PROCESS FOR PROTECTING A STATION'S ACCESSES TO AT LEAST ONE SERVER AND DEVICE WHICH IMPLEMENTS THE PROCESS

The present invention relates to a process for protecting a station's accesses to at least one server and a device which implements the process.

The need to protect the communications between servers and stations in communication networks is known, especially when these communications involve sensitive information for applications executed in the station in cooperation with the server. Up to now the protection principal consisted of adding, between the application and the layers of communication protocols in the network, part of a protection program. This program layer was installed both in the terminal and in the server. The disadvantage of such a method is that it requires a modification of the applications or the telecommunication layers and a program part for producing the interface between the protection program itself and the specific application. Thus, for each application, it is necessary to develop a specific program interface. Moreover, each server, insofar as the terminal is connected to a multiserver network, must be protected. The programming time necessary to protect each server would be a heavy burden on the budget required to protect an application.

The object of the invention is to propose a protection process which does not require any modification of the application programs executed in the terminals or any modification of the servers.

This object is achieved by the fact that the process makes it possible to protect the accesses originating from user stations whose destination is at least one application server linked through a network using a multisession, multiport telecommunication protocol, which process consists of a step for the systematic establishment of a parallel security session

between the user station and a security processor interposed between the user station to be protected during application sessions and the server or servers to be protected, and a step for the cyclic initiation of security sessions.

According to another characteristic, the step for the systematic establishment of a security session includes the following steps:

- transmission by the station through the network of a source IP address and at least one port number associated with the application requested by the station;

- a search by the security processor for the security script associated with the application;

- establishment of the security session between the security processor and the station; a search by the security processor in a local file of the processor for the name and address of the remote server used for the application and the opening of a connection with the remote server by communicating an IP address and a port number.

According to another characteristic, the script associated with an application consists of directly establishing the link between the station and the remote server chosen by the security processor.

According to another characteristic, the security script to be implemented, defined in a stored table, makes it possible to choose one or more of the following functions -- user authentication, identification, verification of the user's rights, certification, encryption key calculation, signature calculation, verification of user profiles -- to provide selective access to the applications requested from the server.

According to another characteristic, the security processor stores a journal in a mass memory comprising a sequential connection number, the connection dates and beginning and end times, the source IP address and at least one port number, the identifier of the security object used, the name of the remote

server chosen, the destination IP address and port number, and the execution rules.

According to another characteristic, the security processor stores in a second table of a memory a list of the applications processed by the processor, the operations to be executed as a function of the connection type, the security scripts to be implemented, the access rights of the users as defined by a black list, a white list and a subscriber list, and the schedules for the authorization of access to the remote servers.

Another object of the invention is to propose a device which makes it possible to implement this process.

This object is achieved by the fact that the device enables the process to be implemented between, on the one hand, a terminal in which is installed security software which manages the exchanges with the card and a card reader associated with the terminal as well as the exchanges with a multisession, multiport communications protocol, and on the other hand a security processor, characterized in that the security processor includes means for establishing and controlling communications between the station and a server chosen by the processor as a function of the application requested by the station.

According to another characteristic, the means for establishing and controlling communications make it possible either to establish direct communication between the terminal and the server, or to establish communication between the terminal and the server after establishing a security session controlled by a security device which comprises a microprocessor equipped with the memories required for its operation and which communicates with security control modules SAM which enable the security scripts to be interpreted, as determined by a main processor which executes the communication server and security engine programs.

According to another characteristic, the means for establishing communications are constituted by two local network

cards such as, for example, Ethernet or token ring cards, one of which is linked to the station, while the other is linked to the server and communicates with the station and the server using the multisession, multiport communication protocol.

Other characteristics and advantages of the present invention will become more clearly apparent with a reading of the following description, made in reference to the appended drawings, in which:

Fig. 1 represents a view of the schematic diagram of the device which implements the protection process;

Fig. 2A represents the dialogue box managed by the security software of the terminal;

Fig. 2B represents another dialogue box which indicates the absence of any card in the reader;

Fig. 2C represents another dialogue box requesting the user's personal identification number;

Fig. 2D represents another dialogue box which makes it possible to select the destination server;

Fig. 2E represents another dialogue box which allows a character string to be entered;

Fig. 2F represents the main window.

The invention will now be described in connection with Figs. 1 and 2. The invention is installed in a network constituted by terminals (2) which communicate through a network constituted by links (42, 40, 41) with one or more servers (30, 31). The terminals can either be connected locally to the network of the server or can be mobile, portable microcomputers which connect through telecommunications networks of any type -- connected network, GSM, ISDN. Numerous applications run on networks of this type, such as a remote terminal application service, for example Telnet, or file transfer services such as for example FTP, or protocols used by INTERNET such as HTTP or any other application which is currently known. The network is constituted by local network cards, for example Ethernet cards (23), in the

computer of the terminal which operate with a telecommunication protocol of the multisession, multiport type such as, for example, the TCP/IP protocol. Each server (30, 31) also includes an Ethernet card (302, 312) and an associated TCP/IP protocol (301, 311). To protect the network when the network includes several servers, it suffices to interpose, at the junction node of the servers located in the same enclosure as the servers, a security processor (1) which dialogues with one or more terminals (2) in the network. Each of the terminals (2) is equipped with a security application constituted by a piece of software (27) and a physical link (20) with a reader (21) of portable objects (22). These portable objects (22) can be chip cards or PC/MCIA cards.

The security processor (1) is constituted by a central processing unit (14) comprising a PC (Personal Computer) board with the corresponding memories and communicates through a bus (11) with a first network card of the Ethernet type (13) connected to each of the servers (30, 31) by a respective link (40, 41) and with a second network card of the Ethernet type (12) connected to the terminal by a link (42). The bus (11) also communicates with a security application card (15) which comprises a processing unit, memories which are not represented, and security control modules SAM (Security Application Module) (151, 152). The installation can include n cards, each of which comprises n security control modules SAM (151, 152). These modules SAM (151, 152) make it possible to perform, in connection with the reader (21) and the portable object, security functions such as authentication, certification, encryption key calculation, etc., while ensuring the inviolability of the basic secret keys. These security functions also use the information contained in the chip card or the portable object (22) linked by the reader (21) to the security application (27) of the terminal (2). The processing unit (14) operates with a multitask operating system (173), for example of the OS2 type, in order to allow the security processor (1) to execute several tasks

simultaneously. Each Ethernet card (12, 13) includes a software layer which makes it possible to implement the telecommunication protocol specific to the network, such as the TCP/IP protocol (131, 121). In addition to the operating system, the processing unit (14) operates with a communications server (172) which includes a layer (1721) for processing communications between the first card (13) and the second card (12) using the TCP/IP network protocol. The role of this communications server (172) is to determine whether the link between the second Ethernet card (12) and the first card (13) connected to the server should be made directly or if this link can only be made after the implementation of a security procedure. This determination is made by reading a file APPLI.INI stored in a memory (16) comprising a table of correspondence between the application and at least the security script to be implemented. If an implementation is required, this communications server calls a security engine (171) which triggers the operation of the security application card (15) of the security processor (1), thus enabling the security functions to be implemented. The security engine MS makes it possible to configure the security network, to define the list of applications processed by the security processor, to define the operations executed, to define the security scripts to be implemented, to define the access rights of the users and the authorization schedules. The security application (27) installed in the terminal also operates with an operating system of the window display type such as the Windows (registered trademark) software. Once the security software (27) is loaded in the station, this station, by displaying a main window (Fig. 2F) which appears after the start of the security application, enables the user of the terminal to activate the security connection, to deactivate the security connection, or to exit from the application. As shown in Fig. 2F, the selection of one of the three available functions is made by moving the highlight to the desired function then validating

it with a mouse "click" or by hitting the "enter" key on the keyboard. The user connects to the protected network by indicating the IP address of the security processor (1) and the port number assigned to the application he wishes to use (for example, X for the security application, 21 for the FTP application, 23 for Telnet, etc.). The security processor (1) searches in a table for the security script associated with the port number sent by the station and then establishes a communication with the security application (27) in order to implement the security script which specifically includes the authentication of the portable user object (22) and the identification of the user through his personal identification number (PIN). Optionally, the security processor (1) can display on the station the list of applications, with those the user is permitted to use being defined by the white lists and those not permitted being defined by the black lists. The user then selects, through actions on the keyboard or the mouse, a server-application pairing. Once the security script is running normally, the user starts the selected application (Telnet, FTP, HTTP, etc.) by validating the selection. The security processor (1) receives from the terminal (2) a port number corresponding to the application, determines from its tables the IP address of the application server and establishes the connection with the application server requested. Once the connection is established between the terminal (2) and one of the servers (30, 31), the security processor supervises the application sessions established by performing cyclic security checks in the terminal (2). If an abnormal security condition is detected (such as a card removal, an idle period, a signature miscalculation, etc.), the security processor (1) interrupts the connections with the remote server and terminates the security session.

A plurality of security scripts can be used and the choice of which script to activate is made as a function of the port number of the application indicated in the connection data. This

port number and associated script information is in a file LOGON.CAM which constitutes part of a table (161) in the mass memory (16) of the security processor (1). The activation of a security connection implements a logon script which makes it possible to execute one or more of the following operations: data display and capture; source and destination IP address verification; access control by password; access control by means of a smart card which makes it possible to execute an identification of the cardholder, an authentication using a SAM security module, an encryption, a signature, a certificate calculation, a reading and writing of information, a card removal check, and the verification of the user's rights to access the remote server in the black lists, white lists, and subscriber lists, which access rights and lists constitute part of the table T (161); the verification of rights to use the various services of the TCP/IP telecommunication protocol; and the verification of the date and time slot authorized for the user or for access to the chosen machine, which authorized date and time slot is the object of a table which includes the time slots in columns and the identities of the users or machines in rows. Finally, the display of a personalized menu enables the user to choose one of the applications or remote servers he is authorized to use. The file APPLI.INI makes it possible to store in the memory (16), and to identify as a function of the application, the security script to be activated as well as the activation period, which makes it possible, in accordance with the script and the activation period chosen, to trigger the activation of a script cyclically as a function of the application of the remote server chosen. The periodic script verifies that the remote user is in fact the one who has been cleared by requesting the card in the terminal to execute electronic data (random number) signatures chosen by the script. The script is responsible for verifying, using SAM, that these signatures have been produced by a card which has the appropriate secret keys. This process makes it possible to guard

against, among other things, the stealing of IP addresses by an intruding device in the network. When the user has chosen the remote server and the application, the security processor retrieves the port number of the application and uses a local file to open a connection with the remote server chosen by the security processor. This server chosen by the security processor may be different from the one indicated by the user. The user will simply receive the communications through the security processor. These communications are addressed to the station (2) via its port number. Finally, the security processor, using the security engine (171), makes it possible to hold in the mass memory (16) a journal (162) of the connections which stores a sequential connection number, the connection dates and beginning and end times, the source IP address and the port number, the identifier of the security object used, the name of the remote server chosen, the destination IP address, the port number, the volume of data exchanged between the station and the server during the application session, and the execution rule. The security application (27) comprises a presentation module (271) which makes it possible to use the window and dialogue box display system of the Windows operating system to display a first dialogue box (Fig. 2A) requesting the user to enter a password and then to validate this word or to cancel the operation, which causes the deactivation of the security connection. The user interface also makes it possible to display a second dialogue box (Fig. 2B) indicating the messages "no card in reader" and "please insert your card" as well as a third dialogue box (Fig. 2C) which enables the user to enter his personal identification number, with buttons for validating or cancelling the procedure. Finally, the fourth dialogue box makes it possible to select the destination server by allowing a selection from a scrolling list of the possible servers in the network. There are two other dialogue boxes, one of which allows the display of messages received from the security processor, while another box (Fig. 2E)

makes it possible to request the entry of a character string. It is understood that the access is thereby protected, and the conditions for the access procedures can be selected by the person responsible for security, while the periodicity of the security connections prevents a hacker from connecting at a given moment by masquerading as someone else at the terminal connected to the network since if he does not have the access keys to the terminal, the security procedures do not identify him and terminate the session. Finally, this solution has the advantage of remaining transparent with respect to the protocol of the applications running on the connection. In effect, the installation of the security system is performed without modifying the applications in the terminals or even in the servers.

During the installation of the security software (27) and the security processor (1), the installer defines, in an initialization file (SERVER.INI) a security delay which allows the processor (1) to close the security connection established with a client station if there has been no application connection since the predetermined delay, and an inactivity delay which allows the processor to close the security connection and the application connections established with a client station if there have been no data exchanges in the application connections since the predetermined delay.

Other modifications within the scope of one skilled in the art are also part of the spirit of the invention.

CLAIMS

1. A process for protecting access to at least one server (30) characterized in that it makes it possible to protect accesses originating from user stations (2) whose destination is at least one application server through a network (42) using a multisession, multiport telecommunication protocol, said process comprising the following steps:

- a step for the systematic establishment of a parallel security session between the user station (2) and a security processor (1) interposed between the user station to be protected during application sessions and the server or servers (30) to be protected; and

- a step for the cyclic initiation of security sessions.

2. The process for protecting access to at least one server according to claim 1, characterized in that the step for the systematic establishment of a security session comprises the following steps:

- transmission by the station through the network of a source IP address and at least one port number associated with the application requested by the station (2);

- a search by the security processor for the security script associated with the application;

- establishment of the security session between the security processor (1) and the station (2);

- a search by the security processor (1) in a local file of the processor for the name and address of the remote server used for the application and the opening of a connection with the remote server (30, 31) by communicating an IP address and a port number.

3. The process for protecting access to at least one server according to claim 2, characterized in that the script associated with an application comprises the step which consists

of directly establishing the link between the station (2) and the remote server (30) chosen by the security processor.

4. The process for protecting access to at least one server according to claim 1, characterized in that the security script to be implemented, defined in a stored table, makes it possible to choose one or more of the following functions -- user authentication, user identification, verification of the user's rights, certification, encryption key calculation, signature calculation, verification of user profiles -- to provide selective access to applications requested from the server.

5. The process for protecting access to at least one server according to claim 1, characterized in that the security processor stores a journal (162) in a memory (16) comprising a sequential connection number, the connection dates and beginning and end times, the source IP address and at least one port number, the identifier of the security object used, the name of the remote server chosen, the destination IP address and port number, and the execution rules.

6. The process for protecting access to at least one server according to claim 1, characterized in that the security processor (1) stores in a second table (161) of a memory (16) a list of the applications processed by the processor, the operations to be executed as a function of the connection type, the security scripts to be implemented, the access rights of the users as defined by a black list, a white list and a subscriber list, and the schedules for authorization of access to the remote servers.

7. A device for protecting, by means of a security processor (1), accesses originating from a user station (2) whose destination is at least one application server through a network (42) using a multisession, multiport telecommunication protocol,

security software (27) being installed in the station for managing exchanges with a portable object and a portable object reader (21) associated with the station as well as exchanges with a multisession, multiport communication protocol (24), characterized in that the security processor (1) comprises means for establishing (12, 13) and means for controlling (14, 15, 172, 171) communications between the station (2) and a server (30) chosen by the security processor as a function of an application requested by the station (2).

8. The device according to claim 7, characterized in that the means for establishing and controlling communications make it possible either to establish direct communication between the station (2) and the server or to establish communication between the station and the server after establishing a security session controlled by a security device which comprises a microprocessor equipped with memories required for its operation and which communicates with security control modules SAM which make it possible to interpret security scripts chosen by a main processor (14) running programs from a communication server (172) and a security engine (171).

9. The device according to claim 7, characterized in that the means for establishing communications (12, 13) are constituted by two telecommunication cards, one linked to the station, the other linked to the server and communicating with the station and the server using the multisession, multiport communication protocol.