(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 762 417**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **97 05328**

(51) Int Cl^6 : **G 06 F 12/14**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 16.04.97.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 23.10.98 Bulletin 98/43.

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

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

(71) **Demandeur(s) :** *GEMPLUS SOCIETE EN COMMANDITE PAR ACTIONS* — FR.

(72) **Inventeur(s) :** GREGOIRE LOUIS.

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

(74) **Mandataire(s) :** GEMPLUS.

(54) PROCEDE DE CONTROLE DE L'EXECUTION D'UN PRODUIT LOGICIEL.

(57) La présente invention concerne un procédé de contrôle de l'exécution d'un programme d'ordinateur.

Il comporte les étapes suivantes consistant à:

1) Scinder un programme en au moins deux parties, respectivement publique et secrète, la partie publique étant apte à être exécutée sur un premier moyen de traitement, la partie secrète étant apte à être exécutée sur un deuxième moyen de traitement sécurisé.

2) disposer ladite partie publique dans une mémoire du premier moyen de traitement,

3) disposer la partie secrète sur un support sécurisé du deuxième moyen de traitement destiné à être lu par ledit premier moyen de traitement,

4) effectuer les opérations suivantes lors de l'exécution du programme par le premier moyen de traitement:

a) transmission du premier moyen de traitement au deuxième de paramètres/ variables fonctions de signaux externes déclenchés par un utilisateur,

b) exécution d'au moins une partie du programme par le deuxième moyen de traitement en mettant en oeuvre un certain nombre desdits paramètreslvariables reçus,

c) transmission du deuxième moyen de traitement au premier, des résultats de l'exécution de l'alinéa précédent b),

d) exploitation d'un certain nombre desdits résultats dans l'exécution réalisée par le premier moyen.

FR 2 762 417 - A1

Procédé de contrôle de l'exécution d'un produit logiciel.

La présente invention concerne le domaine de la protection de produits logiciels contre le piratage. Elle a pour objet un procédé de contrôle de l'exécution d'un produit logiciel.

On entend par produit logiciel tout programme et/ou données destinés à être traités ou exécutés par une unité centrale notamment d'un micro-ordinateur PC, ainsi que tout fichier contenant des données à caractère audio et/ou vidéo destiné à être traité par un module spécifique notamment multimédia d'un PC. Ils peuvent être enregistrés sur tout support tel que disquette, disque dur, disque optique compact « CD-ROM », ou mémorisés sur tout support tel que mémoire de type « ROM », « EEPROM ».

Les programmes d'ordinateur ou produits logiciels notamment pour PC sont de plus en plus dupliqués et utilisés sans autorisation. Ceci est accentué par la possibilité de diffuser la copie à grande échelle par des réseaux de serveurs ou de la dupliquer par une production de masse de CD-ROM gravés avec le logiciel. On connaît également la simple copie illicite sur le disque dur ou disquettes de micro-ordinateur qui peut se produire au sein d'une même entreprise.

Parmi les solutions pour éviter l'usage illicite de produits logiciels, on connaît un procédé de contrôle de la distribution du programme d'ordinateur. Le programme est enregistré sur son support sous forme chiffrée, et il est ensuite déchiffré avant chargement sur l'ordinateur par l'utilisateur autorisé. L'utilisateur autorisé dispose à cet effet de moyens permettant le déchiffrement. Ce procédé a l'avantage d'éviter la duplication du support contenant le programme chiffré mais à l'inconvénient de ne pas éviter la copie du programme à partir du PC.

On connaît également un procédé de contrôle de l'exécution du programme. Il consiste à mettre en oeuvre une procédure permettant de vérifier la présence d'un dispositif sécurisé branché notamment sur une imprimante, ce dispositif attestant de par sa présence que l'utilisateur est

autorisé à utiliser le programme. Lors de l'exécution du programme, on vérifie la présence et l'authenticité du dispositif sécurisé, la vérification conditionnant la poursuite de l'exécution du programme. Ce procédé a l'inconvénient de pouvoir être contourné en sautant les instructions correspondant à cette vérification.

On connaît également un procédé de contrôle de l'usage d'un micro-ordinateur et donc indirectement de tout programme contenu à l'intérieur, par une personne autorisée. Il met en oeuvre une carte à puce telle qu'une carte à micro-circuit, appélée communément « smart-card ». Dans ce procédé, un micro-ordinateur PC est relié a l'aide d'une interface adaptée à la « smart-card » qui contient un code secret d'authentification. L'usager autorisé doit introduire au clavier le code d'accès qui est comparé à celui stocké dans la « smart-card ». En cas d'adéquation, l'accès à l'ordinateur ou à des informations ou à un programme de l'ordinateur est autorisé.

Ce procédé a l'inconvénient de ne pas protéger directement le support avant le chargement du programme dans l'ordinateur. On peut donc dupliquer le support.

Dans la description qui va suivre on entend par smart-card tout support comprenant au moins un module de sécurité contenant un microprocesseur et un espace mémoire apte à contenir une donnée secrète telle qu'une clé secrète ainsi que des programmes secrets. En particulier, il s'agit d'une carte au format normalisé d'une carte à puce ou d'une mini-carte à puce ou une carte d'extension de PC, ou un module enfichable à un port d'entrée/sortie d'ordinateur.

L'objectif de la présente invention est de proposer une solution au problème de piratage sous ses différentes formes qui soit plus efficace que les solutions actuelles.

La solution apportée par l'invention se situe également au niveau du contrôle de l'exécution d'un programme d'ordinateur. L'exécution est contrôlée du fait qu'elle est uniquement permise aux personnes qui ont acquis un droit d'utilisation. Ce droit est matérialisé par un moyen ou accesoire sécurisé

notamment une « smart-card » selon un exemple de l'invention. Par ce biais, on dissuade d'effectuer toute duplication ou toute diffusion du programme.

A cet effet, l'invention a d'abord pour objet un procédé de contrôle de l'exécution d'un programme d'ordinateur. Selon un premier mode, il est caractérisé en ce qu'il comporte les étapes suivantes consistant à :

1) Scinder un programme en au moins deux parties, respectivement publique et secrète, la partie publique étant apte à être exécutée sur un premier moyen de traitement, la partie secrète étant apte à être exécutée sur un deuxième moyen de traitement sécurisé.

2) disposer ladite partie publique dans une mémoire du premier moyen de traitement,

3) disposer la partie secrète sur un support sécurisé du deuxième moyen de traitement destiné à être lu par ledit premier moyen de traitement,

4) effectuer les opérations suivantes lors de l'exécution du programme par le premier moyen de traitement :

a) transmission du premier moyen de traitement au deuxième de paramètres/variables fonctions de signaux externes déclenchés par un utilisateur,

b) exécution d'au moins une partie du programme par le deuxième moyen de traitement en mettant en oeuvre un certain nombre desdits paramètres/variables reçus,

c) transmission du deuxième moyen de traitement au premier, des résultats de l'exécution de l'alinéa précédent b),

d) exploitation d'un certain nombre desdits résultats dans l'exécution réalisée par le premier moyen.

Selon un autre mode de réalisation, le procédé comporte les étapes suivantes consistant à :

1') Scinder un programme en au moins deux parties, respectivement publique et secrète, la partie publique étant apte à être exécutée sur un premier moyen de traitement, la partie secrète étant apte à être exécutée sur un deuxième moyen de traitement sécurisé.

2') chiffrer au moins une partie secrète et la disposer avec la partie publique sur un même support, celui-ci étant destiné à être lu par ledit premier moyen de traitement,

3') disposer dans le deuxième moyen de traitement une fonction de déchiffrement correspondante,

4') effectuer les opérations suivantes lors de l'exécution du programme:

a') transmission du premier moyen de traitement vers le deuxième de tout ou partie de la partie secrète chiffrée,

b') déchiffrement de ladite partie secrète chiffrée reçue par le deuxième moyen de traitement sécurisé en mettant en oeuvre ladite fonction de déchiffrement et conservation en mémoire sécurisée de la partie secrète en clair,

c') transmission du premier moyen de traitement au deuxième de paramètres/variables fonctions de signaux externes,

d') exécution d'au moins une partie secrète par le deuxième moyen de traitement sécurisé en exploitant un certain nombre desdits paramètres/variables recues,

e') transmission du deuxième moyen de traitement au premier des résultats de l'exécution de l'alinéa précédent d');

f') exploitation d'un certain nombre desdits résultats dans l'exécution réalisée par le premier moyen.

Selon une caractéristique de mise en oeuvre de la seconde variante, à l'opération a'), on transmet une partie du programme chiffré au fur et à mesure des besoins et/ou en fonction de la capacité du deuxième moyen de traitement sécurisé.

Grâce à cette caractéristique, on peut exécuter un programme chiffré de dimension supérieure à la capacité mémoire du deuxième moyen de traitement.

L'invention sera mieux comprise à la lecture de la description des deux modes de mise en oeuvre du procédé sur un exemple de programme d'ordinateur.

Le programme retenu pour l'exemple est un programme de traitement de texte.

Pour la mise en oeuvre du procédé, il est nécessaire de scinder le programme de traitement de texte en au moins deux parties, respectivement publique et secrète. La partie publique est apte à être exécutée sur un premier moyen de traitement tandis que la partie secrète est apte à être exécutée sur un deuxième moyen de traitement sécurisé. Elles peuvent donc être amenées à subir une compilation appropriée distincte pour l'une et l'autre.

La première partie est dite publique et exécutable sur un système d'exploitation de micro-ordinateur (PC) pris dans l'exemple comme premier moyen de traitement.

La deuxième partie dite secrète est quant à elle exécutable sur un circuit sécurisé de carte à puce pris dans l'exemple comme un deuxième moyen de traitement. Le circuit sécurisé comporte un processeur 8 bits, une mémoire permanente ROM contenant le système d'exploitation de la carte, et une mémoire non volatile de type EEPROM et une mémoire volatile de travail de type RAM. Le circuit peut par exemple être le circuit d'une « smart-card ».

Lors du stockage du programme de traitement de texte sur un support destiné à être distribué commercialement, celui-ci est réparti sur des supports de mémorisation ou d'enregistrement distincts. Pour cela, dans l'exemple, on dispose la partie publique sur un disque optique (CD-ROM) tandis que la partie secrète est disposée dans la mémoire EEPROM de la carte à puce. Le programme nécessite donc dans ce cas comme support physique pour le matérialiser deux éléments: le disque optique et une carte à puce associée. Dans l'exemple, on a choisi la fonction de calcul de la position du curseur sur l'écran d'un PC pour constituer la partie secrète. Cette fonction manquante dans le disque optique se trouve donc uniquement dans la carte à puce.

Pour l'exécution du programme, le PC est connecté à la carte à puce par une interface de manière à permettre une communication bi-directionnelle entre eux. Le programme public du disque optique est chargé dans le PC par lecture du disque optique. La carte à puce peut être par exemple connectée au

PC par l'intermédiaire d'un lecteur de carte à puce lui même relié à un port d'entrée/sortie du PC.

Au cours de l'exécution selon l'invention, on effectue les opérations ou étapes ci-après.

On transmet du premier moyen de traitement au deuxième des paramètres/variables fonction de signaux externes.

D'une manière générale, on entend par signaux externes des informations ou des événements qui sont susceptibles d'être différents à chaque utilisation du programme. La sécurité du système est d'autant mieux assurée que l'ensemble des informations communiquées à la carte diffère à chaque utilisation. Elle est également d'autant mieux assurée que le programme dans la carte à puce est complexe parce qu'il comporte, par exemple, énormément de sorties possibles et que la relation entre les entrées et les sorties est sophistiquée.

Au sens de la présente invention, peuvent par exemple constituer des signaux externes, les actions déclenchées par l'utilisateur via une souris ou un clavier ou autre périphérique d'entrée.

Dans l'exemple, c'est l'unité centrale du PC qui transmet, via l'interface, à la carte les données qui correspondent aux touches du clavier actionnées par l'utilisateur. L'unité centrale effectue cette transmission en exécutant le programme public et les fonctions du système d'exploitation. A cet effet, le programme public comporte les instructions nécessaires à cette transmission.

Selon une étape suivante du procédé, on exécute au moins une partie du programme par le deuxième moyen de traitement sécurisé en exploitant un certain nombre desdits paramètres/variables recues. Cela implique que la sortie de l'exécution de cette partie du programme va dépendre fortement de la valeur ou nature des paramètres/variables exploitées ou pris en compte par le deuxième moyen de traitement pour l'exécution du programme secret.

Dans l'exemple, lorsque l'utilisateur frappe les touches du clavier, la carte exécute donc le calcul de la position du curseur dans une ligne de texte

sur l'écran et renvoie le résultat au PC, en l'occurrence la valeur de cette position, conformément à une autre étape du procédé.

Ensuite, selon le procédé on peut utiliser les résultats ci-dessus tel quels ou de préférence prendre en compte ou exploiter un certain nombre desdits résultats ci-dessus dans l'exécution réalisée par le premier moyen. Dans l'exemple, l'unité centrale du PC exécute la partie publique du programme pour afficher sur l'écran la position du curseur.

On constate que l'utilisateur ne peut utiliser la fonction curseur du traitement de texte en l'absence de la carte. Par ce biais, on dissuade toute copie illicite du logiciel du traitement de texte puisqu'il est inutilisable sans la carte. On comprend que grâce à l'invention, la dissuasion ci-dessus soit d'autant plus efficace que la partie secrète correspond à une partie essentielle du programme.

On va décrire maintenant un autre mode de mise en oeuvre du procédé de l'invention.

Le système nécessaire à la mise en oeuvre du procédé est identique à celui décrit précédemment avec les différences ci-après.

La partie secrète est disposée sous forme chiffrée sur le disque optique avec la partie publique au lieu d'être disposée dans la carte à puce.

La mémoire ROM de la carte contient en plus du système d'exploitation, une fonction de déchiffrement et de chargement du programme déchiffré dans sa mémoire RAM.

Au cours de l'exécution du programme selon l'invention, on effectue les opérations ou étapes ci-après.

On transmet du premier moyen de traitement au deuxième tout ou partie du programme chiffré.

Dans l'exemple, c'est la fonction de calcul de la position du curseur qui est chiffrée. Celle-ci est transmise chiffrée par le programme de traitement de texte à la carte à puce par exemple au démarrage du programme. Elle peut également être transmise seulement à l'instant où elle devient nécessaire. A cet effet, le programme de traitement de texte inclut également des

informations permettant de la localiser notamment son adresse ou son nom de fichier.

Selon le procédé, on déchiffre ladite partie secrète chiffrée reçue par le deuxième moyen de traitement sécurisé en mettant en oeuvre ladite fonction de déchiffrement et on conserve en mémoire sécurisée la partie secrète en clair.

Dans l'exemple, la carte à puce déchiffre la fonction de calcul de la position du curseur en mettant en oeuvre sa fonction de déchiffrement et mémorise sous forme exécutable la fonction en question.

On constate dans cet exemple que le procédé met en oeuvre un système comportant une smart-card, celle ci étant apte à charger tout ou partie du programme chiffré, à déchiffrer avec une clé secrète de l'éditeur du logiciel, à recevoir des appels des premier moyens et à les transmettre pour le programme exécutable qui a été préalablement chargé, à retourner les résultats au premier moyen de traitement.

Le programme exécutable public comporte des instructions supplémentaires pour transmettre des parties de programme secret à la carte, via des fonctions entrée/sortie du système d'exploitation de la carte ou éventuellement via celles du système d'exploitation du PC, et des instructions pour des appels à des fonctions chargées dans la carte.

Par extension des applications possibles du procédé de l'invention, le deuxième moyen traitement peut être sous forme câblée dans une carte à mémoire ceci afin de diminuer le coût de l'accessoire.

Quant au premier moyen de traitement, il est généralement une unité centrale d'un ordinateur personnel.

Avantageusement, préalablement au chargement de la partie publique sur le premier moyen de traitement tel un PC, celle-ci peut être disponible sur un centre serveur ou une base de données auquel l'unité centrale du premier moyen peut être relié. La partie publique d'un programme ou logiciel peut être également disponible sur un réseau notamment de type internet auquel le premier moyen de traitement peut être relié au souhait de l'utilisateur.

Ainsi, pour un acquéreur potentiel d'un logiciel, il suffit de rechercher le logiciel disponible sur le réseau tel internet et de le charger dans la mémoire de son PC. Parallèlement, l'acquéreur peut recevoir la carte contenant la partie secrète notamment par courrier.

Bien que le logiciel soit disponible par tout le monde sur le réseau internet, il n'est utilisable que si l'utilisateur dispose de l'accessoire matérialisé notamment par une carte à microprocesseur.

Ainsi, par ce biais, l'invention permet à l'éditeur de logiciel de s'affranchir de la duplication de ces derniers sur un support physique tel qu'une disquette. L'invention le dispense également de la distribution physique du logiciel.

En accompagnement des logiciels exécutables mis sur internet, il est possible de joindre des données telles que le contenu d'un manuel d'utilisation d'un logiciel.

REVENDICATIONS

1. Procédé de contrôle de l'exécution d'un programme d'ordinateur caractérisé en ce qu'il comporte les étapes suivantes consistant à :

1) Scinder un programme en au moins deux parties, respectivement publique et secrète, la partie publique étant apte à être exécutée sur un premier moyen de traitement, la partie secrète étant apte à être exécutée sur un deuxième moyen de traitement sécurisé.

2) disposer ladite partie publique dans une mémoire du premier moyen de traitement,

3) disposer la partie secrète sur un support sécurisé du deuxième moyen de traitement destiné à être lu par ledit premier moyen de traitement,

4) effectuer les opérations suivantes lors de l'exécution du programme par le premier moyen de traitement :

a) transmission du premier moyen de traitement au deuxième de paramètres/variables fonctions de signaux externes déclenchés par un utilisateur,

b) exécution d'au moins une partie du programme par le deuxième moyen de traitement en mettant en oeuvre un certain nombre desdits paramètres/variables reçus,

c) transmission du deuxième moyen de traitement au premier des résultats de l'exécution de l'alinéa précédent b),

d) exploitation d'un certain nombre desdits résultats dans l'exécution réalisée par le premier moyen.

2. Procédé de contrôle de l'exécution d'un programme d'ordinateur caractérisé en ce qu'il comporte les étapes suivantes consistant à :

1') Scinder un programme en au moins deux parties, respectivement publique et secrète, la partie publique étant apte à être exécutée sur un premier moyen de traitement, la partie secrète étant apte à être exécutée sur un deuxième moyen de traitement sécurisé.

2') chiffrer au moins une partie secrète et la disposer avec la partie publique sur un même support, celui-ci étant destiné à être lu par ledit premier moyen de traitement,

3') disposer dans le deuxième moyen de traitement une fonction de déchiffrement correspondante,

4') effectuer les opérations suivantes lors de l'exécution du programme:

a') transmission du premier moyen de traitement vers le deuxième de tout ou partie de la partie secrète chiffrée,

b') déchiffrement de ladite partie secrète chiffrée reçue par le deuxième moyen de traitement sécurisé en mettant en oeuvre ladite fonction de déchiffrement et conservation en mémoire sécurisée de la partie secrète en clair,

c') transmission du premier moyen de traitement au deuxième de paramètres/variables fonctions de signaux externes,

d') exécution d'au moins une partie secrète par le deuxième moyen de traitement sécurisé en exploitant un certain nombre desdits paramètres/variables recues,

e') transmission du deuxième moyen de traitement au premier des résultats de l'exécution de l'alinéa précédent d');

f') exploitation d'un certain nombre desdits résultats dans l'exécution réalisée par le premier moyen.

3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que le deuxième moyen de traitement est une carte à micro-processeur.

4. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que le deuxième moyen de traitement est sous forme cablée dans une carte à mémoire.

5. Procédé selon l'une quelconque des revendications précédentes caractérisé en ce que le premier moyen de traitement est une unité centrale d'un ordinateur.

6. procédé selon l'une quelconque des revendications précédentes caractérisé en ce que l'unité centrale est reliée à un réseau notamment de type internet, sur lequel la partie publique du programme est disponible.

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

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

N° d'enregistrement national

FA 542984
FR 9705328

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
Y	WO 97 04412 A (CABLE TELEVISION LAB INC) * abrégé; figures 1,2 * * page 2, ligne 6 - page 4, ligne 2 * * page 5, ligne 3 - ligne 15 * * page 6, ligne 3 - page 8, ligne 17 *	1,3-6
A	---	2
Y	FERREIRA R C: "THE SMART CARD: A HIGH SECURITY TOOL IN EDP" PHILIPS TELECOMMUNICATION REVIEW, vol. 47, no. 3, 1 septembre 1989, pages 1-19, XP000072642 * le document en entier *	1,3-6
A	---	2
A	EP 0 191 162 A (IBM) * revendications 1-9 *	1,2

A	BE 1 009 122 A (AWAX PROGETTAZIONE) * le document en entier *	1,2

A	KEUL M: ""DONGLES": HARDWARE SCHUTZT SOFTWARE" ELEKTRONIK, vol. 39, no. 10, 11 mai 1990, pages 82-84, 86, XP000117036 * page 83, colonne de droite, ligne 32 - page 86, colonne de droite, ligne 6 *	1,2

A	EP 0 268 138 A (IBM) * colonne 1, ligne 41 - colonne 2, ligne 4 *	2

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G06F

Date d'achèvement de la recherche	Examinateur
8 janvier 1998	Powell, D

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 (P04C13)