PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, G08B 5/22 — A1

(11) International Publication Number: WO 95/19593

(43) International Publication Date: 20 July 1995 (20.07.95)

(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, Varndean 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).

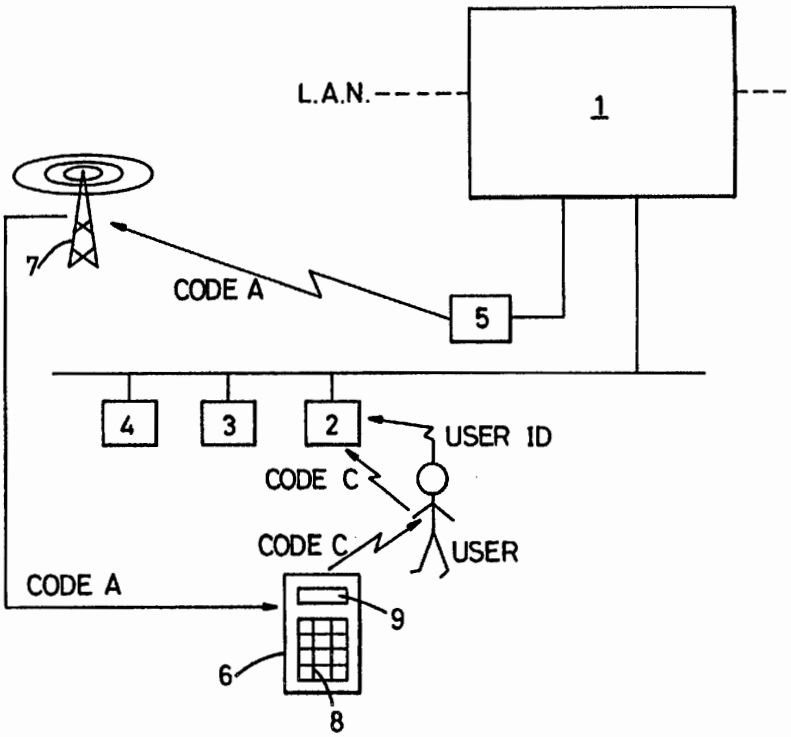
(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, 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
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(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 trasmits 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				

A COMPUTER SECURITY SYSTEM

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

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.

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

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

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

generating a random code (Code A);

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;

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.

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 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 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;

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.

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 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 of the user identification code and holding the corresponding receiver can gain access to the host system.

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.

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.

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.

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.

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

can alert the authorised user that an attempt at unauthorised access is being made. Preferably, therefore, the receiver emits an alarm or otherwise operates to alert the user in these circumstances.

The means for displaying Code C on the receiver can be a liquid crystal display or other conventional display means. Also, the means by which the signal is transmitted via the paging system and the means by which the transmitted signal is received by the receiver may both utilise technology which is generally conventional in paging systems.

In a second more sophisticated embodiment, the method preferably comprises the additional steps of

generating an access code by the terminal based on the user identification code and at least one of a terminal code for identifying the remote terminal, a network identification code for identifying which of a plurality of networks the remote terminal is connected to, and a software code identifying the presence or absence of particular software stored at the remote terminal site and accessible by its CPU;

transmitting the access code to the host computer system;

deconstructing the access code to produce at least one computer identification code and the user identification code;

generating a second random code (Code D);

subjecting Code D and the computer identification code to a transformation characteristic of a transformation algorithm so as to generate a transformed code (Code E);

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

passing Code D to the remote terminal which also subjects Code D and the computer identification code to a transformation characteristic of a transformation algorithm so as to generate a transformed code (Code F);

passing Code F to the receiver from the remote terminal which also subjects Code A to a transformation characteristic of both the transformation algorithm identified by the input user identification code and Code F so as to generate the transformed code (Code C).

As before the terminal compares Code C with Code B and only permits access to the host system if Code C matches Code B. However, it will be appreciated that this embodiment can be used to verify that the actual remote terminal being used is an authorised terminal. This will mean that in practice if the terminal is authorised, Code F will also equal Code E.

Preferably also, the method comprises the further additional steps of

deconstructing the access code to produce the user identification code, a first computer identification code characteristic of the computer hardware identifying portions of the access code and a second computer identification code characteristic of the computer software identifying portions of the access code;

generating a second random code (Code D1) and a third random code (Code D2);

subjecting Code D1 and the first computer identification code to a transformation characteristic of a transformation algorithm so as to generate a transformed code (Code E1);

subjecting Code D2 and the second computer identification code to a transformation characteristic of a transformation algorithm so as to generate a transformed code (Code E2); and

combining in a predetermined fashion Codes E1 and E2 or parts thereof to produce the transformed code (Code E);

passing Code D1 and Code D2 to the remote terminal (2) which subjects Code D1 and the first computer identification code to a transformation characteristic of a transformation algorithm so as to generate a transformed code (Code F1), and which subjects Code D2 and the second computer identification code to a transformation characteristic of a transformation algorithm so as to generate a transformed code (Code F2); and

combining in a predetermined fashion Codes F1 and F2 or parts thereof to produce the transformed code (Code F).

It will be appreciated, therefore, that not only can the actual terminal be verified but the network system it is connected to can be verified too along with software which is accessible to the terminal. The latter can be checked by running security software which monitors the type of software which can be run by the terminal and supplies appropriately encrypted identification codes dependent on this software.

Hence, in this way the system can be used to display sensitive information which, for example, can be made available for viewing only and not for further analysis at the remote terminal.

In this second embodiment, the receiver preferably takes the form of a security key which is linked to the remote terminal. Preferably, the receiver is linked to the central processing unit either by a plug and socket arrangement or by an infrared transmission system for the passage of information therebetween.

The various aspects of the present invention will now be described by way of example with reference to the

accompanying drawings, in which:-

Fig. 1 is a schematic view of a first embodiment of a computer security system according to the invention; and

Fig. 2 is a view similar to Fig. 1 but of a second embodiment of the system and additionally showing logic operations carried out by various components of the system.

With reference first to Fig. 1, a host computer system 1, typically one of several arranged in a local area network (LAN), may be accessed from any one or more of a series of remote terminals 2, 3, 4 via a telephone line link. To gain access to the host system 1, a user at one of the terminals, say terminal 2, must first verify his or her identity by satisfying a security barrier system or security server 5, which is effectively interposed between the remote terminals 2, 3, 4 and the host system 1.

The user carries a receiver unit 6 which includes encryption means for encryption of received codes. Typically, the unit will include logic circuitry to do this which preferably itself includes an EPROM or erasable programmable read only memory where the algorithm required is stored. As previously mentioned, this algorithm is preferably a one-way algorithm.

The receiver unit 6 also stores in the EPROM an identity code. This identity code is a key for the one-way algorithm and is such that when applied to the algorithm, together with a code to be encrypted the resultant code is characteristic of the particular receiver unit 6.

When the user seeks access to the host system 1 via the terminal 2, he enters his user identification code. This code may take any suitable form, for example his

actual name or preferably a more secure code such as a PIN. The security server 5 includes a database of all authorised users and their authorised receiver units 6, and identifies the corresponding identity code for the appropriate receiver unit 6. The security server 5 then generates a random code (Code A) and subjects this number to an encryption using the same one-way algorithm as is stored in the user's receiver 6 together with the corresponding identity code. In this way a transformed code (Code B) is produced.

In addition to producing the transformed Code B, the security server 5 also transmits the random code to a paging system 7 along with an indentifier or identifying tag which can be recognized by the receiver unit 6. The identifying tag and the random code are then broadcast by the paging system 7, typically using a radiofrequency transmitter, in a fashion similar to conventional paging systems. Whilst the receiver unit 6 will pick up all codes broadcast on a particular frequency, the receiver unit 6 will use the identifier to pick out the appropriate signal meant for it from a plurality which may be being transmitted at the same time.

After or before entering his identification code into the terminal 2, the user also activates the receiver unit 6 by entering a second user identification code, which is also preferably in the form of a secret PIN, via a keypad 8. Preferably, the receiver unit 6 can receive the broadcast signal regardless of whether it has been activated or not, but activation enables the logic circuitry of the receiver unit 6 to permit it to encrypt the received random code. The receiver unit 6 therefore uses the received random number and the identity code stored in its own EPROM to produce a transformed code (Code C) via its own characteristic algorithm. This transformed

Code C is then displayed to the user on a display means 9, preferably a liquid crystal display, for a predetermined length of time such as five minutes.

The terminal 2, at the behest of the security server 5 prompts the user to input the transformed Code C displayed by the receiver unit 6. After input, the security server 5 compares the input Code C with the transformed code, Code B, it produced by encryption of the random code, Code A. If Code B and Code C are identical, access to the host system 1 is permitted.

A second more sophisticated embodiment of the invention is shown in Fig. 2 and the same reference numbers are used in Fig. 1 as have been used in Fig. 1 to indicate similar features of the system. In addition, logic operations carried out by various components of the system are shown in the rounded edged boxes.

This second embodiment enables verification of the actual remote terminal 2, the network system to which it is connected, and the software it has access to. In this way, highly secure information can be made available for viewing but not made available to terminals which may have the capability to store or process the information further.

However, whereas in the first embodiment, the receiver unit 6 would probably, but not necessarily, comprise a stand-alone piece of equipment, in this embodiment the receiver unit 6 is intended to be linked to the remote terminal 2 for the passage of information therebetween. This linkage could be by any conventional means, such as a plug/socket arrangement whereby the unit 6 is plugged into one of the output ports of the terminal 2 or an infrared transmission system. In this way, the receiver unit 6 forms a security key for the system and must be connected to the

terminal 2 before the latter can be used to access the host system 1.

The terminal 2 also comprises a central processing unit (CPU) in its own right and is preferably in the form of a personal computer (PC). In a similar fashion to the security key 6, the terminal 2 will also have its own terminal identity code. In addition, it runs security software which monitors other software which can be accessed and run by the terminal. The security software supplies appropriately encrypted software identity codes dependent on this software.

The network system to which the terminal 2 is connected can also be verified. For example, the terminal's token ring identification code can be used for this purpose.

With reference to Fig. 2, the system operates as follows. The user first attaches the receiver unit 6 or security key to the terminal 2 and enables the unit 6 by entering his second user identification code in the form of a secret PIN, via the keypad 8. This PIN is known only to the user and the receiver unit 6 could be constructed so that this number can be changed by the user by following a predetermined routine.

The user's first identification code (USER ID), which can again comprise the user's name is entered into the terminal 2. In this embodiment, it is the security software running on the terminal 2 which enables the dialogue with the user. This security software now generates an access code or what can be considered as an access "claim" based on the user's identification code (USER ID) and one or more, and preferably all of the terminal identity code (TERMINAL ID), the network identification code (NETWORK

ID), and one or more software identity codes (SOFTWARE ID). This access code or claim is passed to the security server 5 of the host computer system 1 that it is desired to access.

The security server 5 deconstructs the access code or claim into its constituent parts. In the same way as the first embodiment, it uses the user identification code (USER ID) to access its database to locate the corresponding identity code for the appropriate receiver unit 6. As before, the security server 5 then generates a random code (Code A) and subjects this number to an encryption using the same one-way algorithm as is stored in the user's receiver 6 to produce the transformed code (Code B). However, in this embodiment a third code (Code E) is used as a second encryption key. This third Code E is obtained by using the other identification codes comprising the access claim as will now be described.

The security server takes the terminal identity code and network identity code and combines these or parts of these in a predetermined manner to form a hardware code (HARDWARE ID) or first computer identification code. It then generates a second random number (Code D1) which is encrypted using a predetermined one-way algorithm, to produce a first transformed code (Code E1).

A similar operation is performed on the software identity codes (SOFTWARE ID). If more than one of these comprises part of the access claim, then they are combined or parts of them are combined in a predetermined manner to form a single code which comprises the second computer identification code. The security server 5 generates a third random number (Code D2), which is encrypted using a predetermined one-way algorithm to produce a second transformed code (Code E2).

The first and second transformed codes, Code E1 and Code E2, are then combined in a predetermined manner to form a single transformed code which comprises the Code E which is used in the production of Code B.

As in the first embodiment, the security server 5 transmits the first random code, Code A, along with an indentifier or identifying tag which can be recognized by the security key 6 to the paging system 7. The identifying tag and the random code, Code A, are then broadcast by the paging system 7 for the security key 6 to pick up, identity and store.

In addition however, the security server 5 passes the second and third random numbers, Code D1 and Code D2, along with the transformed code, Code B, back to the host computer system 1. The host computer system 1 then passes the second and third random numbers, Code D1 and Code D2, back to the terminal 2. The the security software running on the terminal 2 uses the Codes D1 and D2 along with the hardware and software identification codes, which it constructed as part of the access claim, to produce respectively transformed Codes F1 and F2. These are then are then combined in the same predetermined manner as the Codes E1 and E2 to produce a single transformed code, Code F.

This single transformed code, Code F, is then passed by the terminal 2 to the security key 6. The security key is now able to encrypt the received Code A using the Code F and the user identification code it contains via the one-way algorithm in its logic circuitry to produce the transformed code, Code C.

The resultant code, Code C, is then displayed on the display means 9 of the security key for the user to enter

into the terminal 2 at the behest of the host computer system 1. The system 1 can then compare the entered transformed code, Code C, with that, Code B, transmitted to it from the security server 5. Access to the system 1 is then only permitted if the two codes, Code B and Code C, are identical.

It will be appreciated that for Code B and Code C to be identical, then Codes E and F will also be identical assuming that the one-way algorithms used to produce same are also equivalent.

Thus, the computer security system not only verifies that the user's identification code and the security key 6 but also the terminal 2 and its network and stored software.

It will be appreciated that a less complex security system code could simply verify the computer hardware being used and not the software. In this case a single random generated code, Code D, can be encrypted to produce a single transformed code, Code E, which can then be used directly in the encryption of Code A.

As in the first embodiment, preferably all the algorithms used in the system should comprise one-way algorithms.

In addition, in both embodiments the receiver unit or security key 6 is preferably always responsive to reception of its identifier regardless of whether or not it has been enabled by the user. Hence, the receiver 6 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 6 can be used to alert the authorised user that an attempt at unauthorised

access is being made as well as act as a conventional pager which can request the user to log into a particular computer system 1 or otherwise receive pager messages. Thus, a host computer system 1 can request users to log in to receive, for example, electronic mail, or to carry out other operations.

CLAIMS

1. A method of preventing unauthorised access to a host computer system (1) by a user at a remote terminal (2) comprising the steps of

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

generating a random code (Code A);

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 (7), to a receiver (6) held by the user, the receiver (6) comprising 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;

accepting input of Code C to the terminal (2) by the user;

comparing Code C with Code B; and

permitting access to the host system (1) only if Code C matches Code B.

2. A method as claimed in Claim 1, wherein the transformation algorithm identified by the input user identification code comprises a one-way algorithm.

3. A method as claimed Claim 1 or Claim 2, wherein the receiver (6) 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.

4. A method as claimed in any one of Claims 1 to 3, wherein the signal incorporating Code A which is transmitted by the paging system (7) 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.

5. A method as claimed in Claim 4, wherein the receiver (6) is always responsive to reception of its identifier regardless of whether or not it has been enabled by the user.

6. A method as claimed in any one of Claims 1 to 5, wherein the remote terminal (2) comprises a central processing unit (CPU) and the method comprises the additional steps of

generating an access code by the terminal (2) based on the user identification code and at least one of a terminal code for identifying the remote terminal, a network identification code for identifying which of a plurality of networks the remote terminal is connected to, and a software code identifying the presence or absence of particular software stored at the remote terminal site and accessible by its CPU;

transmitting the access code to the host computer system (1);

deconstructing the access code to produce at least one computer identification code and the user identification code;

generating a second random code (Code D);

subjecting Code D and the computer identification code to a transformation characteristic of a transformation algorithm so as to generate a transformed code (Code E);

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

passing Code D to the remote terminal (2) which also subjects Code D and the computer identification code to a

transformation characteristic of a transformation algorithm so as to generate a transformed code (Code F);

passing Code F to the receiver (6) from the remote terminal which also subjects Code A to a transformation characteristic of both the transformation algorithm identified by the input user identification code and Code F so as to generate the transformed code (Code C);.

7. A method as claimed in Claim 6, comprising the additional steps of

deconstructing the access code to produce the user identification code, a first computer identification code characteristic of the computer hardware identifying portions of the access code and a second computer identification code characteristic of the computer software identifying portions of the access code;

generating a second random code (Code D1) and a third random code (Code D2);

subjecting Code D1 and the first computer identification code to a transformation characteristic of a transformation algorithm so as to generate a transformed code (Code E1);

subjecting Code D2 and the second computer identification code to a transformation characteristic of a transformation algorithm so as to generate a transformed code (Code E2);

combining in a predetermined fashion Codes E1 and E2 or parts thereof to produce the transformed code (Code E);

passing Code D1 and Code D2 to the remote terminal (2) which subjects Code D1 and the first computer identification code to a transformation characteristic of a transformation algorithm so as to generate a transformed code (Code F1), and which subjects Code D2 and the second computer identification code to a transformation characteristic of a transformation algorithm so as to generate a transformed code (Code F2); and

combining in a predetermined fashion Codes F1 and F2 or parts thereof to produce the transformed code (Code F).

8. A method as claimed in Claim 6 or Claim 7, wherein the receiver (6) can be releasably connected to the remote terminal (2) by means of a plug and socket arrangement or an infrared transmission system for the passage of information therebetween.

9. A method as claimed in any one of Claims 1 to 8, wherein the host computer system (1) comprises a security server system (5) which generates each of the random codes, stores the transformation algorithms identified by the input user identification codes, and transmits codes to the receiver (6) via the paging system (7).

10. Apparatus for preventing unauthorized access to a host computer system (1) by a user at a remote terminal (2), the apparatus comprising

means for accepting a user identification code input 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 system (7);

a receiver (6) held by the user, the receiver (6) comprising 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;

means (8) 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.

11. Apparatus as claimed in Claim 10, wherein the remote terminal (2) comprises a central processing unit (CPU).

12. Apparatus as claimed in Claim 11, wherein the receiver (6) can be linked to the central processing unit (2) either by a plug/socket arrangement or by an infrared transmission system for the passage of information therebetween.

13. Apparatus as claimed in Claim 11 or 12, wherein the remote terminal (2) comprises a terminal connected into a token ring network.

14. Apparatus as claimed in any one fo Claims 10 to 13, comprising a security server system (5) which generates each of the random codes, stores the transformation algorithms identified by the input user identification codes, and transmits codes to the receiver (6) via the paging system (7).

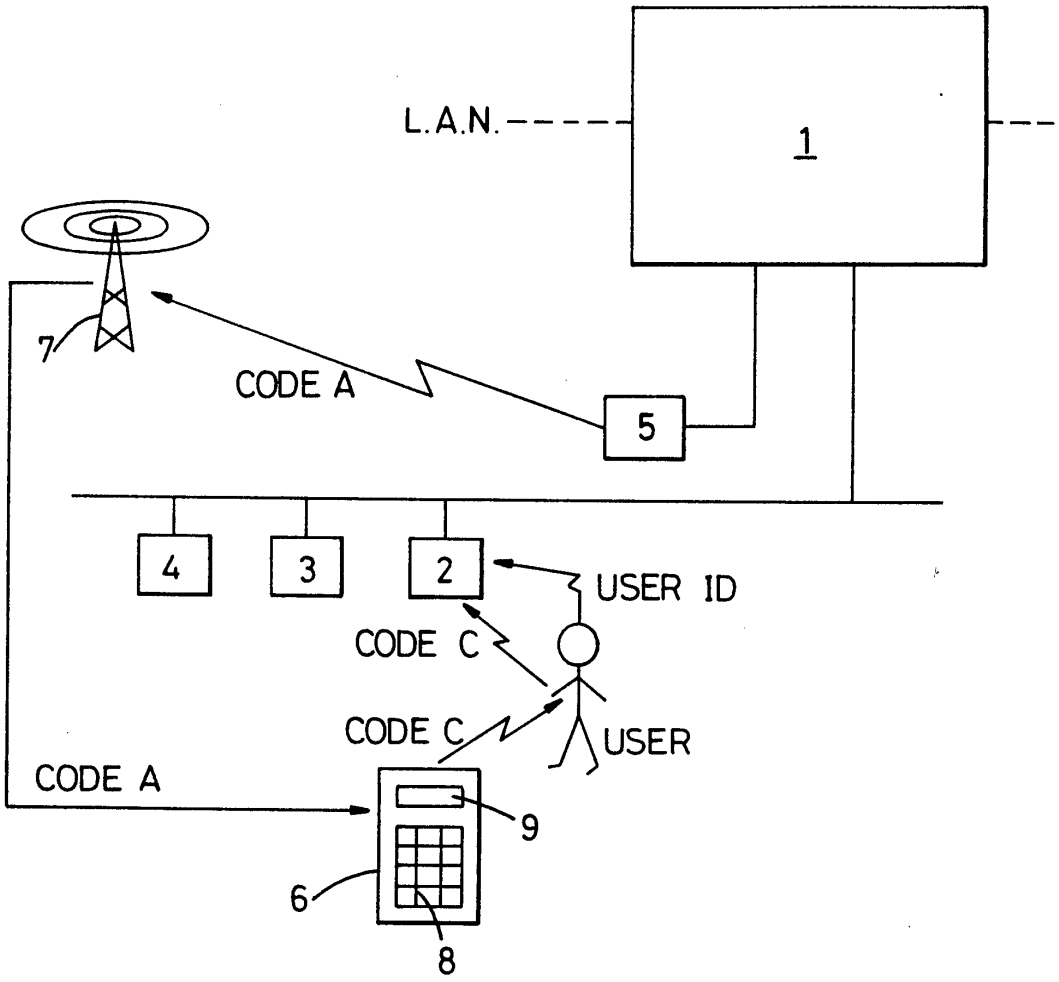


Fig. 1

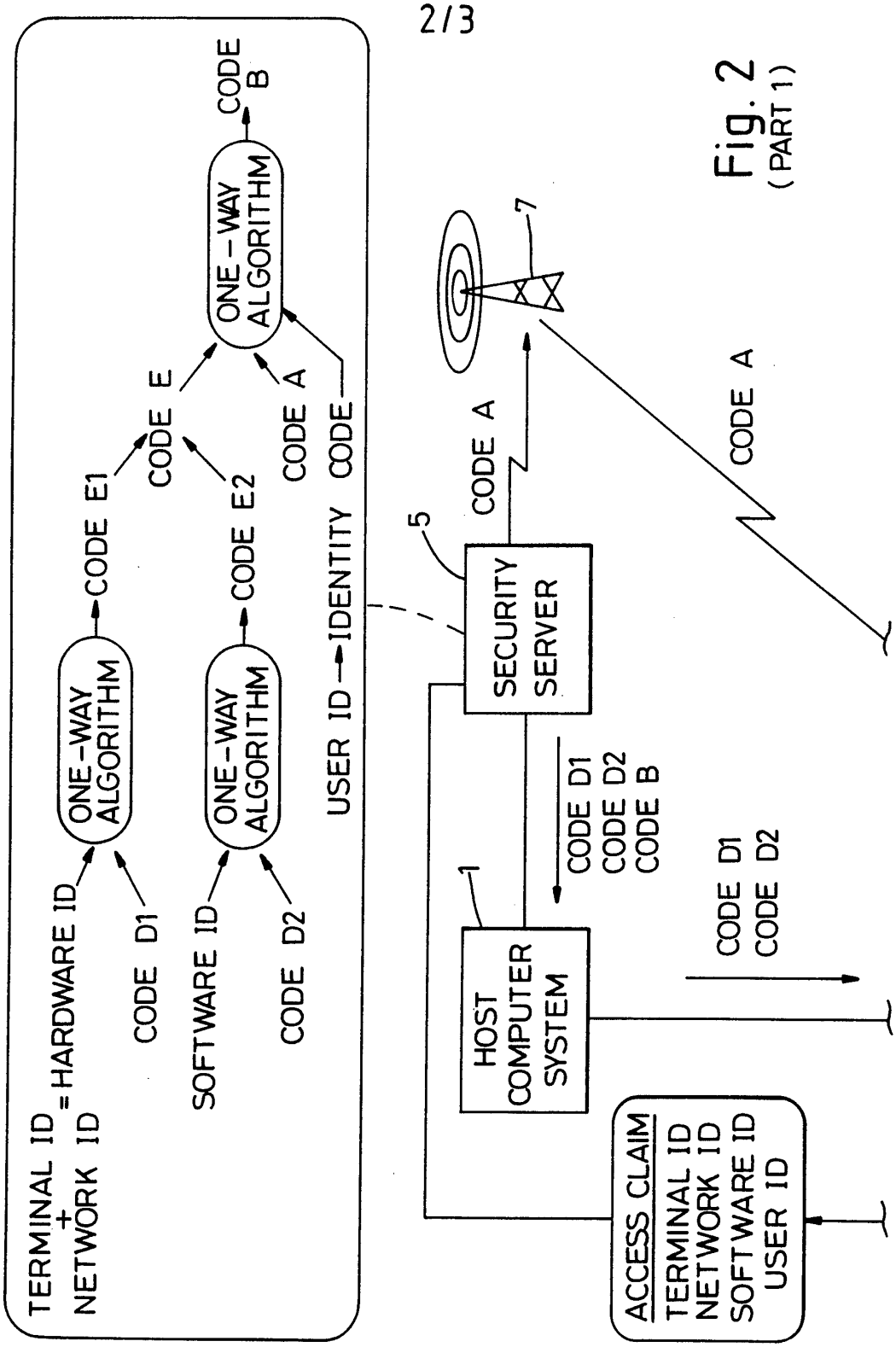

TERMINAL ID
+
NETWORK ID
=HARDWARE ID
CODE D1
ONE-WAY ALGORITHM
CODE E1
SOFTWARE ID
CODE D2
ONE-WAY ALGORITHM
CODE E2
CODE E
USER ID
IDENTITY CODE
CODE A
ONE-WAY ALGORITHM
CODE B
5
SECURITY SERVER
CODE A
7
CODE A
1
HOST COMPUTER SYSTEM
CODE D1
CODE D2
CODE B
CODE D1
CODE D2
ACCESS CLAIM
TERMINAL ID
NETWORK ID
SOFTWARE ID
USER ID

Fig. 2
(PART 1)

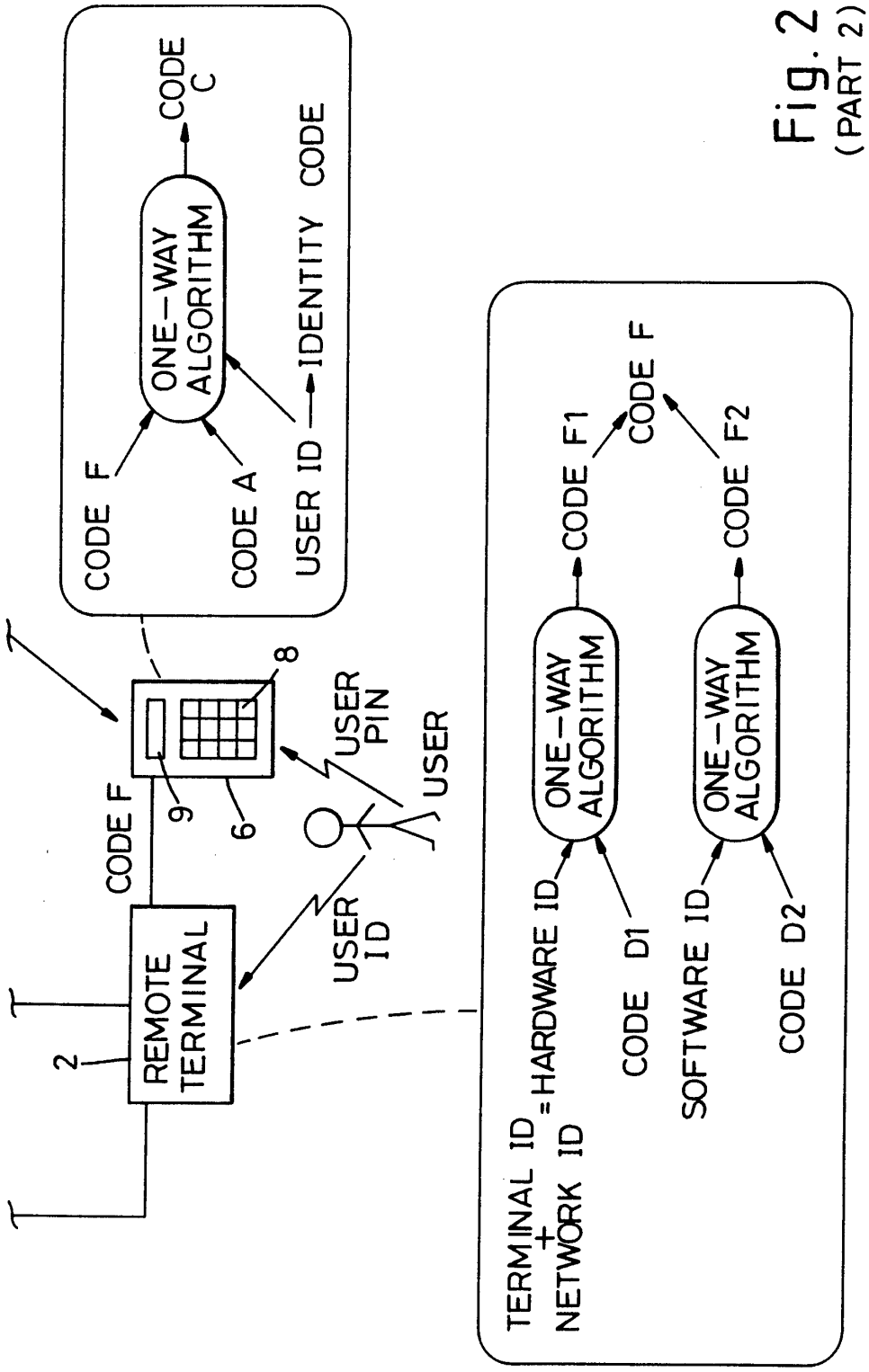

CODE F
CODE A
USER ID
ONE-WAY ALGORITHM
IDENTITY CODE
CODE C
CODE F
9
6
8
USER PIN
USER
USER ID
REMOTE TERMINAL
2
TERMINAL ID + NETWORK ID = HARDWARE ID
CODE D1
ONE-WAY ALGORITHM
CODE F1
SOFTWARE ID
CODE D2
ONE-WAY ALGORITHM
CODE F2
CODE F

Fig. 2
(PART 2)

INTERNATIONAL SEARCH REPORT

Inter. onal Application No
PCT/GB 95/00059

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00 G08B5/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F G08B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,4 679 236 (DAVIES) 7 July 1987 see the whole document ---	1-14
A	WO,A,90 13213 (GLOSTER ET AL) 1 November 1990 see page 6, last paragraph - page 7, line 14 -----	1,4,10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

·1

Date of the actual completion of the international search	Date of mailing of the international search report
4 May 1995	16. 05. 95
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Moens, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter .onal Application No
PCT/GB 95/00059

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-4679236	07-07-87	NONE	
WO-A-9013213	01-11-90	GB-A,B 2247810	11-03-92

Form PCT/ISA/210 (patent family annex) (July 1992)