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.