the random digits to the user's personal identification number, and generates an authentic password by sequentially encrypting the user's previous password with encryption steps corresponding to each of the digits in the selected encryption sequence. The user generates a purported password by entering his PIN and the displayed random number(s) on the keyboard of his password issuing device, which responds to encrypting a stored previous password value with encryption steps corresponding to the user's keystrokes, and displaying a new password on its display. The user submits his purported new password to the protected system, and the protected system enables access to the protected system when the purported password matches the internally generated authentic password. Each password issuing device can store and generate passwords for a multiplicity of distinct protected host systems.

25 Claims, 8 Drawing Sheets

PROTECTED COMPUTER SYSTEM 22

STORED PROGRAMS 30 STORED DATA

PROTECTED PROGRAMS 40

PROTECTED DATA

UNPROTECTED PROGRAMS

42

ACCESS CONTROL PROGRAM UNPROTECTED DATA

44

PROCESSOR(S)

32 34

I/O MEANS

(E. G., KEYBOARD AND DISPLAY)

20

PASSWORD ISSUING DEVICE

PASSWORD DISPLAY 26

KEYBOARD

24

ADDITIONAL PASSWORD ISSUING DEVICES
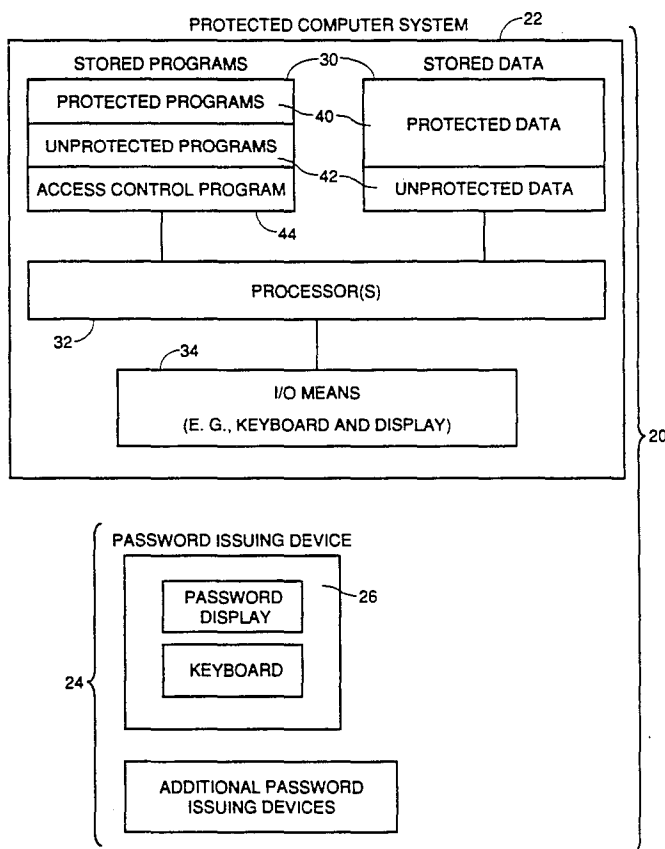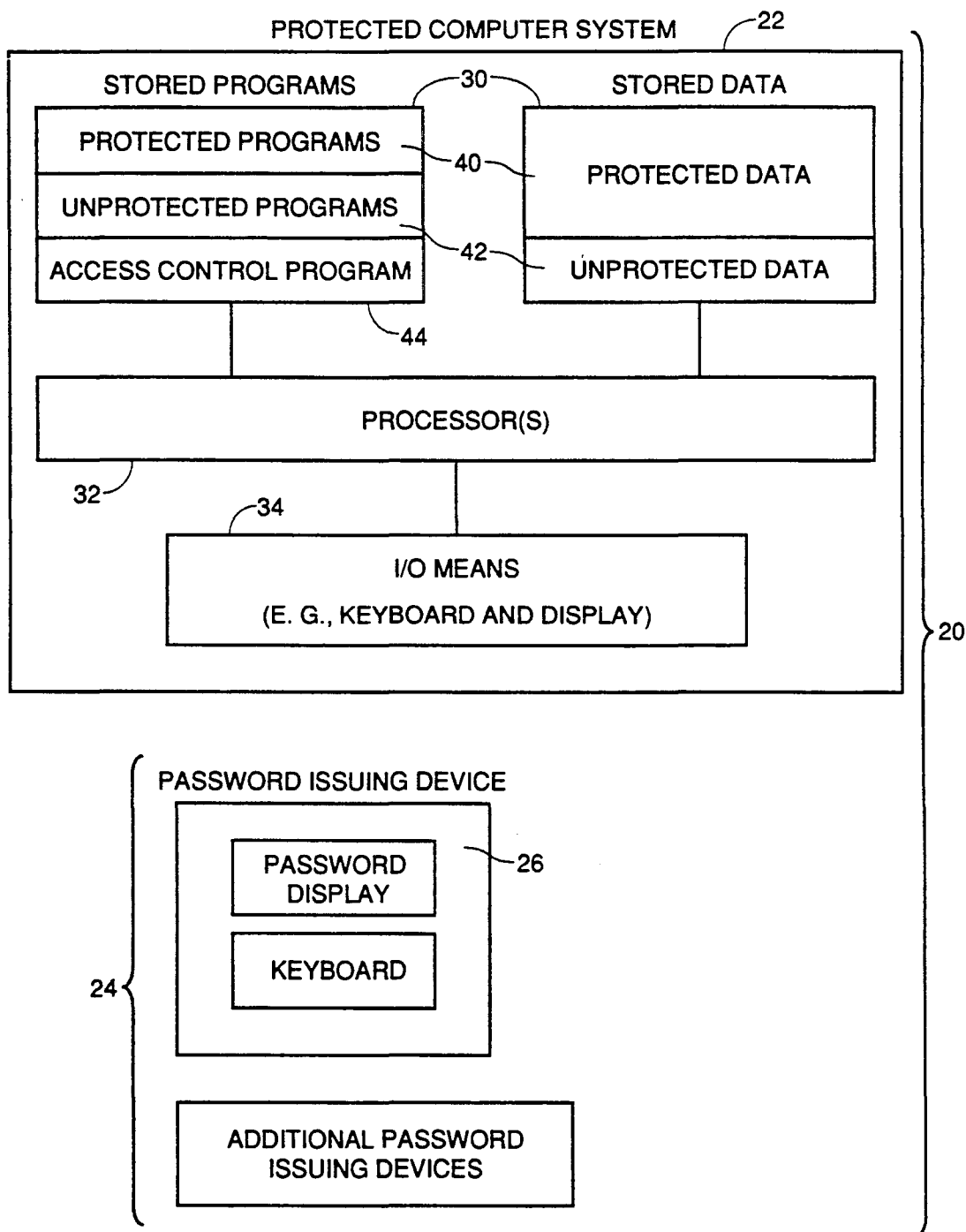
FIGURE 1

	PASSWORD	PIN	LIMITATIONS ON AUTHORIZED ACCESS	DES KEYS 0-9
USER 0	PASSWORD 0	PIN 0	SPECIFIED LIMITS: 0	DES KEYS FOR 0
USER 1	PASSWORD 1	PIN 1	SPECIFIED LIMITS: 1	DES KEYS FOR 1
USER 2	PASSWORD 2	PIN 2	SPECIFIED LIMITS: 2	DES KEYS FOR 2
USER 3	PASSWORD 3	PIN 3	SPECIFIED LIMITS: 3	DES KEYS FOR 3
USER N	PASSWORD N	PIN N	SPECIFIED LIMITS: N	DES KEYS FOR N

50⌐   52⌐

FIGURE 2

60 — ACCESS REQUEST BY USER
(INCLUDES USER'S ID)

62 — GENERATE ENCRYPTION SEQUENCE
K1, K2, K3 ... KN
= USER'S PIN + RANDOM CHALLENGE

64 — GENERATE NEW AUTHENTIC PASSWORD A_u :

$$X_1 = DES_{K1} \quad (PREVIOUS\ PASSWORD)$$
$$X_2 = DES_{K2} \quad (X_1)$$
$$X_3 = DES_{K3} \quad (X_2)$$
$$X_4 = DES_{K4} \quad (X_3)$$
$$X_5 = DES_{K5} \quad (X_4)$$
$$\vdots$$
$$A_u = DES_{KN} \quad (X_{N-1})$$

66 — DISPLAY CHALLENGE

68 — (A) USER ENTERS PURPORTED PASSWORD P_p

70 — COMPARE P_p WITH A_u

MATCH

NO MATCH

72 — PERMIT ACCESS TO SYSTEM
USING SPECIFIED LIMITS,
AND REPLACE STORED PASSWORD
WITH A_u

74 — DISPLAY: INCORRECT

NUMBER OF TRIES N:

76 — N=1
GENERATE NEW A_u
AND DISPLAY NEW
CHALLENGE

(A)

N=2
GENERATE NEW A_u USING
RESYCHRONIZATION
CHALLENGE, AND
DISPLAY RESYCHRONIZATION
CHALLENGE

78
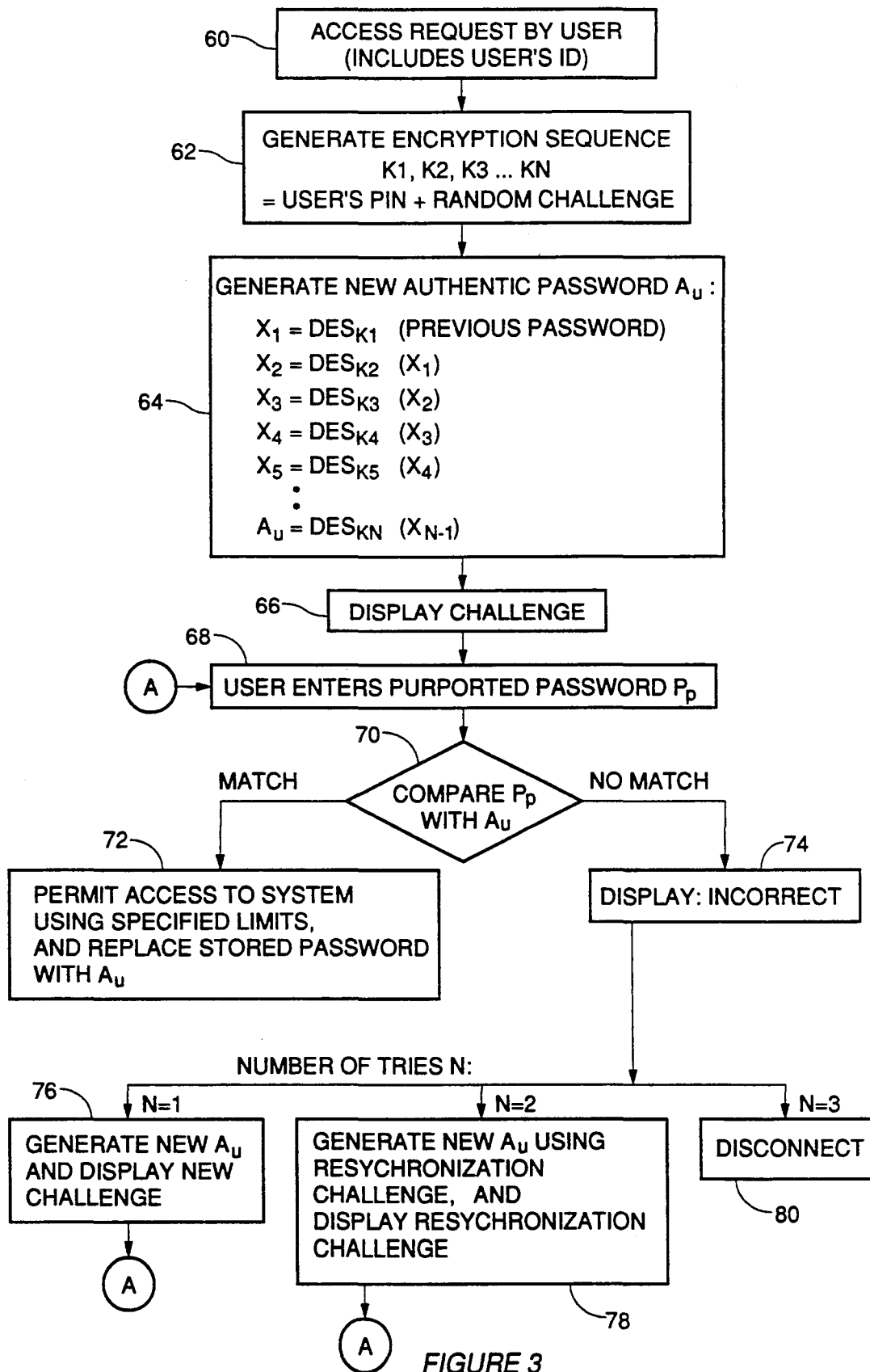
(A)

N=3
DISCONNECT

80

FIGURE 3

FIGURE 4

FIGURE 5

DOCKET ALARM
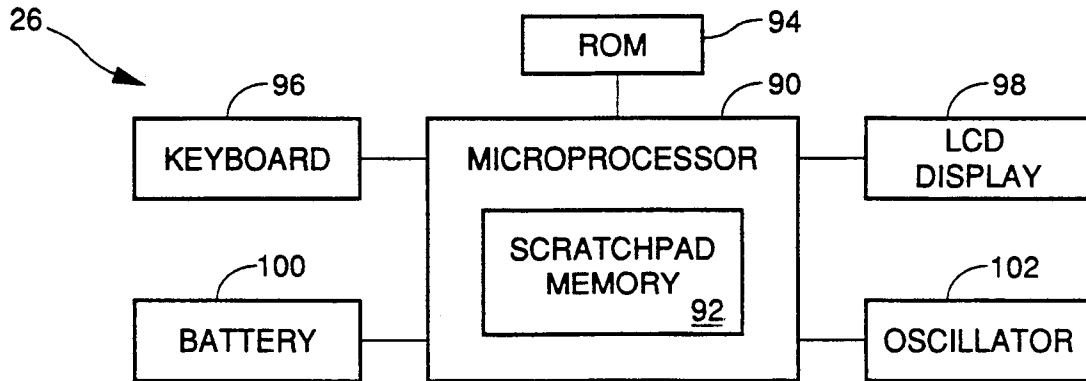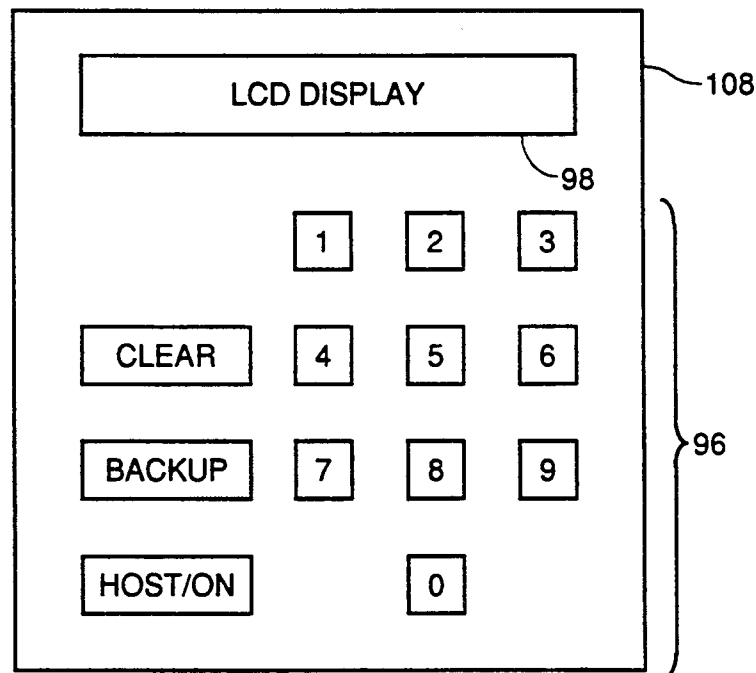
Explore Litigation Insights

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.