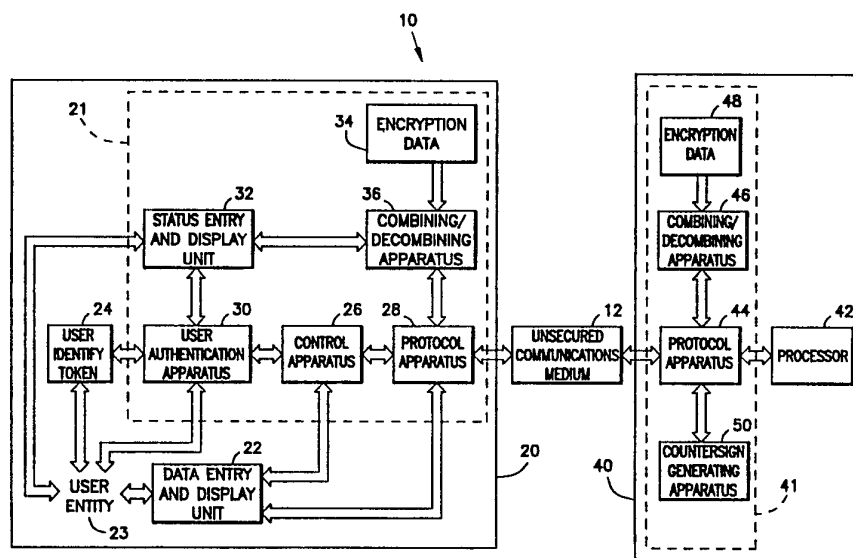




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁵ : H04K 1/00	A1	(11) International Publication Number: WO 92/17958 (43) International Publication Date: 15 October 1992 (15.10.92)
(21) International Application Number: PCT/US92/02381 (22) International Filing Date: 25 March 1992 (25.03.92) (30) Priority data: 676,885 28 March 1991 (28.03.91) US (71) Applicant: SECURE COMPUTING TECHNOLOGY CORPORATION [US/US]; 1210 West County Road E, Suite 100, Arden Hills, MN 55112 (US). (72) Inventor: BOEBERT, William, E. ; 4915 Dupont Avenue South, Minneapolis, MN 55409 (US). (74) Agent: HAMRE, Curtis, B.; Merchant, Gould, Smith, Edell, Welter & Schmidt, 3100 Norwest Center, 90 South Seventh Street, Minneapolis, MN 55402 (US).		(81) Designated States: AT (European patent), AU, BE (European patent), CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, LU (European patent), MC (European patent), NL (European patent), SE (European patent). Published <i>With international search report.</i>

(54) Title: SECURE COMPUTER INTERFACE**(57) Abstract**

Communication elements for secure data communication between remote nodes of a computer system on a standard communications medium (12). Terminals (21), workstations and personal computers are connected through a user-side terminator to a standard unsecured communications medium (12). Processors (42) are connected through a computer-side terminator (41) to the same medium (12). The combination of a user-side terminator (21), a computer-side terminator (41) and a standard communications medium (12) constitutes a secure computer interface.

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	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	RU	Russian Federation
CG	Congo	KP	Democratic People's Republic of Korea	SD	Sudan
CH	Switzerland	KR	Republic of Korea	SE	Sweden
CI	Côte d'Ivoire	LI	Liechtenstein	SN	Senegal
CM	Cameroon	LK	Sri Lanka	SU	Soviet Union
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
DE	Germany	MC	Monaco	TG	Togo
DK	Denmark			US	United States of America

SECURE COMPUTER INTERFACE

Background of the Invention

5 Field of the Invention

The present invention relates to an apparatus and method for secure communications between computers, and more particularly to the application of end-to-end encryption to ensure secure communications on standard
10 communications media.

Background Information

In the design of a secure computing environment the communication links are the most difficult to
15 protect and therefore the easiest to compromise. Terminals and computers can be placed in limited access, physically secure areas to limit exposure to hostile agents. But any computer with an electrical connection extending outside the physically secure area is subject
20 to penetration and compromise. Communication links can be attacked in a variety of ways. Active attacks are those in which masquerading "imposter" hardware or software is inserted into the link. For example, hardware might be inserted that emulates a user with
25 extensive access privileges in order to access sensitive information. Or a shell program may be constructed that deceives a user into revealing sensitive information such as a password. Passive attacks are those in which data on the link intended for one user is copied and
30 sent to another user, or captured by other individuals.

As computers have proliferated various methods have developed for computer-to-computer and computer-to-terminal communication. The first communications were point-to-point. However, as the number of points
35 increased, point-to-point communications became too complex and costly. For large networks over relatively short distances, point-to-point connections have been replaced with local area networks (LANs) such as Ethernet or Token Ring which permit communication

between a number of different computers and terminals on one or two wires.

For longer distances, modems offer a point-to-point link over a telephone line. Wide area networks (WANs) using combinations of fiber optic and copper telephone lines connect local area networks into larger networks.

Networks are at great risk in a security breach. The typical computer network functions like a telephone party line; anyone on the line can listen to and participate in the conversation. Passive attacks can eavesdrop on all communication on the network while active attacks have the potential to gain access to each network computer.

There are two aspects to security in a computer network with remote nodes. The first is authenticating the identity of both the source and the destination node in a communication. The second is making sure that communication between the nodes remains confidential.

Prior art systems have typically addressed one or the other of these security aspects. Perhaps the best known identity authentication method is the use of a password on logging into a system. Passwords provide a level of user authentication by tying a series of keystrokes to a user. The user must enter the password at the beginning of a session, or when moving to a higher level of access privilege.

A second method is the use of a dial-back modem. Dial-back modems are used to verify that the location of the remote device is one of the acceptable places for remote devices. This reduces the chances of an unauthorized user accessing the computer by requiring all remote access be performed from a set of authorized sites.

These techniques and others like them rely on restricting access to a computer service to authenticated users. Once the restriction is overcome,

access is achieved and there is no more checking. These methods offer limited feedback to the user; security is geared toward authenticating the remote site, not the computer being addressed. This approach is flawed in a security sense. There are certain functions where one wants to make sure that both ends - the computer and the user - are sure who is at the other end. The computer needs to make sure that it is talking to the authorized user and the authorized user needs to make sure he or she is talking to the computer and not some piece of malicious software masquerading as the computer.

Efforts to keep communications confidential have typically revolved around encrypting data prior to sending it on an unsecured medium or securing the medium by building a barrier around it to restrict access (hardening). Attempts to encrypt data traffic to improve security have encountered little commercial success due to a reliance on costly cryptographic devices which depend on complex and error-prone procedures for management of cryptographic keys and which may be subject to export restrictions. Hardening is often costly and may be impossible to accomplish (for instance, on public telephone lines).

It is clear that there is a need for an improved method of communication between computers and between computers and terminals that provides a high degree of security in data transfers. The method should provide a mechanism for authenticating the source node and the destination node in each message transfer and for maintaining confidentiality within each transfer. It should limit cost by permitting the use of standard communications methods and media.

Summary of the Invention

The present invention provides communication elements for secure data communication between remote nodes of a computer system on a standard communications

medium. Terminals, workstations and personal computers are connected through a user-side terminator to a standard unsecured communications medium. Processors are connected through a computer-side terminator to the same medium. The combination of a user-side terminator, a computer-side terminator and a standard communications medium constitutes a secure computer interface.

Transfers can be user node to user node, computer node to computer node or between a user node and a computer node. Communications between nodes are end-to-end encrypted under user control using a one-time pad algorithm.

Access to the computer system is restricted. To gain access to a user node, a prospective user must insert a token containing his name and access authorization level into the user-side terminator attached to the terminal at that node and then enter a password. A secure computer node verifies the user and restricts activity to the access authorization level.

According to another aspect of the present invention, a multilevel secure computer is connected through a computer-side termination to the unsecured communications medium. The combination of the secure computer interface and a multilevel secure computer provides a computing environment that is difficult to penetrate or compromise.

According to yet another aspect of the present invention, a countersign is provided to limit accesses to a secure user node by an agent using a reproduced token.

Brief Description of the Drawings

FIG. 1 is a system level block diagram representative of a user node and a computer node according to the present invention.

FIG. 2 is an electrical block diagram representation of a user node and a computer node according to the present invention.

5 FIG. 3 is a block diagram representative of a network of user nodes and computer nodes according to the present invention.

10 FIG. 4 is a flow chart representation of the steps taken in logging into a secure computer according to the present invention.

15 FIG. 5 is a flow chart representation of the steps taken in handling a compromised token according to the present invention.

20 FIG. 6 is a flow chart representation of the steps taken in entering the Trusted Path mode according to the present invention.

25 FIG. 7 is a flow chart representation of the steps taken in handling a garbled packet according to the present invention.

25 Detailed Description of the Preferred Embodiments

30 In the following Detailed Description of the Preferred Embodiments, reference is made to the accompanying Drawings which form a part hereof, and in which are shown by way of illustration specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

35 The present invention consists of communicating elements placed at remote nodes of a computer system. These elements implement end-to-end encryption with a one-time pad encryption algorithm to ensure secure

communication over unsecured media. End-to-end encryption, as distinguished from link encryption, is a technique whereby data is encrypted as close to its source node as possible and decrypted only at its ultimate destination. The present invention defines two modes of communicating between remote nodes of a computer system: Trusted Path and Untrusted User. In Trusted Path mode all message transfers are sent encrypted using the one-time pad encryption algorithm. In Untrusted User mode data is sent unencrypted. In the present invention, Trusted Path mode can be initiated and terminated by either node in a node-to-node transfer. Trusted Path mode cannot be used for broadcasting messages.

In the present invention, data is sent in packets. Encrypted messages are encrypted before being formed into a packet such that the packet protocol fields are left unencrypted. This is necessary for intelligible communication.

A one-time pad is an encryption technique in which a message of n bits is encrypted by combining the message with a random sequence of n bits, called a keystream. This type of cipher is theoretically unbreakable. The only way to recover the message is to decombine the encrypted message with the original random keystream. Therefore a copy of the keystream must be present in some form at both the source and destination. This requirement is usually met by delivering the keystream separate from the encrypted message using a separate trusted path to maintain confidentiality.

Each keystream is used one time then discarded. The first bit of a message is combined with the first bit of the keystream, the second with the second bit and so on. The next message to be encrypted starts after the last bit used in the previous message. Once the keystream is exhausted, message encryption is prevented until a new keystream has been installed. This is a

cardinal rule; keystreams that are used repeatedly increase the risk of providing enough information to break the code of previous messages. Nodes that communicate to more than one remote node require a
5 separate keystream for each remote node. For a fully secure system of n remote nodes, the system administrator may need to maintain up to $(n-1)$ factorial keystreams.

One-time pad combining and decombining can be
10 done using any reversible method, such as addition/subtraction with or without carry, or other, more complex algorithms. In the preferred embodiment of the present invention the one-time pad encryption algorithm enciphers a message of n bits by XORing it
15 with a random sequence of n bits. The message is then deciphered by XORing it with the same sequence of bits.

Trusted Path mode transfers provide protection against active and passive wire tapping through end-to-end encryption of all transfers. Agents monitoring the
20 communications medium can neither observe nor alter encrypted communications between the two nodes.

A computer system 10 incorporating a secure computer interface according to the present invention is shown in FIG. 1. Computer system 10 includes a user
25 node 20 connected through a communications medium 12 to a computer node 40. Computer node 40 acts as a server for a multi-user system. User node 20 serves as an interface between a user 23 and computer node 40.

Secure communications is ensured by encrypting
30 sensitive information that is to be transferred between user node 20 and computer node 40 on medium 12. All transfers, encrypted or not, are passed through a user-side terminator 21 in user node 20 and a computer-side terminator 41 in computer node 40. User-side terminator
35 21 and computer-side terminator 41 are the two ends of the secure communications path. Computer-side terminator 41 is connected to a processor 42 for

performing data processing while user-side terminator 21 is connected to data entry unit 22. In order to maintain security, each terminator must be placed in a physically secure area in close proximity to its
5 respective data entry unit 22 or processor 42. Data is formatted into packets and can be transferred as either encrypted (Trusted Path) or unencrypted (Untrusted User) data.

Computer-side terminator 41 encrypts and
10 decrypts Trusted Path data passed between processor 42 and communications medium 12. Computer-side terminator 41 is enclosed in a tamper-resistant housing separate from processor 42. Terminator 41 includes protocol apparatus 44, combining/decombining apparatus 46,
15 encryption data storage device 48 and countersign generating apparatus 50. Protocol apparatus 44 is connected to combining/decombining apparatus 46 and countersign generating apparatus 50. Protocol apparatus 44 packetizes data sent from processor 42 to
20 communications medium 12. That data may be sent either encrypted or unencrypted. If encrypted, data is sent through combining/decombining apparatus 46 for the performance of an encryption algorithm such as the one-time pad.

25 A user authentication apparatus 30 is provided to verify the identity of a user entity 23 who wishes to gain access to system 10. User authentication apparatus 30 is connected to control apparatus 26 and status entry and display unit 32. It is designed to accept a user
30 token 24 and to transmit information read from token 24 to processor 42. In order to gain access to computer system 10, a user identity token 24 belonging to user entity 23 is placed in proximity to user authentication apparatus 30. A password or other secondary means of
35 proving identity is entered through status entry and display unit 32 and used to verify that the proper user 23 is accessing system 10. Status entry and display

unit 32 also provides feedback to user entity 23 as to the status of communications medium 12.

Countersign generating apparatus 50 operates in conjunction with token 24 to provide another layer of computer system security. Each time a user 23 logs off the system countersign generating apparatus 50 generates a new countersign and sends the new countersign to user-side terminator 21 where it is written to token 24. This prevents an agent from making a copy of token 24 and repeatedly accessing computer system 10 as user 23. Use of more than one copy of token 24 in system 10 is detected through the countersign. An incorrect countersign results in processor 42 generating a "Countersign Failure" control packet and denying access to the user.

A copy of the keystream is kept at both ends of the medium 12 (in encryption data storage devices 34 and 48). As stated previously, each keystream is used only one time. Once exhausted, encryptions are prevented until a new keystream has been installed on both sides of medium 12. In computer system 10, combining/decombining apparatus 46 is connected to encryption data storage device 48 which provides the keystream data used in the one-time pad algorithm.

Likewise, user-side terminator 21 encrypts and decrypts sensitive data passed between data entry unit 22 and communications medium 12. In the preferred embodiment, user side terminator 21 is enclosed in a tamper-resistant housing separate from data entry means 22 and having a control apparatus 26, a protocol apparatus 28, a user authentication apparatus 30, a status entry and display unit 32, an encryption data storage device 34 and a combining/decombining apparatus 36. Protocol apparatus 28 performs the packetizing function on data before transferring it out onto medium 12. Protocol apparatus 28 also receives packets from medium 12, removes the protocol layers, forwards the

message to data entry unit 22 and generates appropriate status messages. Protocol apparatus 28 is connected to combining/decombining apparatus 36 and data entry unit 22 for transfer of data to and from medium 12. Data may
5 be transferred as encrypted or unencrypted data. If encrypted, data is passed from protocol apparatus 28 to combining/decombining apparatus 36 for execution of the one-time pad. Combining/decombining apparatus 36, in turn, is connected to encryption data storage device 34
10 for retrieval of the keystream required for the one-time pad.

Control apparatus 26 is connected to protocol apparatus 28 for execution of the end-to-end verification tests required to prove secure
15 communication. Communication between control apparatus 26 and processor 42 can be either in encrypted or unencrypted message packets.

In the preferred embodiment, processor 42 is a multilevel secure computer capable of recognizing data
20 of varying sensitivity and users of varying authorizations, and ensuring that users gain access to only that data to which they are authorized. Such a computer is described in "Secure Computing: The Secure Ada Target Approach" by Boebert, Kain, and Young
25 published in *Scientific Honeyweller* in June, 1985 and disclosed in U.S. Patent Nos. 4,621,321; 4,713,753; and 4,701,840 granted to Boebert et al. and assigned to the present assignee, the entire disclosures of which are hereby incorporated herein by reference. A multilevel
30 secure computer comprises a Security Kernel used for enforcing the rules of access and an Untrusted Subset which performs the functions unrelated to security. The Security Kernel restricts the actions of software running in the Untrusted Subset such that malicious code
35 cannot affect other code or data in the system.

The use of a multilevel secure computer in conjunction with the present invention creates a

computing environment which is very difficult to penetrate or compromise. Data entry unit 22 communicates with the multilevel secure computer through communications medium 12 by means of user-side terminator 21 and computer-side terminator 41. All communication between user node 20 and processor 42 is handled by the Security Kernel. The Security Kernel verifies that data requested by data entry unit 22 is at an access level authorized for user 23 and that data to be stored in processor 42 by data entry unit 22 is written to files with the correct access levels.

During Trusted Path mode and when used with a multilevel secure computer, the countersign mechanism offers additional protection against malicious intrusion. Countersign generating apparatus 50 is implemented in software in the Security Kernel of the multilevel secure computer. Each time a user entity 23 is identified to the Security Kernel (e.g., each new session on processor 42), countersign generating apparatus 50 generates a fresh countersign. Countersigns are words, symbols, or phrases which are easy to remember and which are generated by some process which makes it computationally infeasible to guess from one countersign what the value of the next one will be.

This countersign is passed to the Security Kernel and presented by it as the header to each message it sends to user 23. The countersign is never made available to malicious software in the Untrusted Subset of processor 42, is protected by encryption when exposed to communications medium 12, and is computationally infeasible to guess. Its presence at the start of a message therefore is a positive indication to user entity 23 that the message is actually from the Security Kernel and not from malicious code or from an active wiretap on communications medium 12.

This approach provides a constant verification not only of the user's identity but also of the identity

of processor 42. This is crucial for the transfer of sensitive information.

An electrical block diagram representative of the preferred embodiment of computer system 10 of Fig. 1 is shown in Fig. 2. Data entry unit 22 is connected through user side terminator 64 to communications medium 80. Communications medium 80 is connected through computer side terminator 62 to multilevel secure computer 60. Multilevel secure computer 60 includes an operating system and the application code needed to interface to a remote node. User side terminator 64 encrypts sensitive information intended for computer 60 and sends it in packets over communications medium 80. Computer-side terminator 62 receives the encrypted data from medium 80, decrypts it and sends the result to computer 60. Likewise, computer-side terminator 62 encrypts sensitive information sent from computer 60 and sends it over medium 80 to user-side terminator 64 where it is decrypted and presented to data entry unit 22. User-side terminator 21 and computer-side terminator 41 can be realized in hardware, software or a combination of both and may reside as separate boxes or be integrated in a greater or lesser degree into data entry unit 22 and multilevel secure computer 60.

In the preferred embodiment, user side terminator 64 is enclosed in a separate housing having a controller 66 connected to a media interface 67, a keystream storage device 68, a mode select button 69, a token reader 70, an LED 71, a user authentication device 72 and a display device 74. Mode select button 69 can be actuated by user 23 to move between Trusted Path and Untrusted User modes. LED 71 is a standard light emitting diode used to indicate Trusted Path mode (ON) or Untrusted User mode (OFF). User authentication device 72 is a keypad that can be used to enter a password in order to verify the owner of identity token

24. And display device 74 is an LCD display for displaying status and error messages.

In an alternate embodiment, user authentication device 72 could include a biometric device for
5 determining a unique physical attribute of user 23 such as fingerprints, palmprints or retinal pattern. That data would then be sent to computer 60 during the user verification process described in FIG. 4.

In the preferred embodiment, controller 66
10 includes a microprocessor and read-only memory. Program code for the encryption algorithm and for controlling message transfer and user interface control is stored in read-only memory and executed by the microprocessor.

Controller 66 receives messages from data entry
15 unit 22 intended for computer 60, encrypts those messages with the keystream stored in keystream storage device 68 and sends them to media interface 67. Media interface 67 packetizes the messages and sends the packets over communications medium 80 to computer-side
20 terminator 62. Computer-side terminator 62, likewise, is a separate enclosure containing a controller 76 connected to a media interface 77 and a keystream storage device 78. Media interface 77 receives packetized information from communications medium 80,
25 removes the packet protocol and sends the result to controller 76. Controller 76 performs the decryption and presents the decrypted messages to computer 60. Likewise, messages sent from computer 60 to data entry unit 22 are encrypted by controller 76 using keystream
30 storage device 78. The resulting packets are sent over communications medium 80 to the user side terminator 64. There they are decrypted and presented to data entry unit 22.

In the preferred embodiment, keystream storage
35 devices 68 and 78 are Digital Audio Tape (DAT) drives. Digital Audio Tape is used because of its superior density and since, due to the serial nature of the one-

time pad, DAT's higher seek times become less significant. Keystreams are generated at computer 60 and recorded on a DAT cartridge by device 78. One cartridge is then carried to the remote node by the system administrator. Encryption data cartridges must be protected by some appropriate physical security mechanism, such as storage in a safe, when the terminators are unattended.

A separate keystream is used for communication between each set of nodes that require enciphered communication. That keystream is used both to encrypt messages to be sent to the other node and to decrypt messages received from the other node. Therefore a separate remote node pointer pointing at its respective next keystream bit must be maintained at each node for all relevant remote nodes. If the pointers become unsynchronized, communication becomes undecipherable. If this should happen the first node to recognize the problem will resynchronize the keystream by sending an unencrypted message to the other node listing the location of the next keystream bit to use. In the preferred embodiment more than one keystream can be accommodated in each DAT device 68 or 78. That is, a tape cartridge can be segmented into as many keystream segments as necessary.

Once installed, a keystream is used until it is exhausted. Then a cartridge containing a new keystream must be installed in order to perform encryption.

In the preferred embodiment, user identity token 24 is a smart card, a planar module the size of a credit card which contains a microcontroller and nonvolatile memory. Token reader 70 is smart card reader capable of reading and writing data from user identity token 24. Communications medium 80 is Ethernet and media interfaces 67 and 77 are commercially available Ethernet interface integrated circuits used for implementing the TCP/IP protocol. The TCP/IP

protocol permits the use of different preambles in messages to the same node. In the present invention this is used to differentiate encrypted messages from unencrypted messages. Messages are encrypted prior to
5 being packetized. This is because protocol layers cannot be encrypted without being rendered unintelligible to standard Ethernet components.

In an alternate embodiment, communications medium 80 could be a telephone line and media interfaces
10 67 and 77 could be implemented with modems. In that implementation message packetizing would be performed by controllers 66 and 76.

In the preferred embodiment, controller 66 is connected to data entry unit 22 through a serial
15 communications link. Terminator 64 also provides power (not shown) to data entry unit 22 in order to perform a reset by cycling power. Data entry unit 22 can be a terminal, workstation or personal computer. Controller 76 is connected to computer 60 through a bus interface
20 card (not shown).

In order to maintain security it is necessary to reset data entry unit 22 to a known state at the initiation or termination of certain operations. A typical reset state for data entry unit 22 would be one
25 in which its display screen was blank and all internal storage (e.g., type-ahead buffers) was cleared. A typical situation requiring reset is when user entity 23 finishes work and leaves data entry unit 22 unattended; it should not be possible for an unauthorized person to
30 examine the residual data left on the display screen or probe data entry unit 22 for any residual data carried inside it. In addition, data entry unit 22 is reset each time user node 20 toggles from Untrusted User mode to Trusted Path mode and back.

35 The manner of this reset is dependent upon the degree to which user-side terminator 64 is integrated into data entry unit 22. If the degree of integration

is high, the reset may occur as the result of an internal control signal. If user-side terminator 21 is physically separate from data entry unit 22, then the reset may occur by a process such as cycling the power to data entry unit 22 off and on as in the preferred embodiment above, or by sending appropriate commands via the data stream for data entry unit 22.

Fig. 3 illustrates a network in which user nodes 20.1 through 20.N are connected over communications medium 80 to computer nodes 40.1 through 40.M. Each user node 20 includes a user side terminator 21 that serves as the interface between communications medium 80 and a data entry unit 22. Likewise, each computer node 40 contains a computer side terminator 41 which serves as the interface between communications medium 80 and a processor 42. Other data entry units 22 and processors 42 (not shown) could be attached to medium 80 without terminators 21 or 41. These nodes could only be used for unencrypted transfers.

Operation of controller 66 and controller 76 in user-side terminator 64 and computer-side terminator 74, respectively, will be described next. A sequence of steps representative of logging in to a secure computing system according to the present invention is illustrated in FIG. 4. On receiving power, controller 76 and computer 60 execute diagnostic self-tests and perform initialization routines. Computer 60 then waits for users to log in.

On receiving power, controller 66 and data entry device 22 execute power-on self tests and initialization routines. In the preferred embodiment data entry unit 22 is held reset until controller 66 successfully completes its initialization routines. On successful completion of the routines, at 100 controller 66 displays an "Insert Token" prompt on display device 74 and waits for the insertion of a token 24. The identification and authentication sequence begins at 102

when a user entity 23 approaches an unoccupied data entry unit 22 and inserts token 24 into token reader 70. Token reader 70 reads the contents of token 24 and, at 104, controller 66 prepares a "Initialize Authorization" control message and sends it as a packet to computer-side terminator 62. Computer-side terminator 62 receives the packet and forwards it to computer 60.

At 106, computer 60 generates an "Acknowledge Initialize Authorization" control message and sends it as a packet to user-side terminator 64. At 108, controller 66 receives the "Acknowledge Initialize Authorization" control message and displays a password entry prompt. The user enters a five digit password into authentication device 72 at 110 and, at 112, controller 66 builds a message containing the password and the user name, access authorization and last countersign. This message is sent as a packet to computer-side terminator 62. Computer-side terminator 62 receives the packet and forwards it to computer 60 for verification.

At 114, computer 60 checks the password for correctness. If the password is not correct, at 116 computer 60 sends a "PIN Failure" control packet to user-side terminator 64. Controller 66 receives the "PIN Failure" control packet and, at 118, increments the error count. If the error count is less than three, control moves to 108 where controller 66 again displays the password entry prompt. If the error count equals three, control moves to 124 where an unsuccessful login error message is displayed. The user must then remove his token before he tries to gain access again.

If, at 114, the password is correct, at 120 computer 60 checks the last countersign read from token 24. If the countersign is not as expected, at 122 computer 60 sends a "Countersign Failure" control packet to user-side terminator 64. Controller 66 receives the "Countersign Failure" control packet and moves to 124

where an unsuccessful login error message is displayed. The user must then remove his token before he tries to gain access again.

If, at 120, the countersign is as expected, at 5 126 computer 60 sends an "Acknowledge Authorization" control packet to user-side terminator 64. Controller 66 receives the "Acknowledge Authorization" control packet and moves to 128 where a welcoming message is displayed to the user.

10 User authorization is performed in Trusted Path Mode to protect the integrity of the password and countersign. In Trusted Path Mode all messages between data entry unit 22 or controller 66 and computer 60 are encrypted. Once the user is authorized, user 23 can 15 switch to Untrusted User mode by depressing mode select button 69. Untrusted User mode should be used for innocuous transfers such as electronic mail or public access data.

The sequence of steps that would lead to a 20 "Countersign Failure" control packet as in 122 above is illustrated in FIG. 5. An agent (spurious user) other than the legitimate user 23 gains access to token 24, makes a reproduction and returns the original token 24 undetected. Spurious user also gains knowledge of the 25 password associated with token 24 by looking under the desk mat at the desk of user 23. At 140, spurious user uses the token reproduction and the discovered password to gain access to a user node 20, log into the system and, at 142, to access files. At 144, spurious user 30 logs off the system, computer 60 updates the countersign associated with user 23 to a new countersign and that countersign is written by user-side terminator 64 to the reproduced token.

Some time later, at 146, legitimate user 146 35 attempts to login. Controller 66 and computer 60 go through the steps of FIG. 4 above and at 120 computer 60 determines that the countersign read from token 24 is

not the last countersign issued to that user. A "Countersign Failed" is issued at 122 and at 148 controller 66 issues a compromised token warning.

The countersign method does not eliminate the
5 threat of an illegitimate user gaining access to the system but it should severely cut down the time window during which that user can gain access to information.

The sequence of steps taken to enter Trusted Path mode is illustrated in FIG. 6. At 160 the
10 communication link between a user node 20 and a computer node 40 is in the Untrusted User mode. At 162 user 23 depresses mode select button 69 of user-side terminator 64. At 164, controller 66 of user-side terminator 64 generates a control message requesting a switch to
15 Trusted Path mode. That message is sent as a packet to computer-side terminator 62, processed and presented to computer 60.

At 166, computer 60 processes the request and at 168 returns a control packet acknowledge. Controller
20 66 receives the acknowledge and, at 170, clears the display of data entry unit 22, displays the countersign on the display of unit 22 and lights LED 71. All subsequent communication between node 20 and node 40 will be encrypted until mode select button 69 is again
25 depressed (to switch to Untrusted User mode) or the keystream falls out of synchronization.

FIG. 7 is a representation of the steps taken in handling a packet garbled in the transmission between two remote nodes in Trusted Path mode according to the
30 present invention. At 180, user 23 enters a command at data entry unit 22. At 182, the command is encrypted and transmitted to computer-side terminator 62. During transmission a portion of the packet is changed. This change is detected by computer-side terminator 62 at 184
35 through a cyclic redundancy check and the error is flagged to computer 60. At 186 computer 60 increments the keystream pointer and send the new pointer value in

an unencrypted message to user-side terminator 64. Controller 66 receives the new keystream pointer value at 188, sets its keystream pointer to that value, encrypts the message again and sends it as a packet to
5 computer-side terminator 62 so that at 190 normal processing resumes.

The present invention applies end-to-end encryption with the one-time pad to ensure secure communication. The one-time pad offers simplicity and,
10 with adherence to simple administrative procedures, unbreakable encryption of communications. The end-to-end characteristic of the encryption permits secure communication without the need to perform costly analysis of complex elements of typical multilevel
15 secure computers such as network controllers.

In addition, the present invention allows user entities to be identified and authenticated through a process which is simpler and more acceptable than present techniques such as passwords. It provides a
20 more secure identification and authentication process that can then be used with a variety of data entry and display devices, either as a separate unit or integrated inside them. And it provides the confidentiality of a true trusted path mode, immune to observation or forgery
25 by outside parties, with true authentication to either end of the communications path.

Although the present invention has been described with reference to the preferred embodiments, those skilled in the art will recognize that changes may
30 be made in form and detail without departing from the spirit and scope of the invention.

What is claimed is:

1. An apparatus for providing secure communication on a communication medium connecting a data entry unit to a computer, comprising:

computer-side terminator means connected to said communication medium and said computer for processing data as it passes between said computer and said communication medium, wherein said computer-side terminator means includes:

encryption means connected to said computer for selectively translating unencrypted computer data received from said computer into encrypted computer data;

packetizing means connected to said encryption means for forming encrypted and unencrypted computer data into computer data packets and writing said computer data packets to the communications medium and for receiving user data packets from said communications medium and translating the packets into received data; and

decryption means for translating encrypted received user data into unencrypted received user data and transferring unencrypted received user data to said computer;

user-side terminator means connected to said communication medium and said data entry unit for processing data as it passes between said data entry unit and said communication medium, wherein said user-side terminator means comprises:

encryption means connected to said data entry unit for selectively translating unencrypted user data received from said data entry unit into encrypted user data;

packetizing means connected to said encryption means for forming encrypted and unencrypted user data into user data packets and writing said user data packets to the communications medium and for

receiving computer data packets from said communications medium and translating said computer data packets into received computer data; and

decryption means for translating said encrypted received computer data into unencrypted computer data and transferring said unencrypted data to said data entry unit.

2. The apparatus according to claim 1 wherein the user-side terminator means further comprises:

token interface means for receiving a token and generating token data; and

control means connected to said token entry means and said encryption means for transferring said token data through said encryption means to said computer-side terminator for token verification.

3. The apparatus according to claim 1 wherein the control means includes password means for entering a password and for transferring said password through said encryption means to the computer-side terminator, said password serving to verify the user of the token.

4. The apparatus according to claim 1 wherein the control means includes biometric means for measuring a physiological parameter associated with a user and for transferring said measurements through said encryption means to the computer-side terminator, said physiological measurements serving to verify the user of the token.

5. The apparatus according to claim 1 wherein each of said terminators includes keystream storage means connected to said encryption means and said decryption means for the storage of an identical keystream to be used in a one-time pad encryption algorithm and pointer means connected to said storage means for pointing to

the location of the next bit of the keystream that will be used for encryption or decryption.

6. The apparatus according to claim 5 wherein the keystream storage means includes a Digital Audio Tape (DAT) drive and the keystream is stored on DAT cassettes.

7. The apparatus according to claim 5 wherein the keystream storage means includes an optical disk drive and the keystream is stored on optical disk media.

8. The apparatus according to claim 5 wherein the keystream storage means includes a floppy disk drive and the keystream is stored on floppy disk media.

9. The apparatus according to claim 1 wherein the user-side terminator further comprises display means for displaying the status of the communications medium and for displaying error messages.

10. A method of ensuring secure communication between two nodes of a communications medium, comprising:

- establishing a keystream for a one-time pad encryption algorithm, wherein said keystream will be used only for communication between the two nodes;
- placing a copy of said keystream at each of the two nodes;
- encrypting data to be sent from one node to the next with the keystream;
- forming said encrypted data into a packet;
- sending the packet containing the encrypted data from one node to the next on said communications medium;
- checking the received packet for data corruption;

if the received packet is corrupted, generating an error message; and

if the received packet is correct, decrypting the received encrypted data.

11. The method according to claim 10 wherein:

the step of forming said encrypted data into a packet includes calculating a cyclic redundancy code;

the step of sending the packet containing the encrypted data from one node to the next on said communications medium includes sending said cyclic redundancy code; and

the step of checking the received packet for corruption includes checking the received packet for the correct cyclic redundancy code.

12. The method according to claim 10 wherein the method further comprises retransmitting said packet on receiving of a data corrupted error message.

13. A method for authenticating a prospective user of a secure communication link between a computer and a user interface, comprising:

providing a user-side terminator connected between said user interface and said communications medium, said terminator including keystream storage means and a token reader;

providing a computer-side terminator connected between said communications medium and said computer;

inserting a token into said token reader, said token including data identifying the user to whom the token is assigned;

reading said token to obtain token data including the identity of the user;

encrypting said token data and transmitting the encrypted data to said computer-side terminator;

decrypting the received encrypted token data and sending the resulting data to said computer;
comparing the received token data against a list of acceptable users; and
returning an error message if the user is not acceptable.

14. The method according to claim 13 wherein the user-side terminator further includes data entry means and the method further comprises:
entering a password into said data entry means;
encrypting said password and transmitting said encrypted data to said computer-side terminator;
comparing, at said computer, the received password to a list of passwords associated with said token; and
returning an error message if the password does not match the expected password.

15. The method according to claim 13 wherein the user-side terminator further includes biometric measuring means and the method further comprises:
measuring a physical attribute of the prospective user;
encrypting said measurement and transmitting said encrypted data to said computer-side terminator;
comparing, at said computer, the received physical attribute measurement to a stored measurement associated with said token; and
returning an error message if the measurement does not match the expected measurement.

16. A secure computer system, comprising:
a multilevel secure computer, said computer including security kernel means for enforcing a multilevel access security protocol and a program execution means for executing user programs;

computer-side terminator means connected to said computer and to a communications medium for processing data as it passes between said computer and said communications medium, wherein said computer-side terminator means includes:

encryption means connected to said computer for selectively translating unencrypted computer data received from said computer into encrypted computer data;

packetizing means connected to said encryption means for forming encrypted and unencrypted computer data into computer data packets and writing said computer data packets to the communications medium and for receiving user data packets from said communications medium and translating the packets into received data; and

decryption means for translating encrypted received user data into unencrypted received user data and transferring unencrypted received user data to said computer;

a data entry unit;

user-side terminator means connected to said communications medium and said data entry unit for processing data as it passes between said data entry unit and said communications medium, wherein said user-side terminator means comprises:

encryption means connected to said data entry unit for selectively translating unencrypted user data received from said data entry unit into encrypted user data;

packetizing means connected to said encryption means for forming encrypted and unencrypted user data into user data packets and writing said user data packets to the communications medium and for receiving computer data packets from said communications medium and translating said computer data packets into received computer data; and

decryption means for translating said encrypted received computer data into unencrypted computer data and transferring said unencrypted data to said data entry unit.

17. The apparatus according to claim 16 wherein the user-side terminator means further comprises:

token interface means for receiving a token and generating token data; and

control means connected to said token entry means and said encryption means for transferring said token data through said encryption means to said computer-side terminator for token verification.

18. The apparatus according to claim 16 wherein the control means includes password means for entering a password and for transferring said password through said encryption means to the computer-side terminator, said password serving to verify the user of the token.

19. The apparatus according to claim 16 wherein the control means includes biometric means for measuring a physiological parameter and for transferring said measurements through said encryption means to the computer-side terminator, said physiological measurements serving to verify the user of the token.

20. The apparatus according to claim 16 wherein each of said terminators includes keystream storage means connected to said encryption means and said decryption means for the storage of an identical keystream to be used in a one-time pad encryption algorithm and pointer means connected to said storage means for pointing to the location of the next bit of the keystream that will be used for encryption or decryption.

21. The apparatus according to claim 20 wherein the keystore storage means includes a Digital Audio Tape (DAT) drive and the keystore is stored on DAT cassettes.

22. The apparatus according to claim 20 wherein the keystore storage means includes an optical disk drive and the keystore is stored on optical disk media.

23. The apparatus according to claim 20 wherein the keystore storage means includes a floppy disk drive and the keystore is stored on floppy disk media.

24. The apparatus according to claim 16 wherein the user-side terminator further comprises display means for displaying the status of the communications medium and for displaying error messages.

25. A method for establishing a secure computer system having a remote user node, comprising:

- providing a multilevel secure computer, said computer including security kernel means for enforcing a multilevel access security protocol and a program execution means for executing user programs;

- providing a computer-side terminator including keystore storage means, data encryption means, data decryption means and interface means for communicating on a standard communications medium;

- providing a user interface for data entry;

- providing a user-side terminator including keystore storage means, data encryption means, data decryption means, a token reader and interface means for communicating on a standard communications medium;

- connecting said multilevel secure computer through said computer-side terminator to a communications medium;

connecting said user interface through said user-side terminator said communications medium; and
defining a user authentication mechanism wherein a token inserted into said token reader is read and its contents sent to the security kernel means of said multilevel secure computer for verification;
wherein a user, in order to access said multilevel secure computer, must insert a token into said token reader; the token must then be verified by said security kernel before said user interface is enabled.

26. An apparatus for limiting access to a computer system to authorized users, comprising:

computer-side terminator means connected to said communication medium and said computer for processing data as it passes between said computer and said communication medium, wherein said computer-side terminator means includes communications means for writing data received from said computer to the communications medium and for receiving data from said communications medium and transferring said data to said computer; and

user-side terminator means connected to said communication medium and said data entry unit for processing data as it passes between said entry unit and said communication medium, wherein said user-side terminator means comprises:

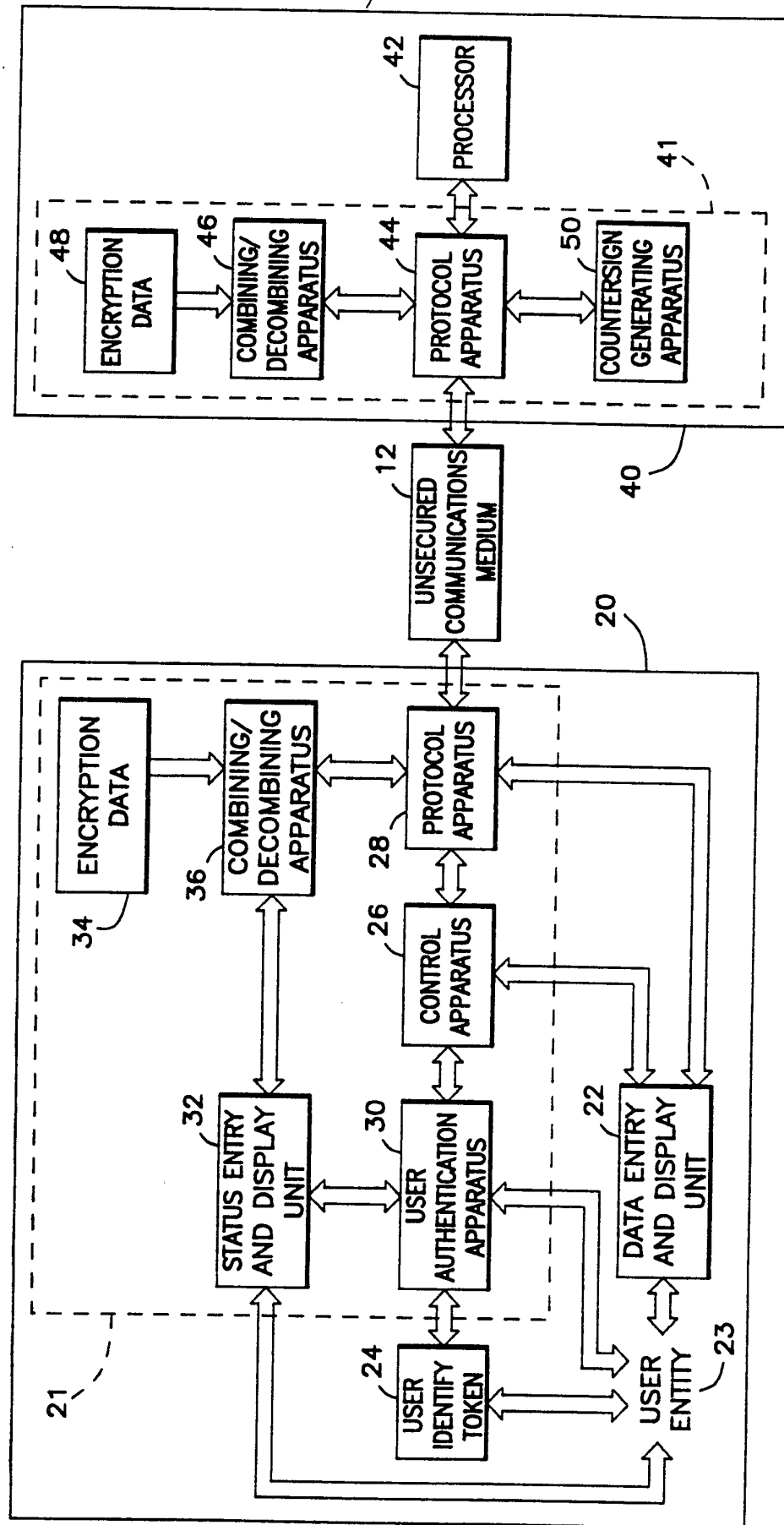
communications means for writing data received from said data entry unit to the communications medium and for receiving data from said communications medium and transferring said data to said data entry unit;

token interface means for receiving a token and generating token data; and

control means connected to said token entry means and said communications means for

transferring said token data through said communications means to said computer-side terminator for token verification.

FIG. 1



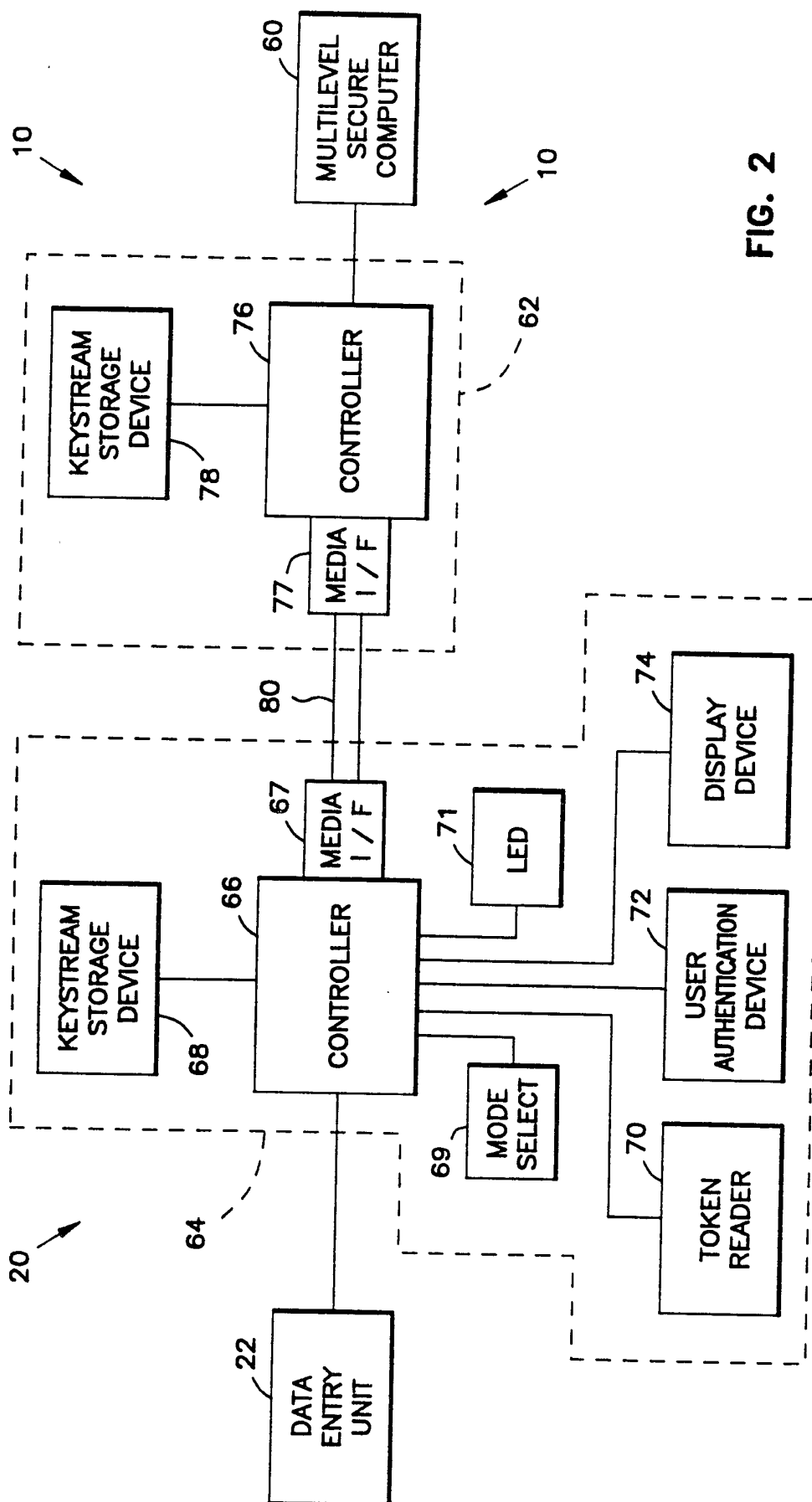


FIG. 2

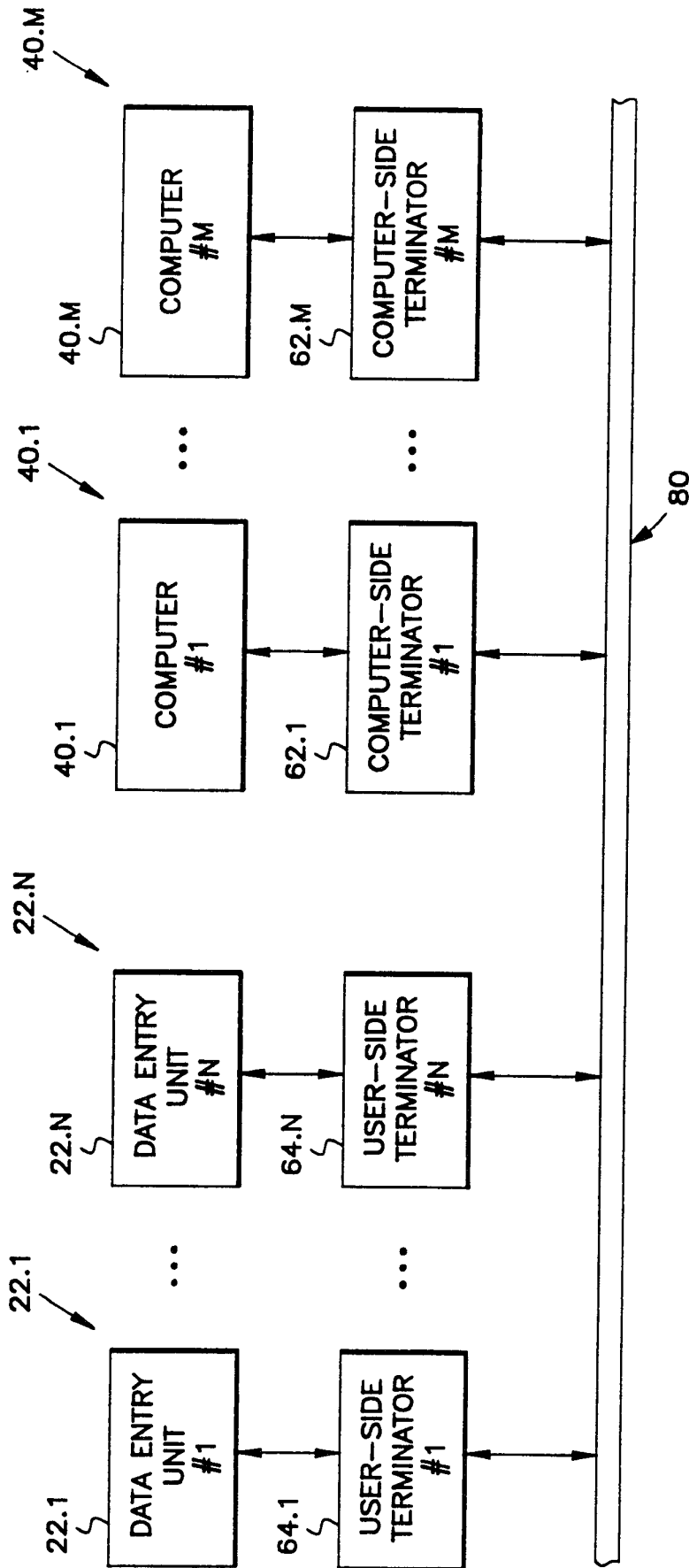


FIG. 3

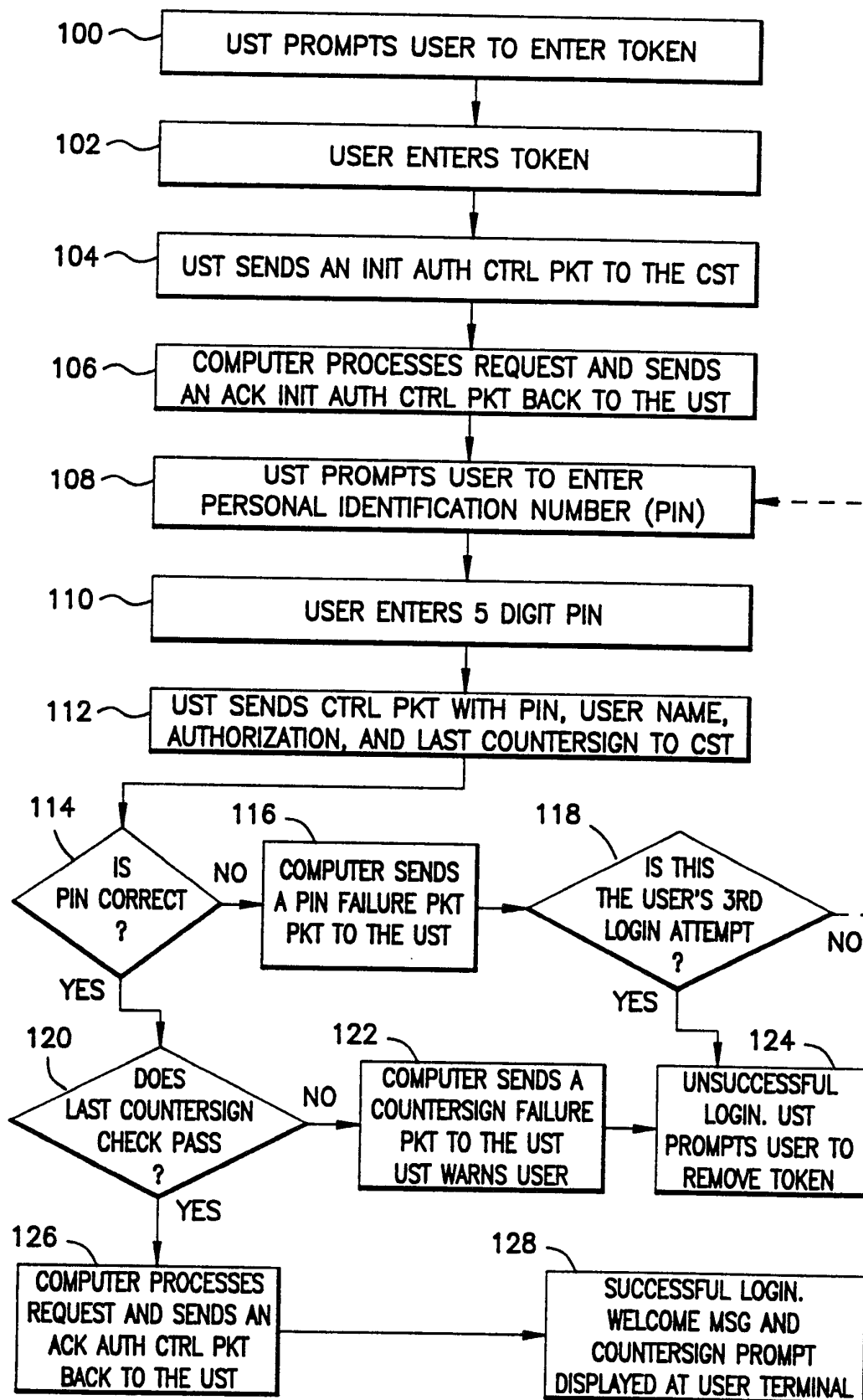


FIG. 4

5/7

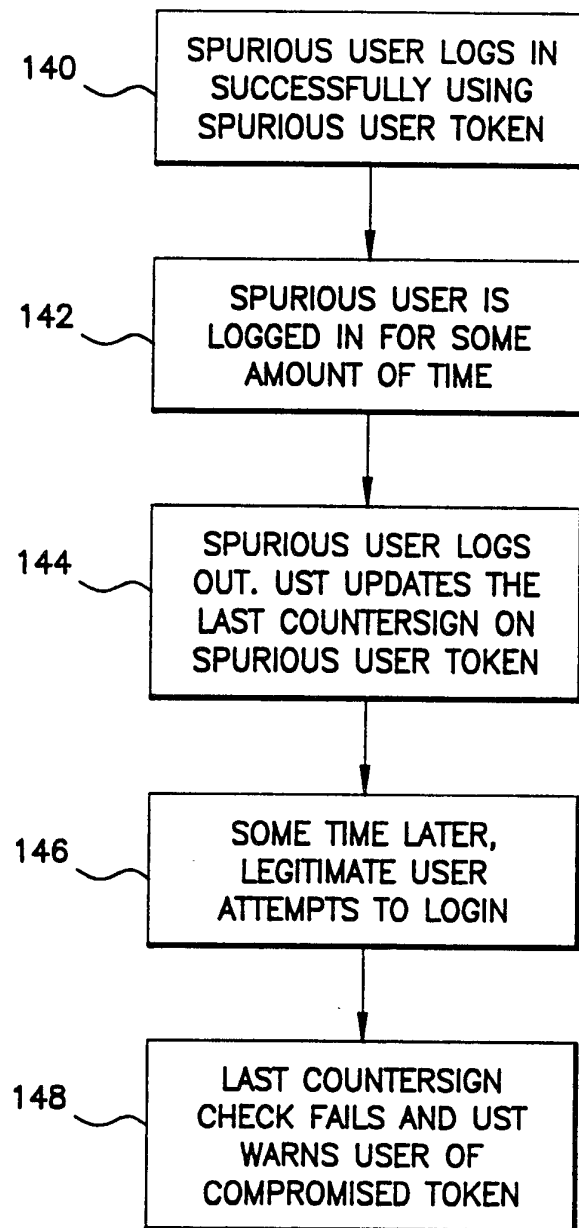


FIG. 5

6/7

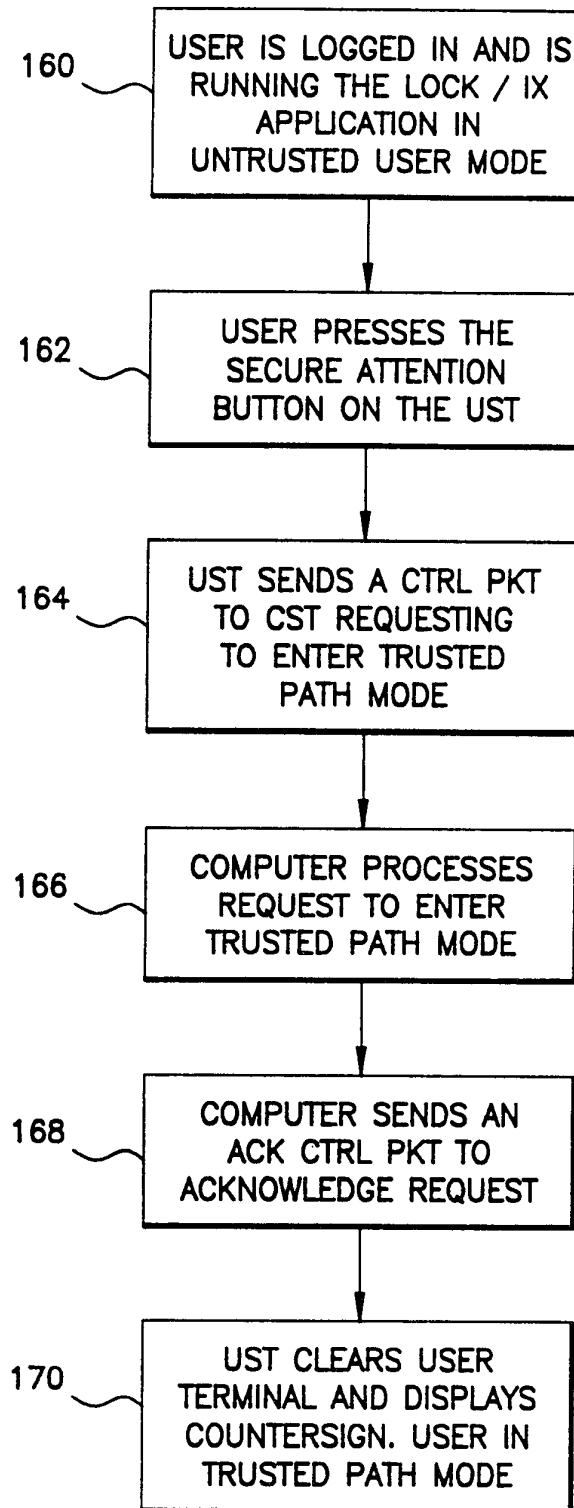


FIG. 6

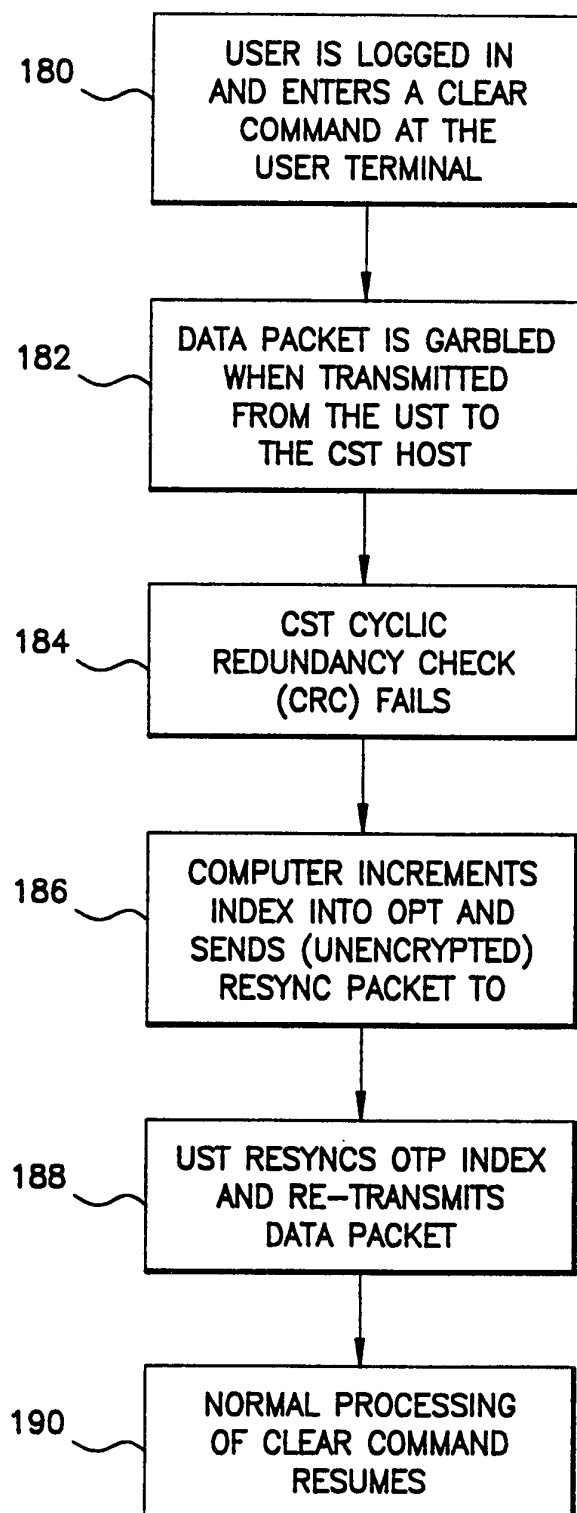
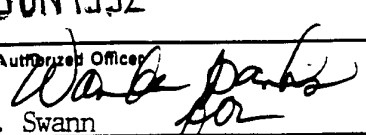


FIG. 7

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US92/02381

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) ⁶		
According to International Patent Classification (IPC) or to both National Classification and IPC IPC (5): H04K 1/00 U.S.Cl.: 380/25		
II. FIELDS SEARCHED		
Minimum Documentation Searched ⁷		
Classification System	Classification Symbols	
U.S.	380/23,24,25,49,4,47	
Documentation Searched other than Minimum Documentation to the extent that such Documents are included in the Fields Searched ⁸		
III. DOCUMENTS CONSIDERED TO BE RELEVANT ⁹		
Category ⁹	Citation of Document, ¹¹ with indication, where appropriate, of the relevant passages ¹²	Relevant to Claim No. ¹³
<u>X</u> Y	US, A, 4,438,824 (MUELLER-SCHLOER) 27 March 1984 See figure 5.	1-5,9-20 & 24-26 6-8 & 21-23
A	US, A, 4,998,279 (WEISS) 05 March 1991	1-26
A	US, A, 4,965,568 (ATALLA ET AL.) 23 October 1990	1-26
A	US, A, 4,885,789 (BURGER ET AL.) 05 December 1989	1-26
A	US, A, 3,956,615 (ANDERSON ET AL.) 11 May 1976	1-26
<div style="display: flex; justify-content: space-between;"> <div style="width: 48%;"> <p>¹⁰ Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"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)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> </div> <div style="width: 48%;"> <p>"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</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step</p> <p>"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.</p> <p>"&" document member of the same patent family</p> </div> </div>		
IV. CERTIFICATION		
Date of the Actual Completion of the International Search		Date of Mailing of this International Search Report
13 May 1992		19 JUN 1992
International Searching Authority		Signature of Authorized Officer
ISA/US		 Tod R. Swann