PROCEDE DE SECURISATION DES ACCES D'UNE STATION A AU MOINS UN SERVEUR ET DISPOSITIF METTANT EN OEUVRE LE PROCEDE

La présente invention concerne un procédé de sécurisation des accès d'une station à au moins un serveur et le dispositif mettant en oeuvre le procédé.

Il est connu dans les réseaux de communication entre serveurs et stations de chercher à sécuriser les communications surtout lorsque celles-ci mettent en jeu des informations sensibles pour les applications exécutées sur la station avec le concours du serveur. Jusqu'à présent le principe de sécurisation consistait à rajouter entre l'application et les couches des protocoles de communication du réseau une partie de programme de sécurisation. Cette couche de programme était implantée à la fois sur le terminal et sur le serveur. L'inconvénient d'une telle méthode est qu'elle nécessite la modification des applications ou des couches de télécommunication et une partie de programmation réalisant l'interface entre le programme sécuritaire proprement dit et l'application spécifique. Pour chaque application il est donc nécessaire de développer une interface de programme spécifique. Par ailleurs chaque serveur dans la mesure où le terminal est connecté sur un réseau multi serveur, doit être sécurisé. Le temps de programmation nécessaire pour chaque application combiné à la nécessité de sécuriser chaque serveur venait grever lourdement le budget nécessaire pour sécuriser une application.

Le but de l'invention est de proposer un procédé de sécurisation qui ne nécessite aucune modification des programmes d'application exécutés sur les terminaux et aucune modification des serveurs.

Ce but est atteint par le fait que le procédé permet de sécuriser les accès en provenance de stations

d'utilisateur à destination d'au moins un serveur d'application relié à travers un réseau utilisant un protocole de télécommunication multi sessions et multi ports, ledit procédé consiste en une étape :

d'établissement systématique d'une session de sécurité en parallèle entre la station d'utilisateur et un processeur de sécurité interposé entre la station d'utilisateur à protéger pendant le déroulement des sessions d'applications et le ou les serveurs à protéger et une étape de déclenchement cyclique de session de sécurité.

Selon une autre particularité l'étape d'établissement systématique d'une session de sécurité comporte les étapes suivantes :

transmission par la station sur le réseau d'une adresse source IP et d'au moins un numéro de port associé à l'application demandée par la station ;

recherche par le processeur de sécurité du scénario sécuritaire associé à l'application ;

établissement de la session de sécurité entre le processeur de sécurité et la station ; recherche par le processeur sécuritaire dans un fichier local du processeur le nom et l'adresse du serveur distant utilisé pour l'application et ouverture d'une connexion avec le serveur distant par communication d'une adresse IP et d'un numéro de port.

Selon une autre particularité le scénario associé à une application consiste à établir directement la liaison entre la station et le serveur distant choisi par le processeur de sécurité.

Selon une autre particularité le scénario de sécurité à mettre en oeuvre et défini dans une table mémorisée permet au choix une ou plusieurs des fonctions ci-après d'authentification de l'utilisateur, d'identification, de contrôle de ses droits, de certification, de calcul de clés de chiffrement, de

calculs de signature, de vérifications de profils de l'utilisateur pour donner un accès sélectif à des applications demandées sur le serveur.

Selon une autre particularité le processeur de sécurité mémorise un journal dans une mémoire de masse, comportant un numéro séquentiel de connexion, les dates et heures de début et fin de connexion, l'adresse IP source et au moins un numéro de port, l'identifiant de l'objet de sécurité utilisé, le nom du serveur distant choisi, l'adresse IP de destination et le numéro de port, les statuts d'exécution.

Selon une autre particularité le processeur de sécurité mémorise dans une seconde table d'une mémoire la liste des applications traitées par le processeur, les traitements à effectuer en fonction du type de la connexion, les scénarios de sécurité à mettre en oeuvre, les droits d'accès des utilisateurs par définition d'une liste noire, blanche et une liste d'abonnés, les calendriers d'autorisation d'accès aux serveurs distants.

Un autre but de l'invention est de proposer un dispositif permettant la mise en oeuvre du procédé.

Ce but est atteint par le fait que le dispositif permet la mise en oeuvre du procédé entre, d'une part un terminal sur lequel est installé un logiciel de sécurité gérant les échanges avec la carte et un lecteur de carte associé au terminal ainsi que les échanges avec un protocole de communication multi sessions et multi ports et d'autre part un processeur de sécurité caractérisé en ce que le processeur de sécurité comporte des moyens d'établir et de contrôler les communications entre la station et un serveur choisi par le processeur en fonction de l'application demandée par la station.

Selon une autre particularité les moyens d'établir et de contrôler les communications permettent soit d'instaurer une communication directe entre le terminal et le serveur, soit d'instaurer une communication entre

le terminal et le serveur après établissement d'une session de sécurité contrôlée par un dispositif sécuritaire comportant un microprocesseur équipé de mémoires nécessaires à son fonctionnement et communiquant avec des modules de contrôle de sécurité MCS permettant d'interpréter les scénarios sécuritaires décidé par un processeur principal exécutant les programmes de serveur de communication et de moteur de sécurité.

Selon une autre particularité les moyens d'établir les communications sont constituées par deux cartes réseau local telles que, par exemple, Ethernet, anneau à jeton (token ring), l'une reliée à la station, l'autre reliée au serveur et communiquant avec la station et le serveur selon le protocole de communication multi sessions multi port.

D'autres particularités et avantages de la présente invention apparaîtront plus clairement à la lecture de la description ci-après faite en référence aux dessins annexés dans lesquels :

la figure 1 représente une vue du schéma de principe du dispositif permettant la mise en oeuvre du procédé de sécurisation ;

la figure 2A représente la boite de dialogue gérée par le logiciel de sécurité du terminal ;

la figure 2B représente une autre boite de dialogue signalant l'absence de lecteur ou de carte ;

la figure 2 C représente une autre boite de dialogue demandant le code porteur ;

la figure 2D représente une autre boite de dialogue permettant le choix du serveur destinataire ;

la figure 2E représente une autre boite de dialogue permettant une saisie d'une chaîne de caractères ;

la figure 2F représente la fenêtre principale.

L'invention va maintenant être décrite en liaison avec les figures 1 et 2. L'invention s'implante sur un réseau constitué de terminaux (2) communiquant à travers

un réseau constitué par des liaisons (42, 40, 41), avec un ou plusieurs serveurs (30, 31). Les terminaux peuvent être soit connectés localement sur le réseau du serveur ou peuvent être des micro-ordinateurs portables mobiles se connectant à travers des réseaux de télécommunication de tout type, réseau connecté, GSM, RNIS. Sur un tel réseau fonctionnent des applications, telles qu'une application de service terminal à distance, par exemple, de type Telnet ou des services de transfert de fichiers tels que, par exemple, FTP ou des protocoles utilisés par INTERNET tel que HTTP ou encore tout autre application connue actuellement. Le réseau est constitué de cartes réseau local par exemple de type Ethernet (23) sur l'ordinateur du terminal fonctionnant avec un protocole de télécommunication 24 du type multi sessions et multi ports tel que par exemple le protocole TCP/IP. Chaque serveur (30, 31) comporte également une carte Ethernet (302, 312) et un protocole TCP/IP associé (301, 311). Pour sécuriser le réseau il suffit d'interposer, dans le cas où le réseau comporte plusieurs serveurs, au noeud de jonction des serveurs situé dans la même enceinte que les serveurs un processeur de sécurité (1) qui dialogue avec un ou plusieurs terminaux (2) du réseau. Chacun des terminaux (2) est équipé d'une application de sécurité constituée d'un logiciel (27) et d'une liaison physique (20) avec un lecteur (21) d'objets portables (22). Ces objets portables (22) peuvent être du type carte à puce ou carte PC/MCIA.

Le processeur de sécurité (1) est constitué d'une unité de traitement (14) comprenant une carte électronique type PC (Personal Computer) avec les mémoires correspondantes et communique par un bus (11) avec une première carte réseau type Ethernet (13) reliée à chacun des serveurs (30, 31) par une liaison respective (40, 41) et avec une deuxième carte réseau de type Ethernet (12) reliée au terminal par une liaison (42). Le

bus (11) communique également avec une carte d'application sécuritaire (15) qui comporte une unité de traitement, des mémoires non représentée, et des modules MCS (S.A.M Security Application Module) de contrôle de sécurité (151, 152). L'installation peut comporter n cartes comprenant chacune n modules de contrôle de sécurité MCS (151, 152). Ces modules MCS (151, 152) permettent de réaliser, en liaison avec le lecteur (21) et l'objet portable, des fonctions de sécurité telles que l'authentification, la certification, le calcul de clé de chiffrement, etc..., tout en assurant l'inviolabilité des clés secrètes de base. Ces fonctions de sécurité mettent en oeuvre également les informations contenues dans la carte à puce ou l'objet portable (22) relié par le lecteur (21) à l'application de sécurité (27) du terminal (2). L'unité de traitement (14) fonctionne avec un système d'exploitation (173) multitâches, par exemple, de type OS2 pour permettre au processeur sécuritaire (1) d'exécuter plusieurs tâches en parallèle. Chaque carte Ethernet (12, 13) comporte sa couche logiciel permettant de mettre en oeuvre le protocole de télécommunication propre au réseau, tel que le protocole TCP/IP (131, 121). En plus du système d'exploitation l'unité de traitement (14) fonctionne avec un serveur de communication (172) qui comporte une couche (1721) permettant le traitement des communications entre la première (13) et la deuxième (12) carte selon le protocole du réseau de type TCP/IP. Ce serveur de communication (172) a pour rôle de déterminer si la liaison entre la deuxième carte Ethernet (12) et la première carte (13) reliée au serveur doit se faire en direct ou si cette liaison ne peut se faire qu'après mise en oeuvre d'une procédure sécuritaire. Cette détermination s'effectue par la lecture d'un fichier APPLI.INI mémorisé dans une mémoire (16) et comportant une table de correspondance entre l'application et au moins le scénario sécuritaire à

mettre en oeuvre. Dans le cas de la mise en oeuvre ce serveur de communication fait appel à un moteur de sécurité (171) qui déclenchera le fonctionnement de la carte d'application sécuritaire (15) du processeur de sécurité (1) permettant de mettre en oeuvre les fonctions de sécurité. Le moteur de sécurité MS permet de configurer le réseau sécuritaire, de définir la liste des applications traitées par le processeur de sécurité, de définir les traitements effectués, de définir les scénarios de sécurité à mettre à oeuvre, de définir les droits d'accès des utilisateurs et les calendriers d'autorisation. L'application de sécurité (27) mise en place sur le terminal fonctionne également avec un système d'exploitation du type à affichage à fenêtre tel que le logiciel Windows (marque déposée). Une fois le chargement du logiciel de sécurité (27) effectué sur la station, ce dernier permet à l'utilisateur du terminal, par l'affichage d'une fenêtre principale (figure 2F) affichée après le lancement de l'application sécuritaire, soit l'activation de la connexion de sécurité soit la désactivation de la connexion de sécurité ou encore de sortir de l'application. Comme représenté à la figure 2F, la sélection d'une des trois fonctions disponibles s'effectue en amenant la surbrillance sur la fonction souhaitée puis en validant par un "clic" souris ou par l'action de la touche "entrée" du clavier. L'utilisateur se connecte sur le réseau sécurisé en spécifiant l'adresse IP du processeur sécuritaire (1) et le numéro de port affecté à l'application qu'il veut utiliser (par exemple, X pour l'application sécuritaire, 21 pour l'application FTP, 23 pour Telnet, etc...). Le processeur de sécurité (1) recherche dans une table le scénario de sécurité associé au numéro de port envoyé par la station et établit ensuite une communication avec l'application sécuritaire (27) pour mettre en oeuvre le scénario sécuritaire avec notamment authentification de l'objet

portable utilisateur (22) et identification de l'utilisateur par son code porteur de carte (P.I.N.). De façon optionnelle le processeur de sécurité (1) peut faire afficher sur la station la liste d'applications, celles utilisées par l'utilisateur définies par les listes blanches et par les listes noires pour celles interdites. L'utilisateur effectue ensuite par des actions sur le clavier ou la souris la sélection d'un couple serveur application. Dès que le scénario sécuritaire s'est déroulé normalement et l'utilisateur lance l'application choisie (Telnet, FTP, HTTP, ...) en validant la sélection. Le processeur de sécurité (1) reçoit du terminal (2) un numéro de port correspondant à l'application, détermine dans ses tables l'adresse IP du serveur d'application et établis la connexion vers le serveur d'application demandé. Une fois la connexion établie entre le terminal (2) et un des serveurs (30, 31), le processeur de sécurité supervise les sessions applicatives établies en effectuant des contrôles securitaires cycliques vers le terminal (2). En cas d'anomalie sécuritaire détectée (telle que, retrait de carte, inactivité, mauvais calcul de signature,...), le processeur de sécurité (1) interrompt les connexions vers le serveur distant et rompt la session de sécurité.

Plusieurs scénarios de sécurité peuvent être mis en oeuvre et le choix du scénario activé se fait en fonction du numéro de port de l'application indiqué dans les données de connexion. Ces informations de numéro de port et de scénario associé sont dans un fichier ACCUEIL.CAM qui constitue une partie d'une table (161) de la mémoire de masse (16) du processeur de sécurité (1). L'activation d'une connexion sécuritaire met en oeuvre un scénario d'accueil qui permet de réaliser n'importe quel traitement parmi un ou plusieurs des traitements suivants : l'affichage et la saisie de données ; le contrôle des adresses IP source et destination ; le contrôle d'accès

par mot de passe ; le contrôle d'accès par carte à microprocesseur permettant la mise en oeuvre de l'identification du porteur, de l'authentification à partir d'un module sécurité MCS, d'un chiffrement, d'une signature, d'un calcul de certificat, d'une lecture et écriture d'informations, d'un contrôle d'arrachage de cartes, la vérification du droit d'accès de l'utilisateur au serveur distant dans les listes noires, blanches, listes d'abonnés. Ces droits d'accès et ces listes constituant une partie de la table T (161) ; le contrôle des droits d'utilisation des différents services du protocole de télécommunication TCP/IP ; la vérification de la plage horaire et calendaire autorisée pour l'utilisateur ou pour l'accès de la machine choisie, cette plage horaire et calendaire autorisée faisant l'objet d'une table comportant d'une part, en colonne les plages horaires et, en lignes l'identité des utilisateurs ou machines. Enfin l'affichage d'un menu personnalisé permet le choix d'une des applications ou serveurs distants autorisés pour l'utilisateur. Le fichier APPLI.INI permet de mémoriser dans la mémoire (16), d'identifier en fonction de l'application le scénario de sécurisation à activer ainsi que la période d'activation, ce qui permet selon le scénario et la période d'activation choisie de déclencher cycliquement l'activation d'un scénario en fonction de l'application du serveur distant choisi. Le scénario périodique vérifie que l'utilisateur distant est bien celui habilité en demandant à la carte du terminal d'effectuer des signatures électroniques d'informations (nombre aléatoire) choisies par le scénario. Le scénario ayant à charge de vérifier à l'aide du MCS que ces signatures ont été produites par une carte disposant des clés secrètes adéquates. Ce procédé permet de se prémunir notamment contre le vol d'adresses IP provenant d'un dispositif intrus sur le réseau. Lorsque l'utilisateur a choisi le

serveur distant et l'application, le processeur de sécurité récupère le numéro de port de l'application et utilise un fichier local, pour ouvrir une connexion avec le serveur distant choisi par le processeur sécuritaire. Ce serveur choisi par le processeur sécuritaire peut être différent de celui indiqué par l'utilisateur. L'utilisateur recevra simplement les communications à travers le processeur de sécurité. Ces communications sont adressées à la station (2) grâce à son numéro de port. Enfin le processeur de sécurité permet grâce au moteur de sécurité (171) de tenir dans la mémoire de masse (16) un journal (162) des connexions qui mémorise un numéro séquentiel de connexion, les dates et heures de début et fin de connexion, l'adresse IP source et le numéro de port, l'identifiant de l'objet de sécurité utilisé, le nom du serveur distant choisit, l'adresse IP de destination, le numéro de port, le volume de données échangées entre la station et le serveur lors de la session applicative, le statut d'exécution. L'application de sécurité (27) comporte un module de présentation (271) qui permet d'utiliser le système d'affichage à fenêtre et boite de dialogue du système d'exploitation Windows pour permettre par l'affichage d'une première boite de dialogue (figure 2A) de demander à l'utilisateur la saisie d'un mot de passe puis ensuite la validation de ce mot ou l'abandon de l'opération qui entraîne la désactivation de la connexion de sécurité. L'interface utilisateur permet également d'afficher une deuxième boite de dialogue (figure 2B) indiquant les messages "carte absente du lecteur" et "veuillez insérer votre carte SVP" ainsi qu'une troisième boite de dialogue (figure 2C) permettant de saisir le code du porteur de la carte avec des boutons de validation ou d'annulation de la procédure. Enfin une quatrième boite de dialogue permet de sélectionner le serveur destinataire en permettant la sélection parmi une liste déroulante des

serveurs possibles du réseau. Deux autres boites de dialogue permettent, l'une l'affichage de messages reçus du processeur sécuritaire puis une autre boite (figure 2E) permet la demande de saisie d'une chaîne de caractères. On comprend que l'on a ainsi sécurisé les accès et permis de sélectionner les conditions des procédures d'accès au choix de la personne chargée de la sécurité, de plus la périodicité des connexions sécuritaires permet d'éviter qu'un fraudeur se connecte à un moment donné en faisant semblant de se substituer au terminal connecté au réseau car s'il ne possède pas les clés d'accès au terminal, les procédures sécuritaires ne l'identifient pas et interdisent la session. Enfin cette solution présente l'avantage de rester transparente par rapport au protocole des applications circulant sur la connexion. En effet l'installation du système sécuritaire se fait sans modification des applications sur les terminaux et encore moins sur les serveurs.

Lors de l'installation du logiciel sécuritaire (27) et du processeur de sécurité (1), l'installateur définit dans un fichier d'initialisation (SERVEUR.INI) un délai de sécurité qui permet au processeur (1) de fermer la connexion de sécurité établie avec un poste client s'il n'y a pas de connexion applicative depuis le délai déterminé et un délai d'inactivité qui permet au processeur de fermer la connexion de sécurité et les connexions applicatives établies avec un poste client s'il n'y a pas de données échangées sur les connexions applicatives depuis le délai déterminé.

D'autres modifications à la portée de l'homme de métier font également partie de l'esprit de l'invention.

REVENDICATIONS

1. Procédé de sécurisation des accès à au moins un serveur (30) caractérisé en ce qu'il permet de sécuriser les accès en provenance de stations (2) d'utilisateur et à destination d'au moins un serveur d'application à travers un réseau (42) utilisant un protocole de télécommunication multi sessions et multi ports, ledit procédé comprenant les étapes suivantes :

-une étape d'établissement systématique d'une session de sécurité en parallèle entre la station d'utilisateur (2) et un processeur de sécurité (1) interposé entre la station d'utilisateur à protéger pendant le déroulement des sessions d'applications et le ou les serveurs (30) à protéger ; et

-une étape de déclenchement cyclique de session de sécurité.

2. Procédé de sécurisation des accès à au moins un serveur selon la revendication 1, caractérisé en ce que l'étape d'établissement systématique d'une session de sécurité comporte les étapes suivantes :

transmission par la station sur le réseau d'une adresse source IP et d'au moins un numéro de port associé à l'application demandée par la station (2) ;

recherche par le processeur de sécurité du scénario sécuritaire associé à l'application ;

établissement de la session de sécurité entre le processeur de sécurité (1) et la station (2) ;

recherche par le processeur sécuritaire (1) dans un fichier local du processeur le nom et l'adresse du serveur distant utilisé pour l'application et ouverture d'une connexion avec le serveur (30, 31) distant par communication d'une adresse IP et d'un numéro de port.

3. Procédé de sécurisation des accès à au moins un serveur selon la revendication 2, caractérisé en ce que le scénario associé à une application comprend l'étape

consistant à établir directement la liaison entre la station (2) et le serveur distant (30) choisi par le processeur de sécurité.

4. Procédé de sécurisation des accès à au moins un serveur selon la revendication 1, caractérisé en ce que le scénario de sécurité à mettre en oeuvre et défini dans une table mémorisée permet au choix une ou plusieurs des fonctions ci-après d'authentification de l'utilisateur, d'identification de l'utilisateur, de contrôle de ses droits, de certification, de calcul de clés de chiffrement, de calculs de signatures, de vérifications de profils de l'utilisateur pour donner un accès sélectif à des applications demandées sur le serveur.

5. Procédé de sécurisation des accès à au moins un serveur selon la revendication 1,caractérisé en ce que le processeur de sécurité mémorise un journal (162) dans une mémoire (16) comportant un numéro séquentiel de connexion, les dates et heures de début et fin de connexion, l'adresse IP source et au moins un numéro de port, l'identifiant de l'objet de sécurité utilisé, le nom du serveur distant choisi, l'adresse IP de destination et le numéro de port, les statuts d'exécution.

6. Procédé de sécurisation des accès à au moins un serveur selon la revendication 1, caractérisé en ce que le processeur de sécurité (1) mémorise dans une seconde table (161) d'une mémoire (16) la liste des applications traitées par le processeur, les traitements à effectuer en fonction du type de la connexion, les scénarios de sécurité à mettre en oeuvre, les droits d'accès des utilisateurs par définition d'une liste noire, blanche et une liste d'abonnés, les calendriers d'autorisation d'accès aux serveurs distants.

7. Dispositif pour sécuriser, au moyen d'un processeur de sécurité (1), des accès en provenance d'une station (2) d'utilisateur et à destination d'au moins un

serveur d'application à travers un réseau (42) utilisant un protocole de télécommunication multi sessions et multi ports, un logiciel de sécurité (27) étant installé sur la station pour gérer des échanges avec un objet portable et un lecteur d'objet portable(21) associé à la station (2) ainsi que des échanges avec un protocole (24) de communication multi sessions et multi ports, caractérisé en ce que le processeur de sécurité (1) comporte des moyens d'établir (12, 13) et de contrôler (14, 15, 172, 171) des communications entre la station (2) et un serveur (30) choisi par le processeur de sécurité en fonction d'une application demandée par la station (2).

8. Dispositif selon la revendication 7, caractérisé en ce que les moyens d'établir et de contrôler les communications permettent soit d'instaurer une communication directe entre la station (2) et le serveur, soit d'instaurer une communication entre la station et le serveur après établissement d'une session de sécurité contrôlée par un dispositif sécuritaire comportant un microprocesseur équipé de mémoires nécessaires à son fonctionnement et communiquant avec des modules de contrôle de sécurité MCS permettant d'interpréter des scénarios sécuritaires décidés par un processeur principal (14) exécutant des programmes d'un serveur de communication (172) et d'un moteur de sécurité (171).

9. Dispositif selon la revendication 7, caractérisé en ce que les moyens d'établir (12, 13) les communications sont constitués par deux cartes de télécommunication, l'une reliée à la station, l'autre reliée au serveur et communiquant avec la station et le serveur selon le protocole de communication multi sessions et multi port.

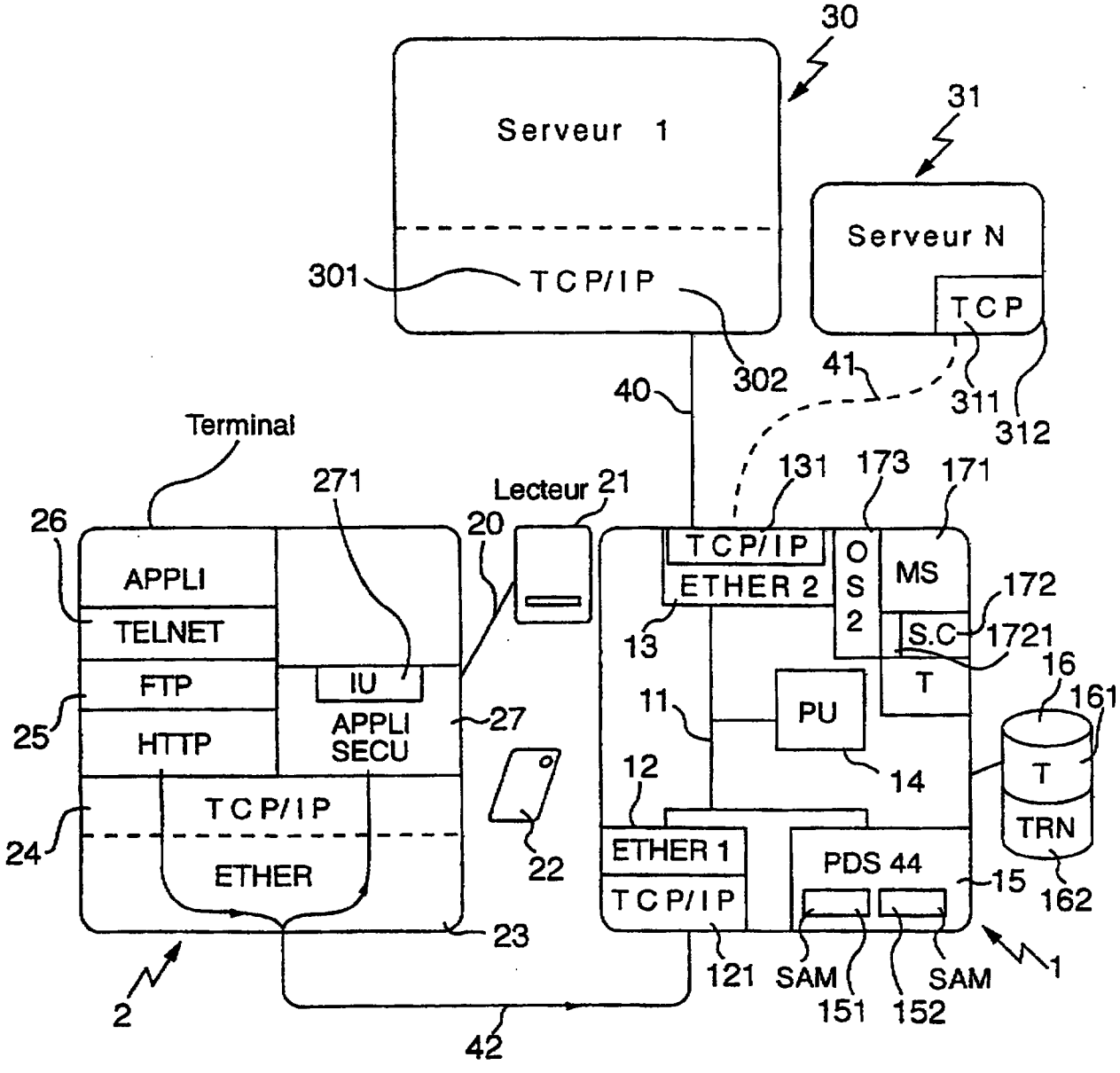

30
Serveur 1
31
Serveur N
TCP
301
TCP/IP
302
41
311
312
40
Terminal
271
Lecteur 21
131
173
171
26
20
APPLI
TELNET
FTP
HTTP
IU
APPLI SECU
25
27
TCP/IP
ETHER
24
22
23
TCP/IP
ETHER 2
OS 2
MS
172
13
S.C
1721
T
16
161
11
PU
12
14
T
TRN
ETHER 1
TCP/IP
PDS 44
15
162
121
SAM
151
SAM
152
1
2
42

Fig.1

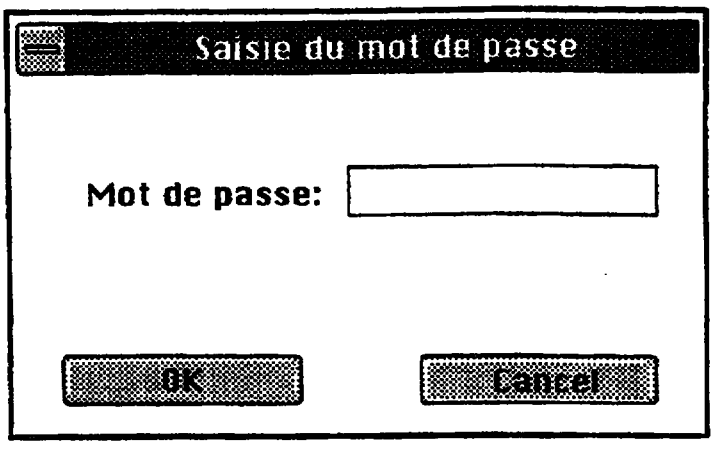


Fig.2A

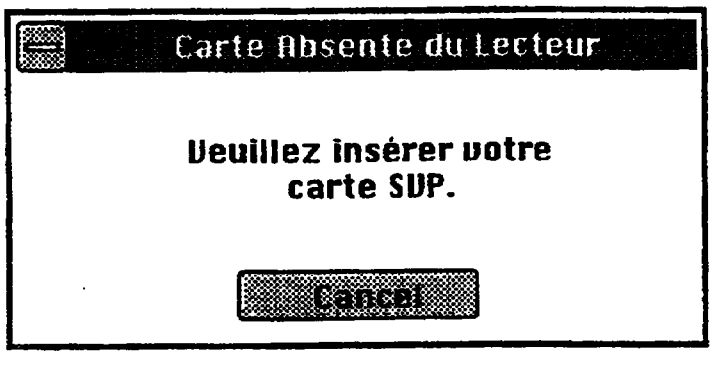


Fig.2B

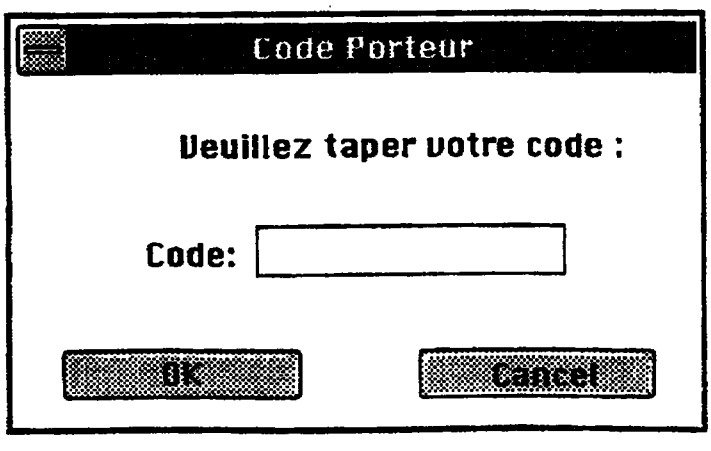


Fig.2C

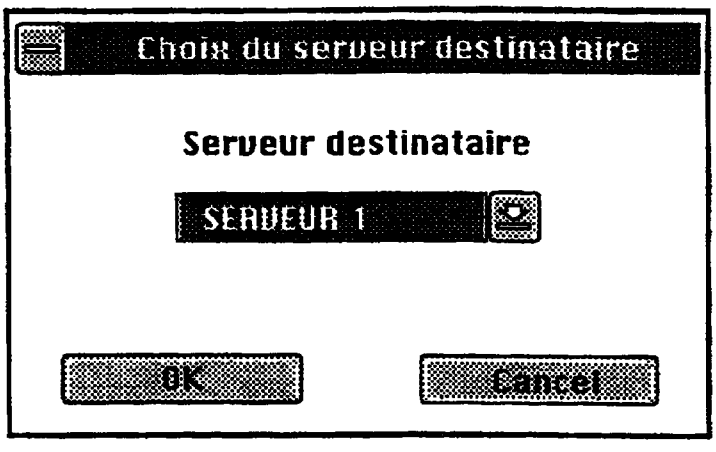

Choix du serveur destinataire
Serveur destinataire
SERVEUR 1
OK
Cancel

Fig.2D

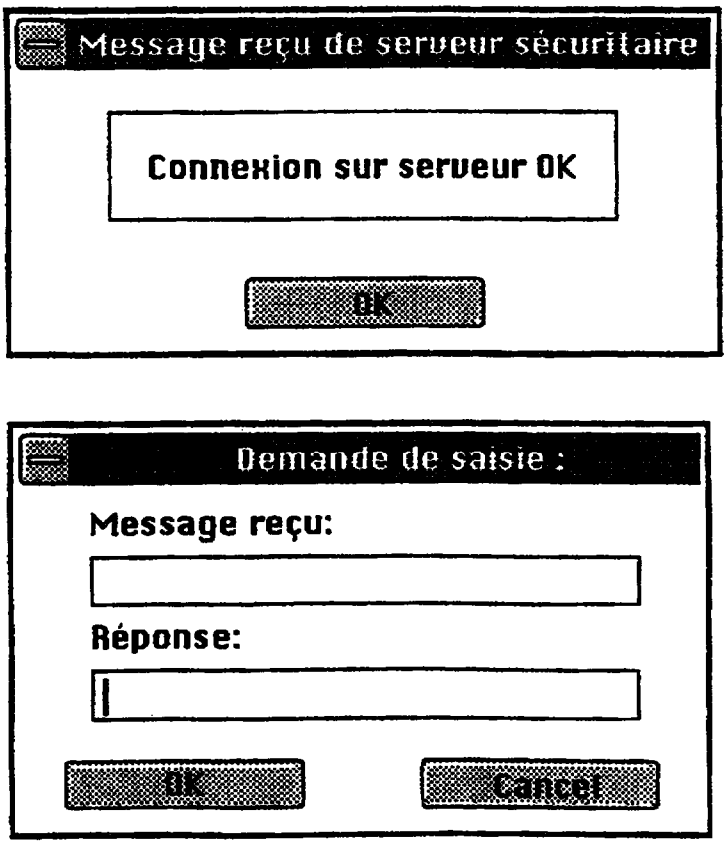

Message reçu de serveur sécuritaire
Connexion sur serveur OK
OK
Demande de saisie :
Message reçu:
Réponse:
OK
Cancel

Fig.2E

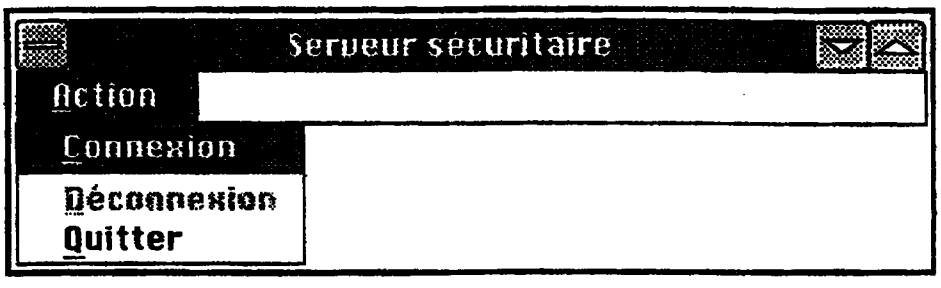

Serveur sécuritaire
Action
Connexion
Déconnexion
Quitter

Fig.2F

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.

ABSTRACT

Applicant: CP8 TRANSAC

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 accesses to servers and the device which implements this process.

The process for protecting accesses to at least one server (30) is 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 consisting of 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.

Fig. 1 to be published.

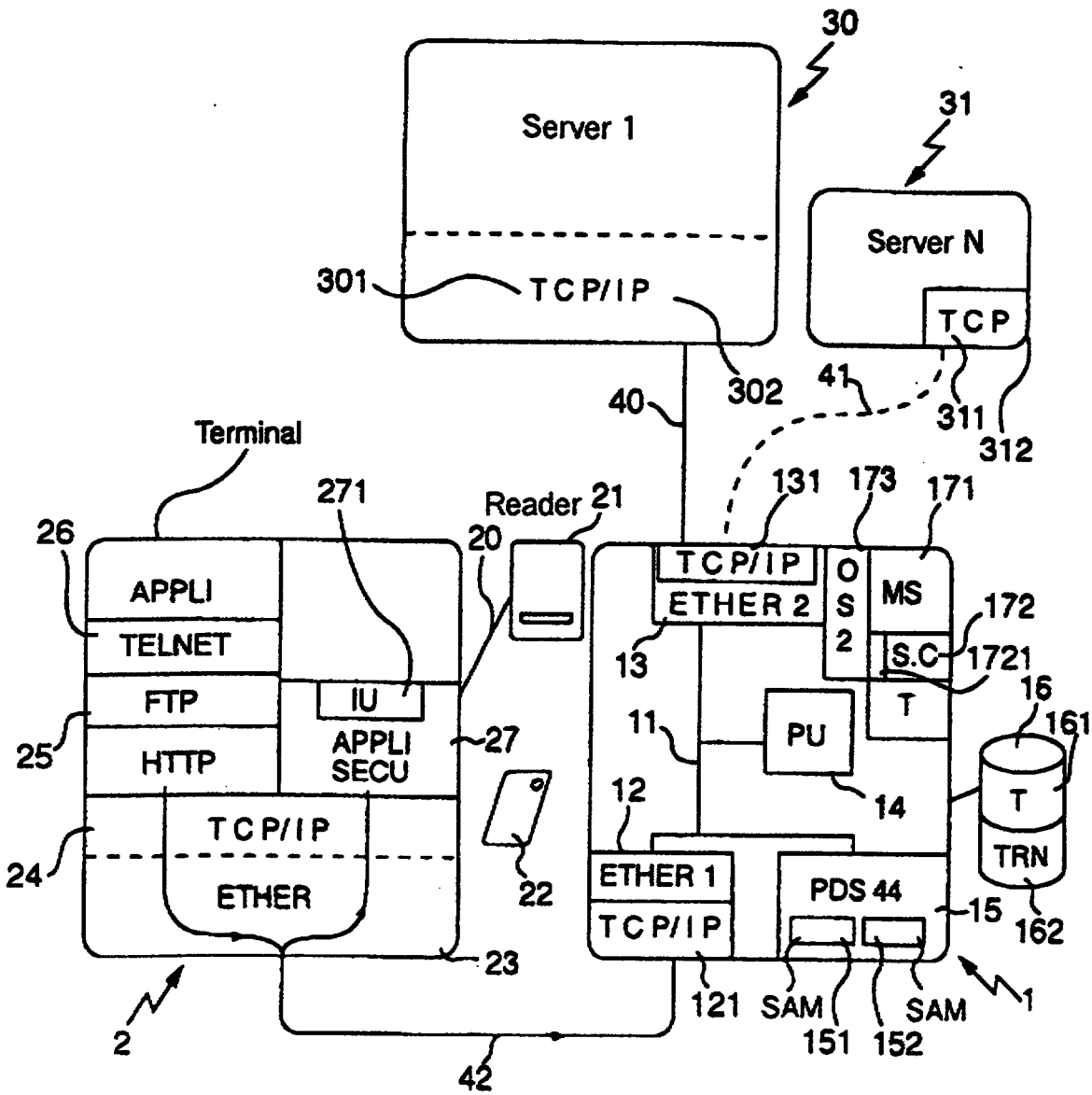

30
Server 1
31
Server N
301
TCP/IP
302
TCP
41
311
312
40
Terminal
271
Reader
21
131
173
171
26
20
APPLI
TELNET
FTP
HTTP
IU
APPLI SECU
TCP/IP
ETHER
TCP/IP
ETHER 2
OS 2
MS
172
13
S.C
1721
T
16
161
11
PU
25
27
12
14
T
TRN
24
22
ETHER 1
TCP/IP
PDS 44
15
162
23
121
SAM
151
SAM
152
1
2
42

Fig.1

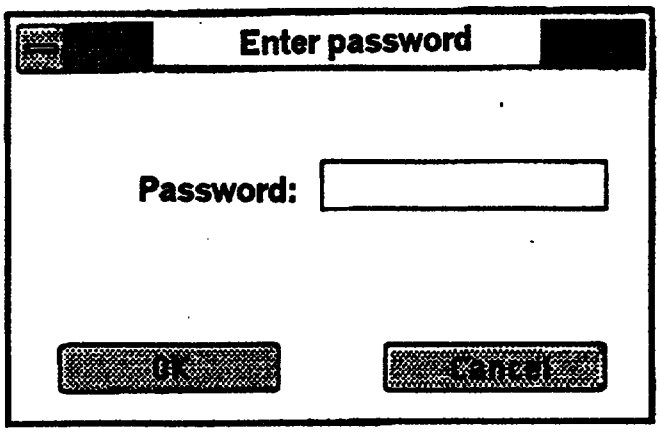


Fig.2A

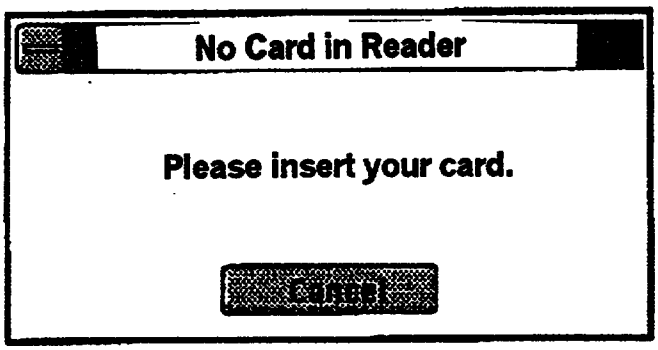


Fig.2B

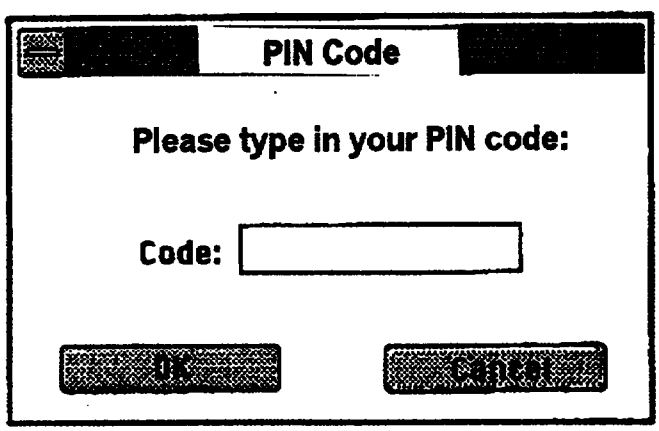


Fig.2C

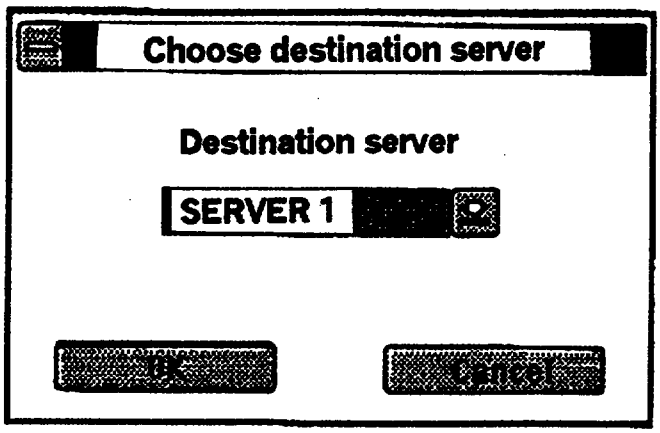

Choose destination server
Destination server
SERVER 1
OK
Cancel

Fig.2D

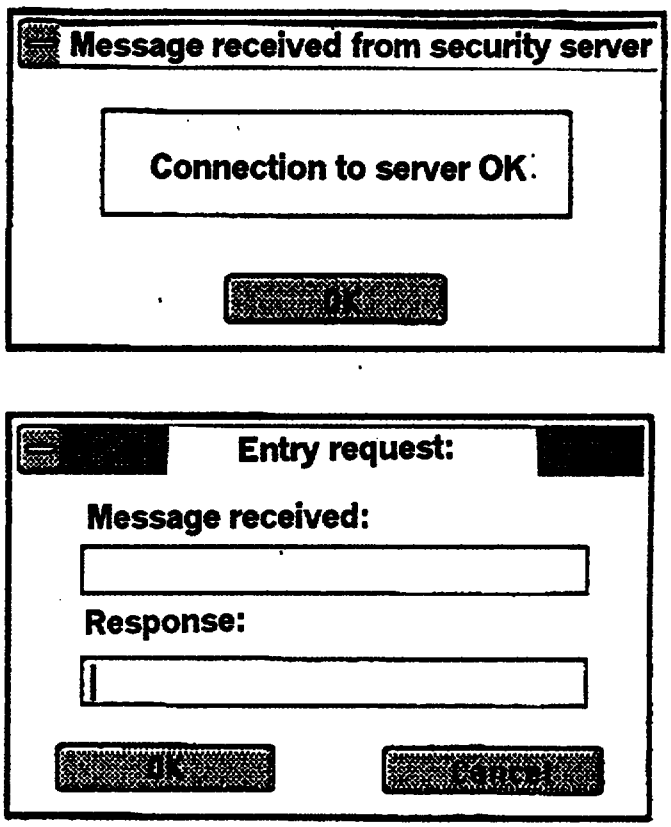

Message received from security server
Connection to server OK.
OK
Entry request:
Message received:
Response:
OK
Cancel

Fig.2E

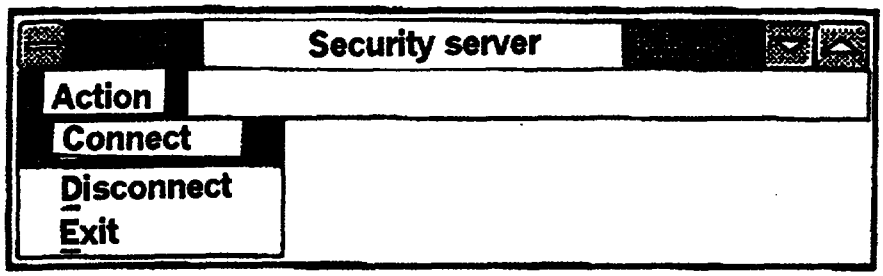


Fig.2F

9705737-6
IPDS's copy!

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : H04L 29/06	A1	(11) Numéro de publication internationale: **WO 97/33415**
		(43) Date de publication internationale: 12 septembre 1997 (12.09.97)

(21) Numéro de la demande internationale: PCT/FR97/00371

(22) Date de dépôt international: 3 mars 1997 (03.03.97)

(30) Données relatives à la priorité:
96/02901 7 mars 1996 (07.03.96) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: CP8 TRANSAC [FR/FR]; 68, route de Versailles, F-78430 Louveciennes (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: SIGAUD, Alain [FR/FR]; 12, hameau de la Vallée, F-78990 Elancourt (FR).

(74) Mandataire: CORLU, Bernard; Bull S.A., 68, route de Versailles, F-78434 Louveciennes (FR).

(81) Etats désignés: AU, BR, CA, CN, JP, KR, NO, SG, US, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: METHOD ENABLING SECURE ACCESS BY A STATION TO AT LEAST ONE SERVER, AND DEVICE USING SAME

(54) Titre: PROCEDE DE SECURISATION DES ACCES D'UNE STATION A AU MOINS UN SERVEUR ET DISPOSITIF METTANT EN OEUVRE LE PROCEDE

(57) Abstract

A server access securing method and a device using same are disclosed. The method for securing access to at least one server (30) enables secure access by user stations (2) to at least one application server via a network (42) that uses a multisession, multiport telecommunication protocol. The method comprises the steps of systematically establishing a parallel security session between the user station (2) and a security processor (1) connected between the user station to be protected during application sessions and the server(s) (30) to be protected, and cyclically initiating a security session.

(57) Abrégé

La présente invention concerne un procédé de sécurisation des accès à des serveurs et le dispositif mettant en oeuvre le procédé. Le procédé de sécurisation des accès à au moins un serveur (30) est caractérisé en ce qu'il permet de sécuriser les accès en provenance de stations (2) d'utilisateur et à destination d'au moins un serveur d'application à travers un réseau (42) utilisant un protocole de télécommunication multi sessions et multi ports, ledit procédé consiste en une étape d'établissement systématique d'une session de sécurité en parallèle entre la station d'utilisateur (2) et un processeur de sécurité (1) interposé entre la station d'utilisateur à protéger pendant le déroulement des sessions d'applications et le ou les serveurs (30) à protéger et une étape de déclenchement cyclique de session de sécurité.

