



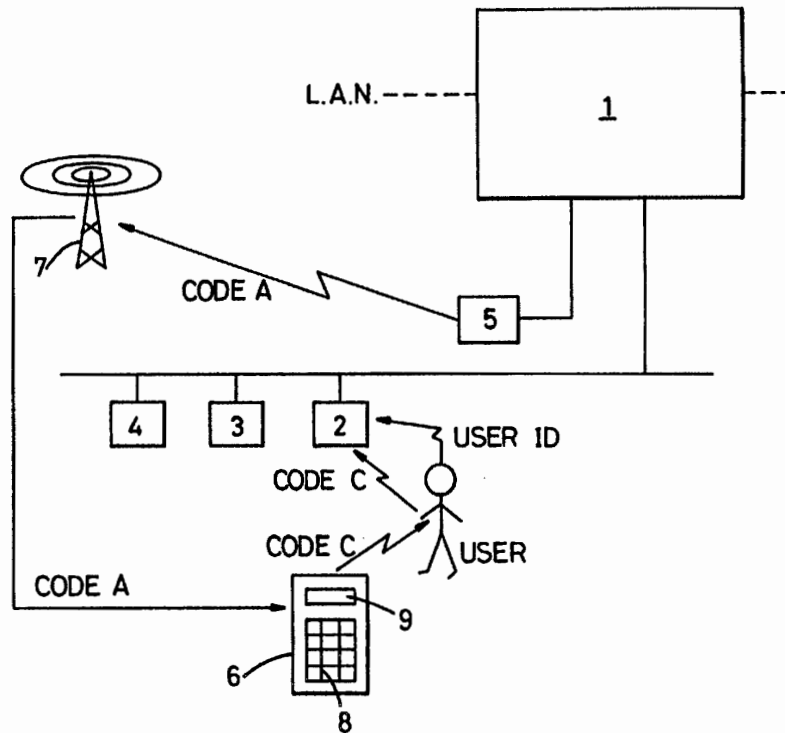
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁶ : G06F 1/00, G08B 5/22</p>	<p>A1</p>	<p>(11) International Publication Number: WO 95/19593 (43) International Publication Date: 20 July 1995 (20.07.95)</p>
<p>(21) International Application Number: PCT/GB95/00059 (22) International Filing Date: 12 January 1995 (12.01.95) (30) Priority Data: 9400602.0 14 January 1994 (14.01.94) GB 9415779.9 4 August 1994 (04.08.94) GB (71)(72) Applicants and Inventors: KEW, Michael, Jeremy [GB/GB]; Heron Bridge, Collapit Creek, Kingsbridge, Devon TQ7 3BB (GB). LOVE, James, Simon [GB/GB]; 18 Monterey Court, Vardean Drive, Brighton, East Sussex BN1 6TE (GB). (74) Agent: BRAY, Lilian, Janet; L.J. Bray & Co., Raw Holme, Midgehole Road, Hebden Bridge, West Yorkshire HX7 7AF (GB).</p>		<p>(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ). Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>

(54) Title: A COMPUTER SECURITY SYSTEM

(57) Abstract

A method of preventing unauthorised access to a host computer system (1) by a user at a remote terminal (2) is provided using paging system technology. In the method, a user inputs his user identification code input into the terminal (2) which transmits same to the host computer system (1). The system then generates a random code (Code A) and subjects Code A to a transformation characteristic of a transformation algorithm identified by the input user identification code so as to generate a transformed code (Code B). Code A is transmitted via a paging system (7), to a receiver (6) held by the user. The receiver (6) comprises transformation means adapted to transform the received Code A to a second transformed code (Code C), and means (9) for displaying Code C to the user. The user then inputs the displayed Code C to the terminal (2) which transmits it to the host system (1). The input Code C is then compared with Code B and access is only permitted if Code C matches Code B.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgystan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SI	Slovenia
CI	Côte d'Ivoire	KZ	Kazakhstan	SK	Slovakia
CM	Cameroon	LI	Liechtenstein	SN	Senegal
CN	China	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
CZ	Czech Republic	LV	Latvia	TJ	Tajikistan
DE	Germany	MC	Monaco	TT	Trinidad and Tobago
DK	Denmark	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	US	United States of America
FI	Finland	ML	Mali	UZ	Uzbekistan
FR	France	MN	Mongolia	VN	Viet Nam
GA	Gabon				

IPMORCAN EXHIBIT 1007

A COMPUTER SECURITY SYSTEM

5 The present invention relates to a computer security system and comprises a method and apparatus for preventing unauthorized access to a host computer system.

10 Many large computer systems require users to gain access via a remote terminal using a telephone link. In cases where access to the computer system is restricted to authorised personnel, attempts by unauthorised persons to gain access are referred to as "hacking". It is common practice for security systems to be installed in the computer system in an attempt to verify the identity of a user. However, to date no completely successful computer security system has been devised.

15 There has now been devised an improved computer security system based on pager technology.

20 According to a first aspect of the present invention there is provided a method of preventing unauthorised access to a host computer system by a user at a remote terminal comprising the steps of

25 accepting a user identification code input to the terminal by the user;

generating a random code (Code A);

30 subjecting Code A to a transformation characteristic of a transformation algorithm identified by the input user identification code so as to generate a transformed code (Code B);

transmitting Code A via a paging system, to a receiver held by the user, the receiver comprising transformation means adapted to transform the received Code A to a second transformed code (Code C), and means for displaying Code C to the user;

35 accepting input of Code C to the terminal by the user;

comparing Code C with Code B; and
permitting access to the host system only if Code C
matches Code B.

5 According to a second aspect of the present invention
there is provided apparatus for preventing unauthorized
access to a host computer system by a user at a remote
terminal, the apparatus comprising
 means for accepting a user identification code input
10 to the terminal by the user;
 means for generating a random code (Code A), and for
subjecting Code A to a transformation to generate a
transformed code (Code B);
 a transmitter for transmitting Code A via a paging
15 system;
 a receiver held by the user, the receiver comprising
transformation means adapted to transform the received Code
A to a second transformed code (Code C), and means for
displaying Code C to the user;
20 means for accepting input of Code C by the user;
 means for comparing Code C with Code B; and
 means for permitting access to the host system if Code
C matches Code B.

25 It will be appreciated that the receiver carried by an
authorized user will have logic circuitry programmed with a
transformation algorithm which is characteristic of that
receiver. When the user enters his user identification
code, the host computer system identifies the corresponding
30 transformation algorithm in a database from the code and
transforms the random code (Code A) to a new Code B in such
a manner that the Code C, produced by the user's receiver
from the transmitted code, will be identical to Code B with
which it is compared. Thus, only a user both with knowledge
35 of the user identification code and holding the
corresponding receiver can gain access to the host system.

5 The transformation algorithms associated with each receiver may be completely different, or may be the same base algorithm which is convoluted with a code corresponding to the user's identification code so as to generate characteristic transformed codes. Preferably, the algorithms used are all, so called, one-way algorithms.

10 The user identification code should preferably be treated by the user as a secret code and not be marked on the receiver. It is thus comparable with a personal identification number (PIN) familiar from many other contexts.

15 Preferably also, the receiver can only be enabled for a predetermined period to permit it to transform the received Code A to the transformed Code C by input of a second user identification code by the user. This second code may also be in the form of a PIN. In this way additional security is provided since an unauthorised user cannot gain access to the system even if he has possession of the receiver and knows the user identification code without knowledge of the second identification or activation code.

25 Preferably also, the signal incorporating Code A which is transmitted by the paging system also incorporates an identifier to enable the receiver to pick out the signal from a plurality which may be being transmitted at the same time.

30 In addition, the receiver is preferably always responsive to reception of its identifier regardless of whether or not it has been enabled by the user. Hence, the receiver is responsive to reception of its identifier in circumstances when the authorised user is not attempting to gain access to the host system. In this way the receiver

35

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.