US005168520A

United States Patent [19]

Weiss

[11] Patent Number: 5,168,520

[45] Date of Patent: * Dec. 1, 1992

[54] **METHOD AND APPARATUS FOR PERSONAL IDENTIFICATION**

[75] Inventor: **Kenneth P. Weiss**, Newton, Mass.

[73] Assignee: **Security Dynamics Technologies, Inc.**, Cambridge, Mass.

[*] Notice: The portion of the term of this patent subsequent to Jun. 11, 2008 has been disclaimed.

[21] Appl. No.: **670,705**

[22] Filed: **Mar. 18, 1991**

Related U.S. Application Data

[63] Continuation-in-part of Ser. No. 341,932, Apr. 21, 1989, Pat. No. 5,023,908, which is a continuation-in-part of Ser. No. 802,579, Nov. 27, 1985, Pat. No. 4,885,778, which is a continuation-in-part of Ser. No. 676,626, Nov. 30, 1984, Pat. No. 4,720,860.

[51] **Int. Cl.**[5] **H04L 9/32**

[52] **U.S. Cl.** **380/23**; 380/24; 380/25; 380/49; 340/825.31; 340/825.34; 235/379; 235/380; 235/382

[58] **Field of Search** 380/3, 4, 23, 24, 25, 380/49, 50; 235/379, 380, 382; 340/825.31, 825.34

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,764,742	10/1973	Abbott et al.	380/23
3,806,874	4/1974	Ehrat	380/23
3,886,451	5/1975	Chu et al.	368/118
3,900,867	8/1975	Wagner	342/45
3,995,111	11/1976	Tsuji et al.	375/109
4,104,694	8/1978	Hargrove	361/172
4,126,761	11/1978	Graupe et al.	380/28
4,145,568	3/1979	Ehrat	380/47
4,185,166	1/1980	Kinch, Jr. et al.	380/43
4,193,073	3/1980	Kohnen	342/56
4,277,837	7/1981	Stuckert	364/900
4,295,039	10/1981	Stuckert	235/380
4,302,810	11/1981	Bouricius et al.	380/24
4,320,387	3/1982	Powell	340/825.34
4,326,098	4/1982	Bouricius et al.	380/25
4,471,216	9/1984	Herve	235/380
4,494,211	1/1985	Schwartz	375/107
4,509,093	4/1985	Stellberger	361/172
4,536,647	8/1985	Atalla et al.	380/24
4,543,657	9/1985	Wilkinson	375/1
4,578,530	3/1986	Zeidler	380/24
4,582,434	4/1986	Plangger et al.	368/46

(List continued on next page.)

OTHER PUBLICATIONS

"PFX Identity Authentication System", Brochure; Sytek, Inc. of Mountain View, Calif.; no date.

McLellan, "The Future of Data Security Looks Credit-Card Thin", Information Week, (Oct. 7, 1985, pp. 24–30).

"Watchword Generator RG500", Brochure; Racal--Guardata; Bulletin RG500, Apr. 1989.

IBM Tech. Discl. Bull., (vol. 26; No. 7A, Dec. 1983, p. 3293).

IBM Tech. Discl. Bull., (vol. 26; No. 7A, Dec. 1983, pp. 3286–3288).

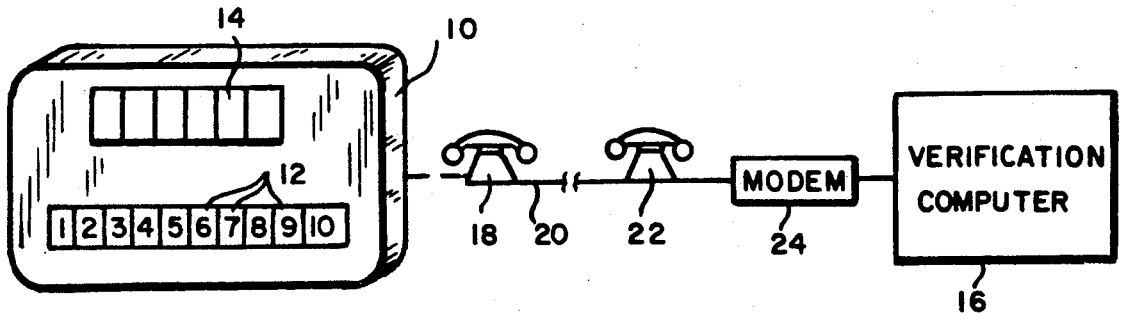
Primary Examiner—Bernarr E. Gregory

Attorney, Agent, or Firm—Wolf, Greenfield & Sacks

[57] **ABSTRACT**

A method and apparatus for providing improved security for a personal identification number (PIN) in a personal identification and verification system of the type wherein a time dependent nonpredictable code is generated at a device in the possession of the individual, which code is unique to the individual and this code is communicated to, and compared with a nonpredictable code generated at a central verification computer. In this system, the PIN is mixed with the nonpredictable code before transmission of these values to the central verification computer. A nonsecret code is previously transmitted to the central verification computer and is used to retrieve the PIN and the appropriate nonpredictable code for the user. These values are used to strip the PIN from the transmitted nonpredictable code and the stripped PIN and remaining nonpredictable code are compared with the corresponding retrieved values in order to determine verification.

19 Claims, 2 Drawing Sheets



Apple 1138

U.S. PATENT DOCUMENTS

4,589,066	5/1986	Lam et al.	364/200
4,599,489	7/1986	Cargile	380/4
4,609,777	9/1986	Cargile	380/4
4,636,583	1/1987	Bidell et al.	380/48
4,641,322	2/1987	Hasegawa	375/1
4,677,617	6/1987	O'Connor et al.	370/50
4,720,860	1/1988	Weiss	380/23
4,731,841	3/1988	Rosen et al.	380/23
4,802,216	1/1989	Irwin et al.	380/23
4,819,267	4/1989	Cargile et al.	380/23
4,849,613	7/1989	Eisele	235/379
4,856,062	8/1989	Weiss	380/23
4,890,323	12/1989	Beker et al.	380/25
5,023,908	6/1991	Weiss	380/23

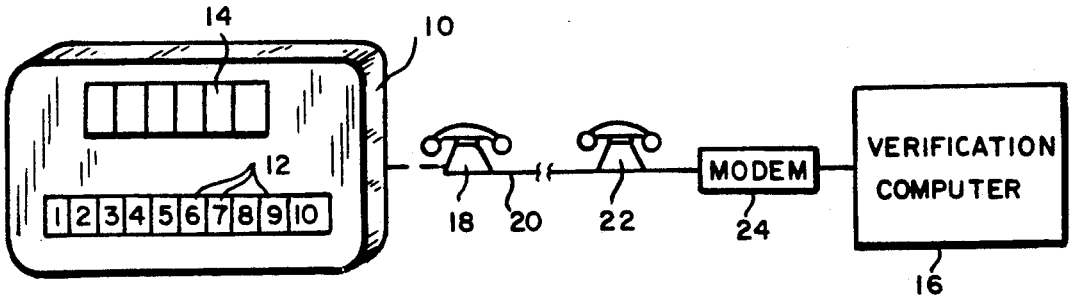


FIG. 1

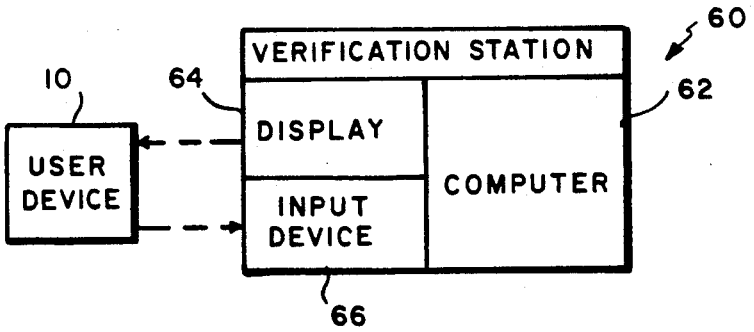


FIG. 2

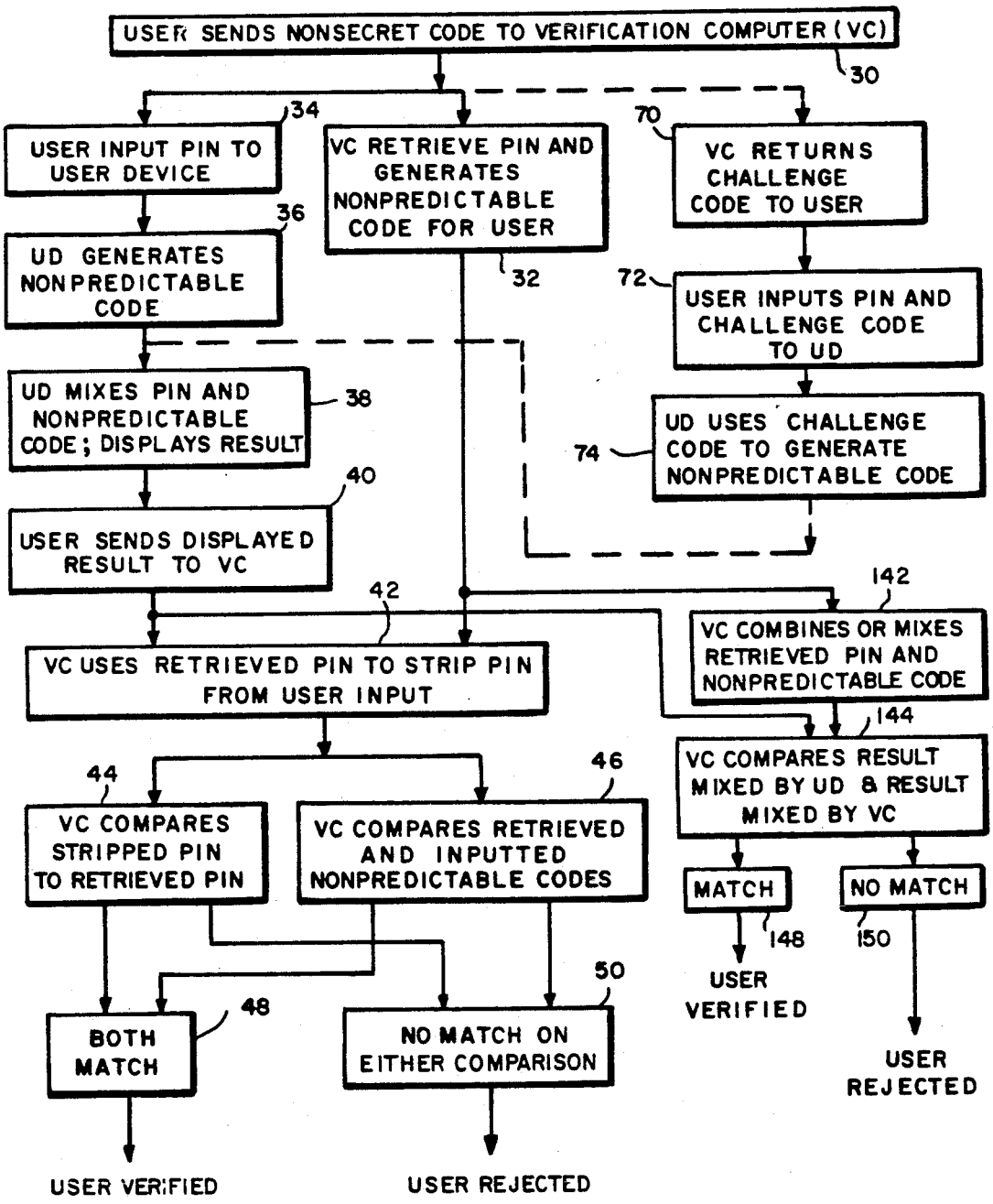


FIG. 3

METHOD AND APPARATUS FOR PERSONAL IDENTIFICATION

CROSS REFERENCE TO OTHER APPLICATIONS

This application is a continuation in-part of application Ser. No. 07/341,932 filed Apr. 21, 1989, now U.S. Pat. No. 5,023,908, which is a continuation-in-part of application Ser. No. 802,579 filed Nov. 27, 1985, issued Dec. 5, 1989 as U.S. Pat. No. 4,885,778, which application is itself a continuation-in-part of application Ser. No. 676,626 filed Nov. 30, 1984, now U.S. Pat. No. 4,720,860, issued Jan. 19, 1988. The disclosures and specifications of all of the foregoing applications/patents are incorporated herein by reference as if fully set forth.

FIELD OF THE INVENTION

This invention relates to methods and apparatus for identifying an individual and more particularly to methods and apparatus for providing improved security for a personal identification number (PIN) utilized in conjunction with such an identification system.

BACKGROUND OF THE INVENTION

Personal identification systems may be based on something someone has, such as a card or badge, something that someone knows, such as a PIN, or some characteristic of the individual, such as his fingerprints or speech pattern. Security for such systems is enhanced by utilizing two or more of the above in performing the identification.

For example, parent U.S. Pat. No. 4,720,860, discloses a personal identification system wherein the individual has a card or other small, portable device which contains a microprocessor programmed to utilize a secret algorithm to generate a nonpredictable number from a stored value unique to the individual and a time varying value provided for example by a clock. The nonpredictable value is preferably displayed on the device. The individual then enters his secret PIN into a central verification system, either directly or over a telephone line, causing the central system to access stored information corresponding to the individual and to utilize at least some of this information to generate a nonpredictable value at the central computer utilizing the same algorithm as at the individual's microprocessor. At the same time this is being done, the individual is entering the number appearing at that period of time on the display of his device. The two values will match, signifying identification of the individual, only if the individual has entered the correct PIN and if the individual has the proper device so that the nonpredictable code displayed corresponds to that being generated at the central verification computer.

In other systems, such as those shown in U.S. Pat. No. 4,599,489 issued Jul. 8, 1986, the PIN may either be stored in the user's device, or may be entered by the user. If the PIN is stored in the device, it is read from the device by a suitable reader and causes the central verification computer to generate a unique challenge code to the individual. This challenge code may either be entered by the individual into his machine, or may be automatically sensed by the machine, and is operated on by the user's device to generate a unique nonpredictable code which is then entered into the central computer to effect verification.

One potential difficulty with either of the systems indicated above is that an unauthorized individual may be able to obtain access to the user s PIN by electronic eavesdropping, reducing the security provided by the system. If, for example, the PIN is transmitted over public lines, such as telephone lines, from the user to the central verification computer, it may be possible to tap these lines and intercept the PIN as it is being transmitted. If the PIN is stored in the device, someone obtaining the device surreptitiously may, through sophisticated means, be able to determine the PIN stored in the device and thus defeat the security of the system. Furthermore, any storing of a PIN or password in the portable device for comparison defeats the purpose of an independent identification factor and reduces security to a "thing" possessed.

A need therefore exists for an improved means of communicating a PIN or other user identification code to a central verification system such that someone tapping the line over which the code is being sent will be unable to determine the secret identification number and someone obtaining possession of the user device will also not be able to obtain access to the user's secret identification number from the device.

SUMMARY OF THE INVENTION

In accordance with the above, this invention provides a method for personal identification and apparatus for the practice thereof wherein a device in the possession of the individual is utilized to generate a unique, time varying, nonpredictable code; the nonpredictable code generated at a given time is mixed with a secret PIN for the individual; the mixed output is communicated to a central verification computer; and the verification computer typically strips the PIN from the communicated value and utilizes the stripped PIN and remaining nonpredictable code to perform a verification operation Alternatively and equivalently, the mixed output which is communicated to the verification computer may be verified in the verification computer without stripping of the PIN. Preferably, before the mixed value is communicated to the verification computer, a nonsecret identifying code for the individual is communicated to the verification computer; the verification computer utilizes the nonsecret identifying code to obtain the PIN and appropriate nonpredictable code for the individual; and the verification operation includes the PIN and appropriate nonpredictable code obtained during the obtaining step being compared with the stripped PIN and remaining nonpredictable code. Alternatively the PIN may not be stripped from the mixed value, the verification computer may utilize the nonsecret identifying code to retrieve or obtain the PIN and appropriate nonpredictable code, combine the retrieved PIN and appropriate nonpredictable code, and perform a verification operation between the mixed value communicated to the verification computer and the combination of the retrieved PIN and appropriate nonpredictable code. The verification computer may also generate a unique challenge value in response to the nonsecret identifying code which challenge code is communicated to the device in possession of the individual. For one embodiment, the challenge code is communicated to the individual and the individual inputs the challenge value and the PIN to his device, the device includes means responsive to the challenge value for generating

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.