

SINGAPORE

**PATENTS ACT 1994
(ACT 21 OF 1994)**

THE PATENT RULES 1995

VERIFICATION OF TRANSLATION

I, Amy Jacobson

of 1941 Roland Clarke Place
Reston, Virginia 20191

hereby declare as follows:

1. I am a translator and am familiar with the English and German languages.
2. I am the translator of the documents attached hereto and certify that the following is a true translation of:

(a) the specification of International Bureau pamphlet numbered

WO 98/41003

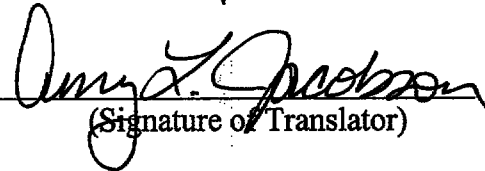
International Application No.PCT/CH98/00099

filed on March 11, 1998

to the best of my knowledge and belief.

Dated this 17th day of

February, 2000


(Signature of Translator)

Method for Protecting a Communications System from Unauthorized Access

The present invention concerns a method according to the introductory clause of claim 1.

5
In modern communications systems, large quantities of information (data and programs) are stored that are necessary for the operation and particularly for the user-specific configuration of the system. The information is distributed among various functional units of the system. Specifically, it involves data that is identical for all users
10 (global data), personal data on the users, and device-specific data of functional units of the system. These data must be protected against unauthorized access. The management of the information is preferably done in a central location from which it is transmitted as necessary to the applicable functional units of the system via data connections. From EP 0 735 785 A1 is known a communications system with a central system manager that can
15 be used as a dealer system. When the system is started up, the system manager ensures that all functional units up to and including the terminal devices are supplied with the necessary information. When the system manager, for example, a commercial personal computer, can be connected to the system via a known interface, the possibility that unauthorized third parties can access the system cannot be excluded with absolute
20 certainty.

Thus the object of the present invention is to preclude, under all circumstances, unauthorized access to information stored in a communications system.

25 This object is attained through the measures given in the characterizing section of claim 1. Advantageous embodiments of the invention are given in additional claims.

The comparison of the password stored in all functional units with a password that is compulsorily transmitted during establishment of a data connection ensures that
30 no unauthorized access to stored information is possible. If a participating functional unit

determines during establishment of a data connection that the transmitted password does not agree with the password stored in that unit, access to information stored in that unit is denied. Additional embodiments and advantages of the method can be seen from the description below.

5

The invention is described in greater detail below by way of example with the aid of a drawing. The drawing shows a digital communications system that is constructed according to the principle known from EP 0 745 785 - A1 with central and distributed functional units. The communications system consists essentially of a switching section VT and a great number of terminal devices EG connected to the switching section VT. Also connected to the switching section VT is a system manager SM. A computer with large memory capacity and with a video display can be provided as the system manager SM.

15 The switching section VT is comprised of a circuit switching network SWU, to which the circuit switching groups SLMY1 ... SLMY3 are connected. Each circuit switching group SLMY is connected on one side via an 8 Mbit line to a circuit switching network SWU and on the other side each via individual 8 Mbit lines to three multiplexers MUX. The circuit switching group SLMY has a coupler for switching the voice, data and signaling channels (time slots) coming from the circuit switching network SWU to the multiplexers. Ten terminal devices EG are each connected via their own 2 Mbit line to each multiplexer MUX. The multiplexers MUX have a coupler that switches the voice and signaling channels of the 8 Mbit line coming from the circuit switching groups SLMY to the appropriate terminal devices EG. The multiplexers MUX are controlled by the associated circuit switching groups SLMY. The circuit switching network SWU is a digital coupler with a control unit ST that serves to switch connections. This configuration makes it possible to connect any desired terminal devices EG with one another via the circuit switching groups SLMY and the circuit switching network SWU, and to exchange useful information in the form of data or program code and also voice information through these connections. An exchange of data between terminal devices

20

25

30

EG takes place, for example, when the current operating state in the terminal devices, such as the busy condition, is to be indicated at other terminal devices. Moreover, external lines, such as analog or digital lines (trunks La, leased lines Lb and dedicated lines Ls) leading to the public telecommunications network OEN, are connected via an interface module SLB to the circuit switching network SWU so that the terminal devices EG can also enter into connection via the switching section VT with partners that are not connected to this communications system. The number of circuit switching groups SLMY, multiplexers MUX, and terminal devices EG shown in the drawing is to be considered an example for the purpose of the present explanation; another configuration of the communications system realized according to this principle is also possible, of course.

The terminal devices EG form the interface between the users and the communications system. Depending on the application, they make a great number of convenient features available to the user. For example, in an embodiment of the communications system used for foreign exchange dealings in banks, the terminal devices EG, have for various inputs and outputs (such as destination selection), a keyboard with program-controlled LCD (Liquid Crystal Display) legends. Furthermore, a display screen with a user interface as well as hands-free and monitoring functions can also be provided in the terminal devices EG. In order to fulfill all these functions, each terminal device EG has its own processor that controls the relevant functions by means of software stored in an associated program memory or data memory. The software involved is switching software and operator software. The switching software controls all functions connected with communication, such as the monitoring and switching of connections (voice channels) to the multiplexers MUX and the circuit switching groups SLMY. The operator software primarily assumes control of the user interface with the keyboard and the display screen.

In the case of enhancements or user-specific modifications, it can become necessary to update information stored in functional units SLMY, MUX, EG of the

system. Thus, for example, information stored in the terminal devices EG (programs and/or data) must be updated because users desire a different configuration or additional features at their workplace. For this purpose, the appropriate information must be transmitted to the appropriate terminal devices EG. Another possible update in the terminal devices EG consists of relabeling a destination key because the associated line has changed. In the course of enhancements to the communications system, it can also become necessary to supply all terminal devices EG with new program versions. In this case, the terminal devices EG must be supplied with new program code and/or data. A change to the data in a circuit switching unit SLMY relates, for example, to the activation of a particular call forwarding route in the "night service" operating state.

The management of the information necessary for operation of the system and user-appropriate configuration of functional units SLMY, MUX and EG are performed by the system manager SM. The system manager SM forms the interface between the operator and the system. It is connected to the circuit switching network SWU via a special interface (with 2 B channels at 64 kbit/s and one D channel at 16 kbit/s) and an interface module SSB. The system manager SM has a large database, which contains, among other things, the data and programs for configuring the circuit switching groups SLMY, the multiplexers MUX and the terminal devices EG.

For transmitting information to a terminal device EG, for example, terminal device EG_n, the operator (system administrator) initiates at the system manager SM a function "Supply terminal device with new information." A loading procedure activated thereby establishes a connection via the circuit switching network SWU, the circuit switching unit SLMY1 and the multiplexer MUX1 from the system manager SM to the terminal device EG_n, which is identified by a device number known to the system manager SM. During this process, a free channel (time slot) is seized on the connection lines between the circuit switching unit SLMY1 and the multiplexer MUX1 and/or between the multiplexer MUX1 and the selected terminal device EG_n, by which means the transmission between the system manager SM and the terminal device EG_n can take

place via a data (point-to-point) connection, for example, with the HDLC protocol. As soon as the connection has been established, the terminal device EGn delivers a sign-on message to the system manager SM, whereupon the transmission of the information to the terminal device EGn begins. As soon as all information has been transmitted to the terminal device EGn, the system manager SM receives an appropriate disconnect message from the terminal device EGn, whereupon it terminates the connection with the terminal device EGn. In like fashion, information can be transmitted from the system manager SM to selected circuit switching units SLMY or multiplexers MUX using analogous procedures.

In its simplest form, the system manager SM can be a commercial personal computer that may be connected via a known special interface to the communications system. Access from the system manager SM to the communications system requires knowledge of the necessary procedures and protocols on the part of the human operator. Despite all conceivable security measures, the possibility that unauthorized third parties can acquire the necessary knowledge cannot be excluded with absolute certainty. Also for this reason, unauthorized access to the communications system and its functional units SLMY, MUX and EG cannot be completely excluded. For this reason, it must be prevented in all events that unauthorized third parties can gain access to the system and extract any information or undertake manipulations that cause service interruptions.

In principle, not only accesses that take place from a system manager SM belonging to the communications system are possible. Accesses that originate from a system manager SME connected to the public communications network OEN are also possible. In addition, accesses are also possible from a system manager SMF connected to a foreign communications system KA that can establish connections with the communications system in question via the public communications network OEN. If these are unauthorized accesses, they must be prevented under all circumstances.

The method according to the invention satisfies this requirement. It provides that

a certain password is entered at the system manager SM which governs access to the communications system that is managed by the system manager SM. At every startup, i.e., at the initial installation startup and at later startups, of the communications system or of parts of the system, at least one of the functional units of the system affected by the startup has transmitted to it an address with which this functional unit can establish a data connection to the system manager SM. Preferably selected as address recipients are functional units that can directly reach as many peripheral functional units of the communications system as possible in a simple way. A centrally located functional unit is selected as the address sender. In the case at hand, the address is sent by the control unit ST of the circuit switching network SWU to the circuit switching groups SLMY1, ... , SLMY3. The address is entered into the control unit ST upon initial installation startup via a central control terminal BT that is used for configuring the switching section. After receiving the address, the circuit switching groups SLMY1, ... , SLMY3 each establish a connection via the circuit switching network SWU to the system manager SM and prompt it to transmit the current password. Then the password is transmitted through the established connection by the system manager SM to the circuit switching groups SLMY1, ... , SLMY3. Following termination of the connection between the circuit switching group SLMY and the system manager SM, each circuit switching group SLMY transmits the password to the associated multiplexer MUX via signaling channels and thence to the connected terminal devices EG. The password is stored in all functional units SLMY, MUX, and EG of the communications system.

When a terminal unit EG is newly attached to a connection of the communications system, the terminal unit is logged on to the associated circuit switching group SLMY through a procedure initiated in the terminal unit, whereupon it transmits to the terminal device the current password, among other things.

Security can be additionally increased if the system manager SM checks, prior to transmitting the password to a requesting circuit switching group SLMY, using its source address, whether the circuit switching group SLMY is authorized at all to receive the

password. Security can be further increased in that the system manager SM verifies an entered password on the basis of various criteria (syntax, etc.) before accepting it.

5 Every time a connection is set up by the system manager SM belonging to the system in question or a foreign system manager SME or SMF for the purpose of exchanging information with functional units of the communications system, the system manager must send the password along with the connection request. Each functional unit involved in the connection (circuit switching group SLMY, multiplexer MUX and terminal device EG) verifies whether the password transmitted in the connection setup
10 information agrees with its stored password. If this is not the case, the functional unit denies access to the information that is stored in it and is to be protected. Likewise, the password is verified when functional units, such as two terminal devices EG, wish to exchange data with one another.

15 The system administrator, either a person authorized by the operator of the system or a person authorized by the manufacturer of the system, can enter the password at the system manager SM and later change it either as needed or as prompted by the system manager SM. It is also conceivable that the system manager SM automatically, i.e., without the participation of the system administrator, changes the password periodically
20 or at arbitrary times. In this case, the valid password is not known to anyone, which considerably increases security against unauthorized access.

 When the password is changed at the system manager SM, it transmits the new password with a change identifier as described to all circuit switching groups SLMY,
25 which then pass on the new password to all functional units MUX and EG of the communications system that they can reach directly, where it replaces the old password. To increase security, a further embodiment of the method provides for the old password to be transmitted simultaneously with the new password when the password is being changed, with the new password being accepted in the affected functional unit only if the
30 old password received agrees with the preexisting old password.



CLAIMS

1. Method for protecting a communications system from unauthorized access to information that is stored in the functional units (SLMY, MUX, EG) of the system and that can be supplied thereto for configuration by a system manager (SM; SME; SMF) via data connections,
5 **characterized in that** a password corresponding to the access authorization is entered in the system manager (SM),
in that at every startup of the system or of parts of the system, an address identifying the system manager (SM) is transmitted to at least one of the functional units (SLMY) of the communications system affected by the startup whereupon the functional unit (SLMY)
10 sets up with this address a connection to the system manager (SM),
in that the system manager (SM) then transmits the password to the functional unit (SLMY),
15 in that the functional unit (SLMY) then transmits the password to all functional units (MUX, EG) reachable by it, and
in that, at every subsequent establishment of a data connection from a system manager (SM; SME; SMF) to functional units (SLMY, MUX, EG), this password is appended to the connection setup information and verified by each of the addressed functional units
20 (SLMY, MUX, EG) for agreement with the password it has stored.
2. Method according to claim 1, characterized in that also during establishment of data connections between functional units (SLMY, MUX, EG) the password is appended to the connection setup information and verified by each of the addressed functional units
25 (SLMY, MUX, EG) for agreement with the password it has stored.
3. Method according to claim 1 or 2, **characterized in that** the system manager (SM), prior to transmitting the password to a functional unit (SLMY) requesting the password, verifies the authorization of that functional unit (SLMY).

30



4. Method according to claim 1, **characterized in that**, when the password is being changed, the new password is transmitted along with a change message to at least one functional unit (SLMY), which then transmits the new password to all functional units (SLMY, MUX, EG) reachable by it.
- 5
5. Method according to claim 4, **characterized in that** both the old password and the new password are transmitted to the functional unit (SLMY) along with the change message.
- 10
6. Method according to claim 4 or 5, **characterized in that** the password can be changed by a system administrator at the system manager (SM) at any time, or upon prompting by the system manager (SM).
- 15
7. Method according to claim 4 or 5, **characterized in that** the password can be changed automatically by the system manager (SM) either periodically or at arbitrary times.
- 20
8. Method according to one of the preceding claims, **characterized in that** a password entered at the system manager (SM) is verified upon entry on the basis of predetermined criteria.

Abstract of the Disclosure

The method prevents unauthorized accesses to operating information that is stored in functional units (SLMY, MUX, EG) of a communications system and can be supplied thereto from a system manager (SM) via data connections for configuration. For this purpose, a password appropriate for access authorization is entered in the system manager (SM). At every startup of the system, an address identifying the system manager (SM) is transmitted to at least one of the functional units (SLMY) of the system, whereupon the functional unit (SLMY) establishes a connection with this address to the system manager, which then transmits the password to the functional unit (SLMY). Subsequently the functional unit (SLMY) transmits the password to all functional units (MUX, EG) reachable by it. Upon every establishment of a data connection to functional units (SLMY, MUX, EG), the password is appended to the connection setup information and the password is verified by each of the addressed functional units (SLMY, MUX, EG) for agreement with the password stored therein.

(Fig.)

