US005559505A

United States Patent [19]

McNair

[11] **Patent Number: 5,559,505**

[45] **Date of Patent: Sep. 24, 1996**

[54] **SECURITY SYSTEM PROVIDING LOCKOUT FOR INVALID ACCESS ATTEMPTS**

[75] Inventor: **Bruce E. McNair**, Holmdel, N.J.

[73] Assignee: **Lucent Technologies Inc.**, Murray Hill, N.J.

[21] Appl. No.: **409,482**

[22] Filed: **Mar. 21, 1995**

Related U.S. Application Data

[63] Continuation of Ser. No. 886,539, May 20, 1992, abandoned.

[51] **Int. Cl.**^{6} **H04Q 1/00**

[52] **U.S. Cl.** **340/825.31**; 340/576; 340/825.56; 340/825.34

[58] **Field of Search** 340/825.31, 825.34, 340/825.56, 576; 380/3.4; 70/267, 271; 235/382, 377, 380; 920/1, 5

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,905,461	9/1975	Davies	902/5
3,953,769	4/1976	Sopko	340/825.31
4,492,959	1/1985	Mochida	340/825.56
4,723,625	2/1988	Komlos	340/576
4,992,783	2/1991	Zdunek	340/825.31
5,081,675	1/1992	Kittirutsunetorn	380/4

OTHER PUBLICATIONS

K. Dehnad "A Simple Way of Improving the Login Security", *Computers and Security*, vol. 8, No. 7, 1989, pp. 607–611.

Primary Examiner—Brian Zimmerman
Attorney, Agent, or Firm—Ronald D. Slusky

[57] **ABSTRACT**

A security system controlling access to a resource is arranged to operate such that when an attempt to access a resource using a password or PIN fails, the time interval "t" that must elapse before a subsequent attempt at access can be successful, is incremented. By making the increments increasingly large (illustratively, an exponential function of the number "n" of unsuccessful attempts), repeated access attempts by hackers or other unauthorized users is discouraged, because they simply cannot wait the time needed to make a large number of trial and error attempts. On the other hand, valid users, while experiencing a delay prior to access, are nevertheless able to gain access, rather than being completely "lockedout". This approach is a better compromise between access control and denial.

17 Claims, 3 Drawing Sheets

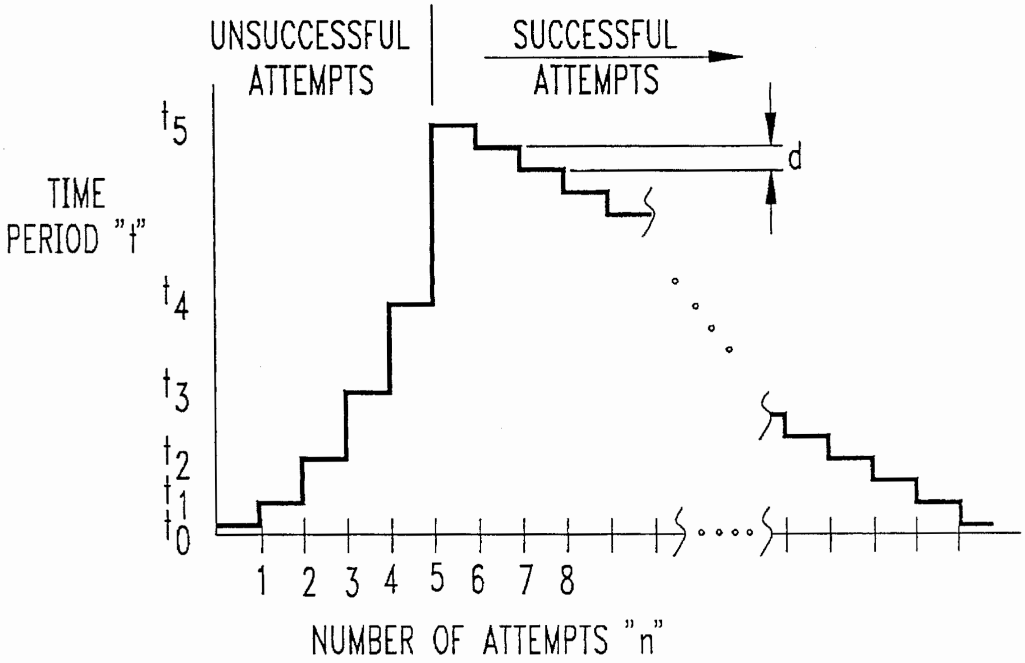


FIG. 1

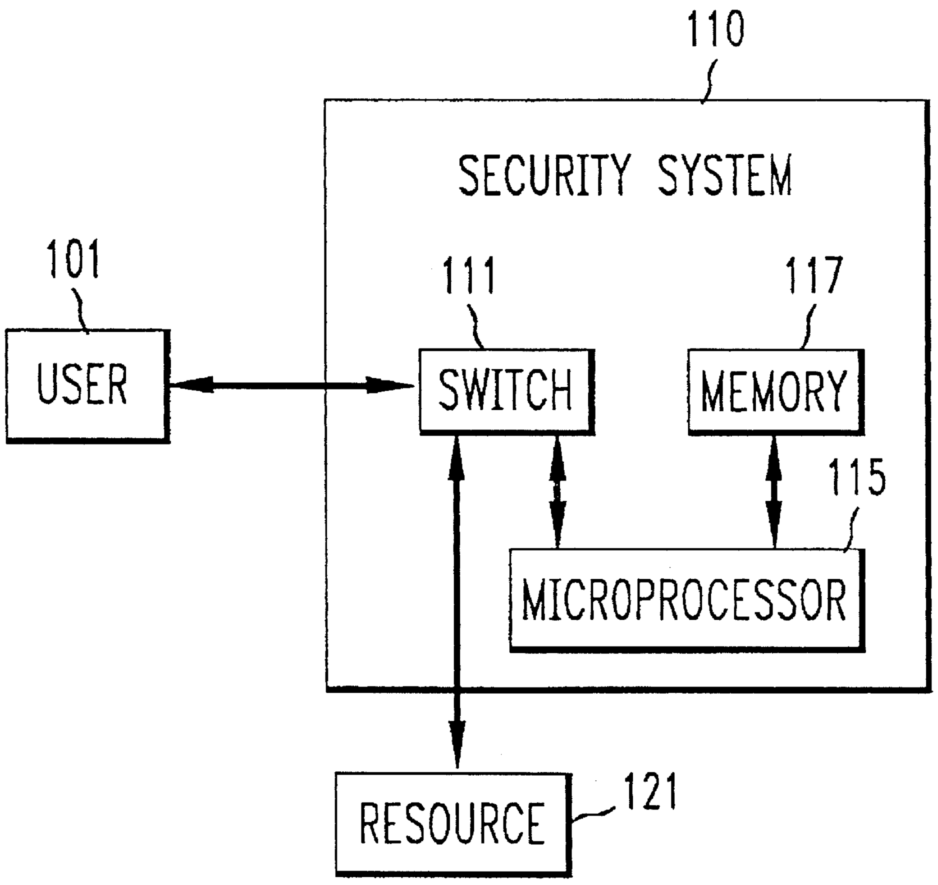

110
SECURITY SYSTEM
101
USER
111
SWITCH
117
MEMORY
115
MICROPROCESSOR
RESOURCE
121

FIG. 2

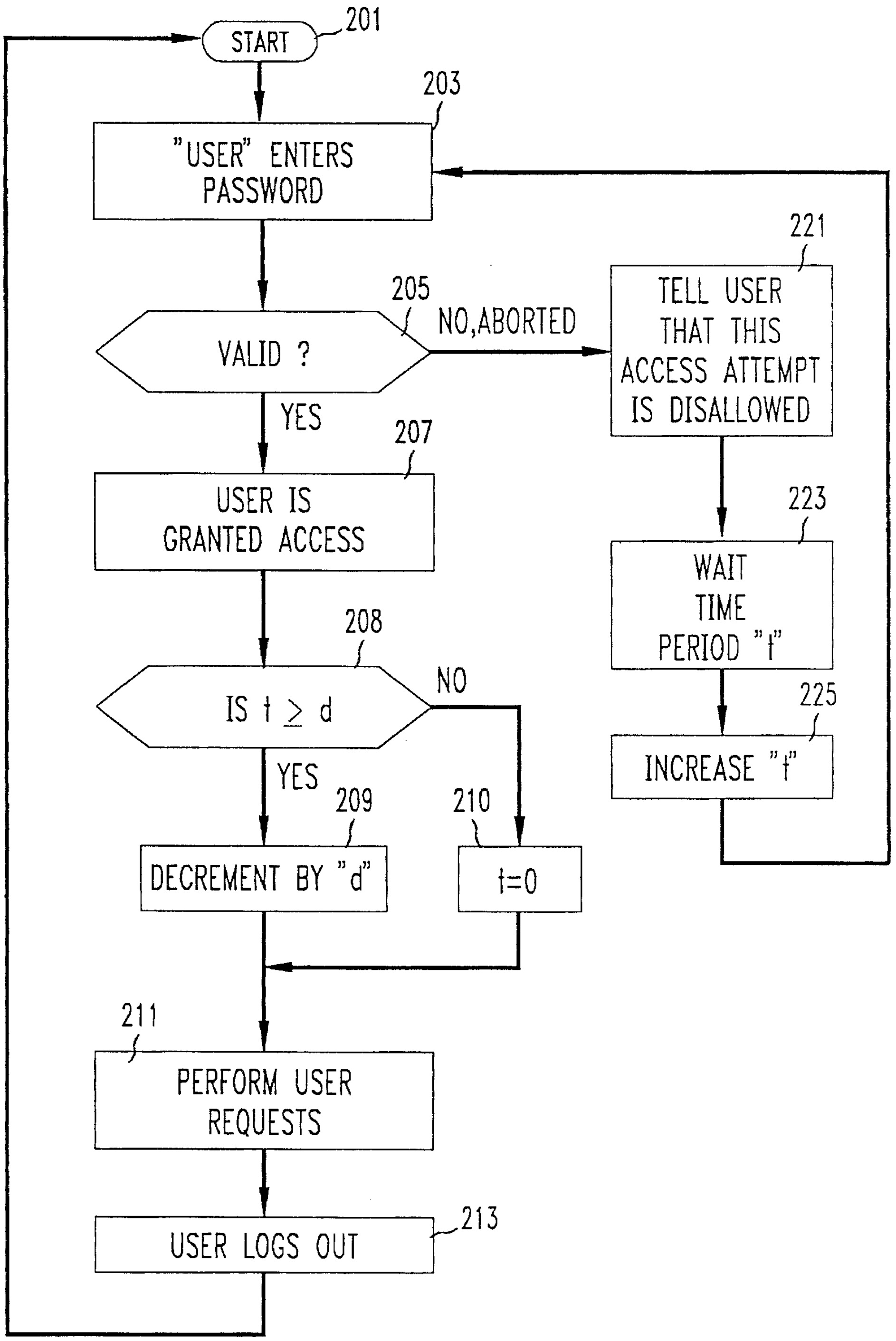
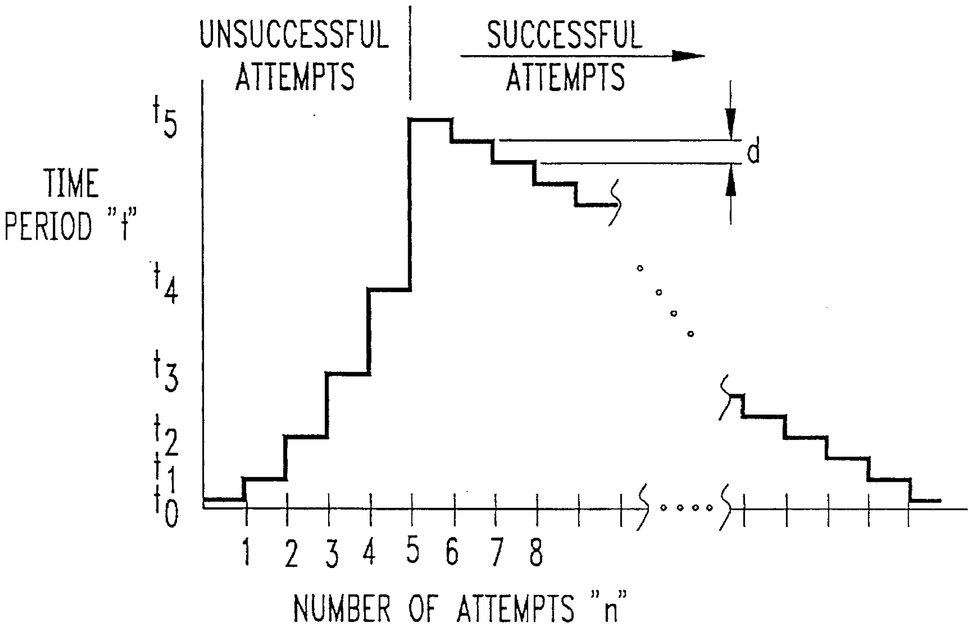

START
201
"USER" ENTERS PASSWORD
203
VALID ?
205
NO,ABORTED
YES
TELL USER THAT THIS ACCESS ATTEMPT IS DISALLOWED
221
USER IS GRANTED ACCESS
207
WAIT TIME PERIOD "t"
223
IS t ≥ d
208
NO
INCREASE "t"
225
YES
DECREMENT BY "d"
209
t=0
210
PERFORM USER REQUESTS
211
USER LOGS OUT
213

FIG. 3


UNSUCCESSFUL ATTEMPTS
SUCCESSFUL ATTEMPTS
TIME PERIOD "t"
t_5
t_4
t_3
t_2
t_1
t_0
d
1
2
3
4
5
6
7
8
NUMBER OF ATTEMPTS "n"

SECURITY SYSTEM PROVIDING LOCKOUT FOR INVALID ACCESS ATTEMPTS

This application is a continuation of application Ser. No. 07/886,539, filed on May 20, 1992 now abandoned.

FIELD OF THE INVENTION

This invention relates generally to security systems for preventing unauthorized access to computers, telecommunications networks and the like, and, in particular, to security systems which provide a "lockout" capability denying access in the event invalid passwords, personal identification numbers (PINs), etc. are used in attempts to gain access.

BACKGROUND OF THE INVENTION

The proliferation of remotely accessed computer and telecommunications systems have increased the need for improved security systems which check for valid passwords, PINS, and access codes/authentication codes (collectively referred to herein as "passwords") before granting access. While breaches of security can take many forms, one of the most common forms of attack by unauthorized users (sometimes called "hackers") is educated guessing and/or trial and error to discover the valid password through repeated, albeit usually unsuccessful, access attempts. With each attempt, the hacker readjusts the password being used; he/she actually gains valuable information from each denial, since most existing security systems permit access "if and only if" the correct password is entered, and deny access if any other password is entered, so that a denial reveals that an attempted password is actually invalid. The trial and error process is most often automated by the hacker, so that convergence to a correct password can sometimes undesirably be very fast.

In order to defeat the hacker or other unauthorized access seeker, legitimate users are instructed not only to keep passwords secret, but also to choose them carefully to avoid guessing. Sometimes it is difficult to insure that authorized users haven't chosen trivial variants of easily guessable words or sequences.

One attempt to improve access security was described by K. Dehnad in an article entitled "A Simple Way of Improving the Login Security", Computers and Security, Vol. 8, No. 7, 1989, pages 607–11. According to the author, the advantage gained by a hacker in repeated access attempts can be reduced by controlling the probability (p) that an authorized user will gain access to the target system even when the proper password is entered. This variability has the effect of reducing the information obtained by the hacker in being denied access: he/she cannot be sure that the denial is due to the fact that an invalid password was used, and thus may have to repeat the attempt, thereby increasing the number of trial and error attempts that may be necessary. This approach necessitates that authorized users be occasionally inconvenienced by having to enter the correct password more than once: if p=0.95, the authorized user will, on average, have to make about 105 attempts to gain access 100 times. Dehnad also suggests that the value of "p" can be reduced, thereby increasing the penalty imposed on a hacker if repeated unsuccessful access attempts are detected. While the author argues that this may be an acceptable price to pay for enhanced security, alternative solutions which have additional flexibility are desired.

To counter the threat of an attacker guessing a password by trial and error, other security systems use a control mechanism sometimes known as "lockout" that relies on counting unsuccessful attempts and completely stopping access to the person seeking access once there have been "too many" unsuccessful access attempts. When the system is "locked", subsequent access attempts, both valid and invalid, will be blocked. There are, unfortunately, problems with this approach, since it essentially trades "Access Control" for "Denial of Service". Specifically, by completely cutting off access after a preset but relatively small number of unsuccessful access attempts, the hacker is frustrated by stringent access control, but the legitimate user who unfortunately erred during attempted access attempts is also undesirably denied service or access. On the other hand, if lockout is not used at all, or is only instituted after a relatively large number of access attempts, the legitimate user may gain access more easily, but the hacker may also more frequently get through to the computer, network or other resource being accessed. To date, there has been no compromise solution.

SUMMARY OF THE INVENTION

In accordance with the present invention, a security system controlling access to a resource is arranged to operate such that when a user's attempt to access a resource using a password fails, the time interval "t" that must elapse before a subsequent attempt at access by that user can be successful, is increased. By making the increments increasingly large (illustratively, an exponential function of the number "n" of unsuccessful attempts), repeated access attempts by hackers or other unauthorized users is discouraged, because they simply cannot wait the time needed to make a large number of trial and error attempts. On the other hand, valid users, while experiencing a delay prior to access, are nevertheless able to gain access, rather than being completely "locked-out".

In accordance with a feature of this invention, the value of "t" may be decreased in relatively small decrements "d" in response to each of "m" subsequent valid access attempts. By maintaining the value of "t" at a high level after multiple unauthorized access attempts, the authorized user is alerted that there may have been an attempt at unauthorized access. Also, an attempt by a hacker to time access attempts to correspond to valid user actions is frustrated. The approach used in the present invention is thus a better compromise between access control and denial.

BRIEF DESCRIPTION OF THE DRAWING

The invention will be better appreciated by consideration of the following detailed description, when read in light of the accompanying drawing in which:

FIG. **1** is a block diagram of a security system embodying the access control system of the present invention;

FIG. **2** is a logic flow diagram illustrating the steps followed in the system of FIG. **1**; and

FIG. **3** is a graph illustrating one example of the relationship, in accordance with this invention, between the number "n" of unsuccessful access attempts made by a user seeking access to a resource, the number "m" of successful access attempts made thereafter, and the value of "t" indicating the time interval that must elapse before a subsequent attempt at access by that user can be successful.

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.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**