(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 676 291**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **91 05520**

(51) Int Cl[5] : G 06 F 12/14

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 06.05.91.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 13.11.92 Bulletin 92/46.

(56) **Liste des documents cités dans le rapport de recherche :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *BULL (S.A.)* — FR.

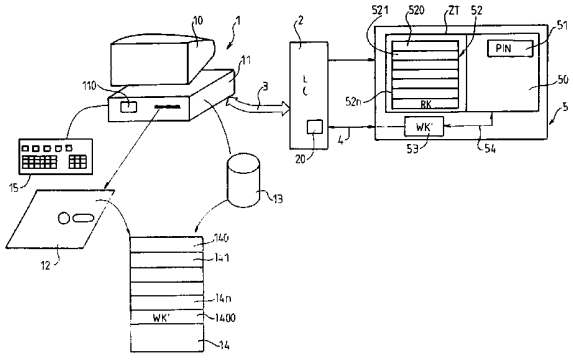
(72) **Inventeur(s) :** Pinkas Denis.

(73) **Titulaire(s) :**

(74) **Mandataire :** Debay Yves.

(54) Dispositif de sécurité pour système informatique et procédé de reprise d'exploitation.

(57) L'invention concerne un dispositif de sécurité pour système informatique comportant un dispositif permettant d'exécuter des programmes d'application sécurisées chacun par un identifiant et une clé d'accès ou mot de passe (5202) défini pour chaque utilisateur (5203) et associé par un lecteur de carte (2) avec une carte à mémoire (5) contenant toutes les clés d'accès (52020 à 5202n) d'un utilisateur donné à chaque programme d'application (52010 à 5201n) caractérisé en ce que lors de la procédure d'ouverture de cession du programme de protection (PASSMAN), le fichier d'accès (52) stocké dans la zone transactionnelle ZT est transféré dans la mémoire vive (110) du système d'exploitation et sauvegardé sous forme chiffrée dans un fichier (14) de sauvegarge (BACK-UP) des moyens de mémorisation permanent (12, 13) du système.



FR 2 676 291 - A1

DISPOSITIF DE SECURITE POUR SYSTEME INFORMATIQUE ET PROCEDE DE REPRISE D'EXPLOITATION.

La présente invention concerne un dispositif de sécurité pour système informatique ainsi que le procédé de reprise d'exploitation de ce dispositif de sécurité.

Le dispositif de sécurité pour système informatique comporte un dispositif permettant d'exécuter des programmes d'application sécurisés chacun par un identifiant et une clé d'accès ou mot de passe défini pour chaque utilisateur et associé par un lecteur de carte avec une carte à mémoire contenant toutes les clés d'accès d'un utilisateur donné à chaque programme et en ce que lors de la procédure d'ouverture de cession du programme de protection, le fichier d'accès stocké dans la zone transactionnelle de la carte est transféré dans la mémoire vive du système d'exploitation.

En cas de perte momentanée ou définitive de la carte , l'utilisateur ne peut plus exploiter le logiciel pour continuer son travail.

Un premier objet de l'invention est de prévoir un dispositif et un procédé permettant de conserver un niveau de sécurité pour l'accès à des programmes d'application tout en permettant à un utilisateur ayant perdu la carte de récupérer et de reprendre les programmes. Ceci est obtenu par l'utilisation d'un fichier de sauvegarde (BACKUP) sauvegardé sous forme chiffrée dans les moyens de mémorisation permanent du système.

Selon une autre caractéristique le fichier d'accès contient le nom de l'application, le mot de passe, le nom de l'utilisateur et une date de mise à jour de ces informations.

Selon une autre caractéristique lorsque l'utilisateur retire la carte du connecteur, des moyens de détection de l'absence de carte déclenchent le blocage de l'écran et du clavier par détournement des interruptions d'entrée/sortie du clavier, sur un autre programme de traitement.

Selon une autre caractéristique le fichier de sauvegarde est chiffré à l'aide d'une clé de travail générée de façon aléatoire et ensuite chiffrée par une clé de reprise d'exploitation mémorisée dans la zone de transaction de la carte .

Un autre but de l'invention est de proposer un procédé de reprise d'exploitation permettant la reprise de l'exploitation du dispositif sécurisé même en cas de perte de la carte.

Ce but est atteint par le fait que le procédé de reprise d'exploitation d'un dispositif de sécurité est caractérisé en ce qu'il comporte les étapes suivantes :

- délivrance par un autorité d'un mot de passe de reprise d'exploitation qui est une fonction codée d'une date et de la clé de reprise d'exploitation ;

- délivrance par un autorité d'une date maximum de validité de ce mot de passe de reprise ;

- introduction du mot de passe de reprise d'exploitation par l'utilisateur dans le système ;

- calcul par le programme de reprise d'exploitation de la clé de reprise d'exploitation à l'aide de la fonction de chiffrement du programme de reprise en prenant en compte d'une part la date maximum de validité du mot de passe de reprise et d'autre part le mot de passe de reprise d'exploitation;

- calcul de la clé de travail à l'aide de la fonction de chiffrement du programme en prenant en compte la clé de reprise d'exploitation et la clé de travail chiffrée ;

- déchiffrement du fichier de sauvegarde.

. Selon une autre particularité le procédé comporte en outre une étape de mémorisation des informations rentrées au clavier une première fois par l'utilisateur et constituées par le nom de l'utilisateur et le mot de passe pour accéder à l' application appelée par l'utilisateur.

D'autres caractéristiques 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 schématique du système de sécurité ;

La Figure 2 représente un mot du fichier avant chiffrement et qui est mémorisé sous forme codée dans la carte et correspondant au fichier qui sera stocké dans les moyens de stockage du système.

Le dispositif de sécurité pour système informatique est constitué d'un dispositif informatique (1)comprenant une unité centrale (11) , un écran (10) , un clavier (15), des moyens de stockage de fichiers tels qu' une disquette (12) ou un disque dur (13) permettant de stocker des fichiers. Ce système informatique (1) est relié par une liaison (3), à un lecteur de carte (2) lequel permet par la connexion (4) de travailler avec une carte (5). La mémoire (50) de cette carte est partagée d'une part en une zone secrète (51) inaccessible de l'extérieur, contenant le code d'identification personnel (PIN) de l'utilisateur et d'autre part en une zone de travail ou zone transactionnelle (ZT) contenant un fichier d'accès (52)

constitué d'une série de mots (520 521...52n), ainsi que la clé de reprise d'exploitation (RK). Comme représenté à la Figure 2, chaque mot du fichier d'accès (52) est constitué du nom de l'application (5201) pour laquelle l'utilisateur dispose d'un mot de passe, d'un mot de passe (5202), du nom de l'utilisateur (5203) autorisé à travailler avec l'application en fonction du mot de passe et de la date de mise à jour (5204).

Ces informations transitent par la liaison (54) vers le processeur (53) pour y être chiffrées à l'aide d'une clé de travail chiffrée (WK') avant leur envoi vers l'unité centrale (11). Le processeur est relié par la connexion (4) au lecteur de carte (2) et à travers ce lecteur de carte avec l'unité centrale (11). En outre, le lecteur de carte (2) comporte un dispositif (20) permettant de détecter le retrait de la carte. Ce dispositif peut, par exemple, être constitué par un interrupteur dont le contact se ferme en l'absence de la carte, ce contact permettant la transmission d'un signal d'interruption à l'unité centrale (11).

Cette interruption transmise par la ligne (3) vers l'unité centrale déclenche un programme de traitement spécial qui permet de bloquer d'une part l'écran en affichant un message, et d'autre part le clavier par détournement des interruptions d'entrée/sortie du clavier. L'unité centrale (11) comporte un programme de sécurité intitulé PASSMAN qui lorsqu'il est lancé à l'initialisation de l'unité centrale demande à l'utilisateur d'insérer sa carte. Lorsque l'utilisateur a inséré sa carte et fourni son code d'identification personnel (PIN), la zone de transaction se trouve déverrouillée dès lors que le PIN est correct. La carte ou l'unité centrale génère de façon aléatoire une clé de travail (WK). Cette clé de travail (WK) est par exemple, chiffrée par l'unité centrale (11) à l'aide de la clé de reprise d'exploitation (RK) contenue dans la zone de transaction (52) de la carte (5) pour générer la clé de

travail chiffrée (WK'). Lors d'une sélection d'application par l'utilisateur, le programme PASSMAN est à même de fournir en fonction du nom de l'application fourni par l'application, le nom de l'utilisateur pour cette application et le mot de passe pour cette application si ces informations se trouvent déjà dans la zone de transaction. Si ces informations ne se trouvent pas déjà dans la zone de transaction, elles seront une première fois et une seule, fournies par l'utilisateur qui les aura obtenues d'un administrateur lui ayant octroyé un accès à l'application. Si les informations fournies par l'utilisateur se revèlent être exactes alors celles-ci sont enregistrées dans la zone de transaction et l'on se trouve alors ramené au cas précédent. Lors d'accès ultérieur à cette application le programme PASSMAN est alors à même de donner ces informations en lieu et place de l'utilisateur qui se trouve alors déchargé du soucis de mémoriser ces informations. Des opérations similaires d'enregistrement sont effectués lors des changements de mot de passe.

En outre, lors de chaque initialisation du système le contenu de la zone de transaction de la carte, est chargé dans la mémoire vive de l'unité centrale (11). Ce fichier est stocké également sous forme chiffrée, soit sur le disque dur (13), soit sur une disquette (12), dans un fichier (14) qui est le fichier de sauvegarde (140,141,...14n) (back-up) appelé lors de la mise en oeuvre de la procédure de reprise d'exploitation. Ce fichier (14) contient également la clé de travail chiffrée (WK') dans une zone (1400). Ceci permet lors de la perte de la carte, de faire déclencher par le programme PASSMAN à la suite de l'initialisation une procédure de reprise d'exploitation. Cette procédure de reprise d'exploitation demande à l'écran la fourniture d'un mot de passe de reprise d'exploitation (RP) qui doit être délivré par une autorité. Ce mot de passe de reprise d'exploitation est fonction de la clé de reprise d'exploitation (RK) et d'une date qui est, par exemple, la date de péremption du mot de passe de reprise.

Ce mot de passe de reprise d'exploitation (RP) permet, à un programme de reprise d'exploitation contenu dans le programme de sécurité PASSMAN, de calculer la clé de reprise d'exploitation (RK) par une fonction inverse de déchiffrement. Cette fonction de déchiffrement tient compte du mot de passe (RP)et de la date. Le programme de reprise d'exploitation permet également de calculer la clé de travail (WK) en fonction de la clé de reprise (RK) et de la clé de travail chiffrée (WK') mémorisée dans la zone (1400) du fichier (14). Ensuite grâce à cette clé de travail (WK), les informations chiffrées peuvent être déchiffrées pour être comparées avec le nom de l'application souhaitée par l'utilisateur. Le nom de l'utilisateur et le nom de l'application entrés au clavier par ce dernier sont comparés avec le contenu déchiffré du fichier (14) pour déterminer si l' utilisateur utilisant le mot de passe de reprise (RP) est habilité à accéder à l'application dont il a demandé l'accès . On comprend ainsi que ce système a permis de sécuriser différents programmes d'application pour différents utilisateurs utilisant chacun une carte personnelle, tout en permettant pour chaque utilisateur d'un système informatique une reprise d'exploitation momentanée suite à l'égarement de la carte ou à la perte définitive de celle-ci en attendant la délivrance d'une nouvelle carte pour l'utilisateur négligent. D'autres modifications à la portée de l'homme de métier font également partie de l'invention.

REVENDICATIONS

1. Dispositif de sécurité pour système informatique comportant un dispositif permettant d'exécuter des programmes d'application sécurisés chacun par un identifiant et une clé d'accès ou mot de passe (5202) défini pour chaque utilisateur (5203) et associé par un lecteur de carte (2) avec une carte à mémoire (5) contenant toutes les clés d'accès (52020 à 5202n) d'un utilisateur donné à chaque programme d'application (52010 à 5201n) caractérisé en ce que lors de la procédure d'ouverture de cession du programme de protection (PASSMAN), le fichier d'accès (52) stocké dans la zone transactionnelle ZT est transféré dans la mémoire vive (110) du système d'exploitation et sauvegardé sous forme chiffrée dans un fichier (14) de sauvegarde (BACK-UP) des moyens de mémorisation permanent (12,13) du système.

2. Dispositif selon la revendication 1 caractérisé en ce que le fichier d'accès (52) contient le nom de l'application (5201) le mot de passe (5202) le nom de l'utilisateur (5203) et une date de mise à jour de ces informations (5204).

3. Dispositif de sécurité selon la revendication 2 caractérisé en ce que, lors du retrait de la carte (5) du connecteur (2) par l'utilisateur, des moyens (20) de détection de l'absence de carte déclenchent le blocage de l'écran (10) et du clavier par détournement des interruptions d'entrée/sortie du clavier, sur un autre programme de traitement.

4. Dispositif de sécurité selon l'une des revendications précédentes caractérisé en ce que le fichier de sauvegarde (14) est chiffré l'aide d'une clé de travail (WK) générée de façon aléatoire et ensuite chiffrée en une clé (WK') par une clé de reprise d'exploitation (RK) mémorisée dans la zone de transaction (ZT).

5. Procédé de reprise d'exploitation d'un dispositif de sécurité selon une des revendications précédentes caractérisé en ce qu'il comporte les étapes suivantes:

- délivrance par une autorité d'un mot de passe de reprise d'exploitation (RP) qui est une fonction codée d'une date de péremption et de la clé de reprise d'exploitation (RK);

- introduction du mot de passe (RP) de reprise d'exploitation par l'utilisateur du système (1) et éventuellement de la date de péremption ;

- calcul par le programme de reprise d'exploitation de la clé de reprise d'exploitation (RK) à l'aide de la fonction de chiffrement du programme de reprise en prenant en compte la date de péremption et le mot de passe de reprise d'exploitation (RP);

- calcul de la clé de travail (WK) à l'aide de la fonction de chiffrement du programme en prenant en compte la clé de reprise d'exploitation (RK) et la clé de travail chiffrée (WK');

-déchiffrement du fichier de sauvegarde (14).

6. Procédé selon la revendication 5 caractérisé en ce qu'il comporte en outre une étape de mémorisation des informations rentrées au clavier une première fois par l'utilisateur et constituées par le nom de l'utilisateur et le mot de passe pour accéder à l' application appelée par l'utilisateur.

7. Procédé selon la revendication 6 caractérisé en ce que l'étape de mémorisation consiste en une première étape de mémorisation des informations dans une carte à mémoire (5) ; et une deuxième étape de sauvegarde des informations

chiffrées par une clé de travail dans un fichier de sauvegarde (14) du système informatique.

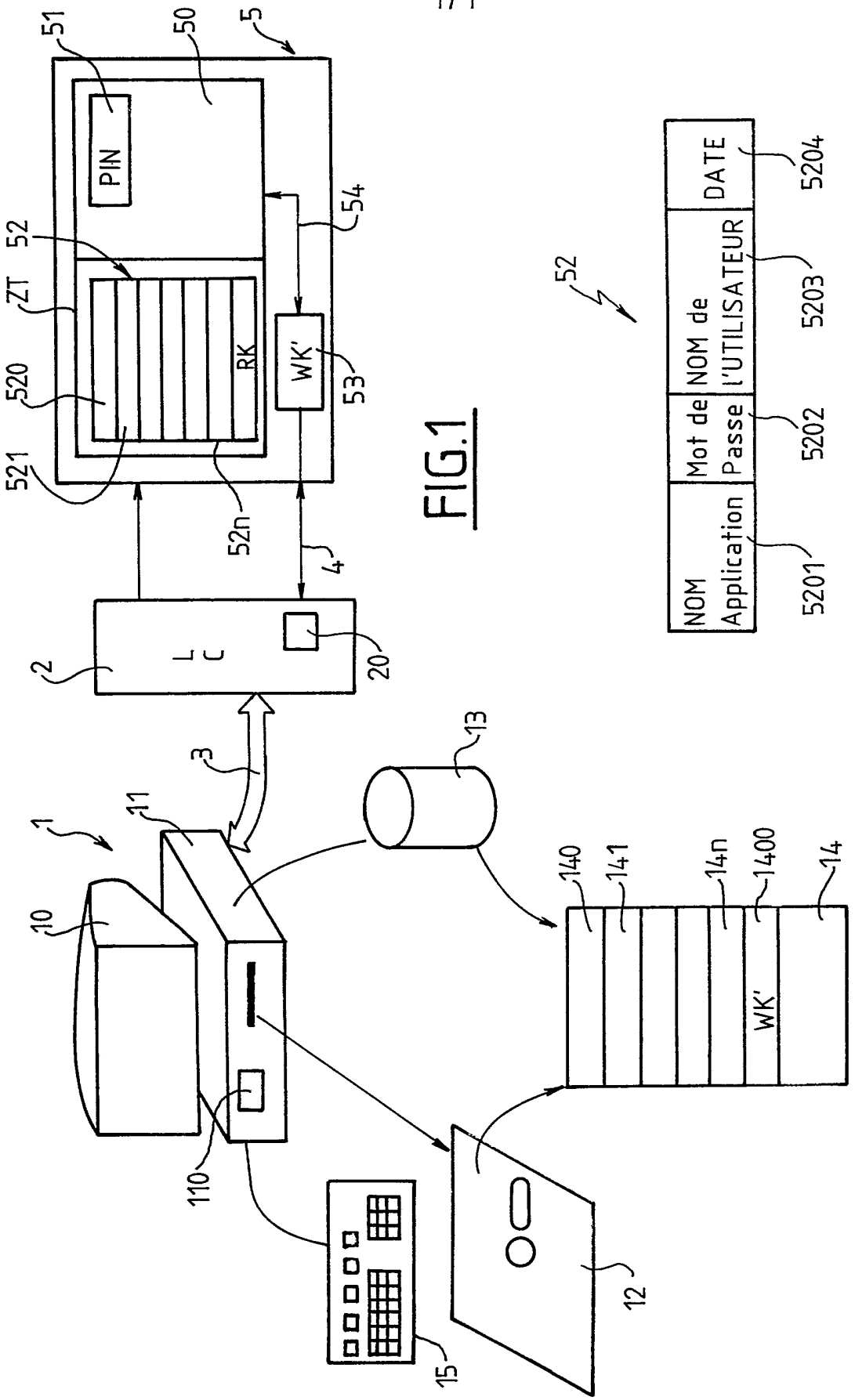

51
50
5
PIN
52
ZT
520
RK
WK'
54
53
521
52n
4
2
L
C
20
3
1
11
10
13
140
141
14n
1400
14
WK'
110
15
12

FIG.1

52
NOM Application
Mot de Passe
NOM de l'UTILISATEUR
DATE
5201
5202
5203
5204

FIG.2

REPUBLIQUE FRANÇAISE

2676291

N° d'enregistrement national

INSTITUT NATIONAL de la PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

RA 9105520
FA 457060

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
Y	EP-A-0 089 876 (CII HONEYWELL BULL) * figure 1 * * page 4, ligne 17 - page 10, ligne 21 *	1,2,4,5
Y	EP-A-0 363 122 (FUJITSU LTD.) * colonne 6, ligne 51 - colonne 7, ligne 25; figures 2,3,4A,4B *	1,2,4,5
Y	EP-A-0 157 303 (TOSHIBA) * page 3, ligne 23 - page 4, ligne 7; figures 1-3 *	1,2,4,5

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)

G06F
G07F

Date d'achèvement de la recherche	Examinateur
06 JANVIER 1992	WEISS P.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P0413)

3