(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

PCT

(43) Date de la publication internationale
21 décembre 2007 (21.12.2007)

(10) Numéro de publication internationale
WO 2007/144504 A3

(51) **Classification internationale des brevets :**
***G06F 21/00* (2006.01)** ***G06F 21/24* (2006.01)**

(21) **Numéro de la demande internationale :**
PCT/FR2007/000974

(22) Date de dépôt international : 13 juin 2007 (13.06.2007)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0605360 16 juin 2006 (16.06.2006) FR

(71) **Déposant** *(pour tous les États désignés sauf US)* : **OLFEO** [FR/FR]; 47 rue de Sèvres, F-75006 Paris (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **SOUILLE, Alexandre** [FR/FR]; 47 rue de Sèvres, F-75006 Paris (FR).

(74) Mandataire : KEIB, Gérard; Pontet Allano & Associés SELARL, 6 avenue du Général de Gaulle, F-78000 VERSAILLES (FR).

(81) **États désignés** *(sauf indication contraire, pour tout titre de protection nationale disponible) :* AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, **BR,** BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, **HR,** HU, **ID,** IL, IN, IS, **JP,** KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, **BJ,** CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

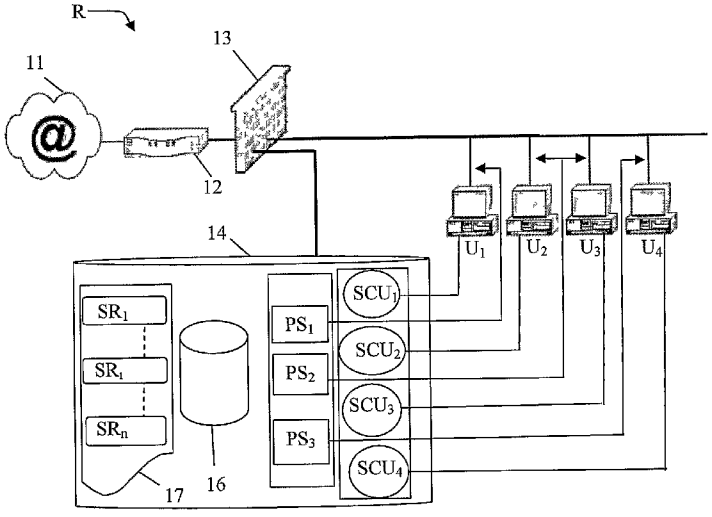
Publiée :

— *avec rapport de recherche internationale*

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM FOR PROCESSING SECURITY DATA OF A COMPUTER NETWORK

(54) Titre : PROCÉDÉ ET SYSTÈME DE TRAITEMENT DE DONNÉES DE SÉCURITÉ D'UN RÉSEAU INFORMATIQUE



(57) Abstract: Method of processing security data of a computer network (R) comprising a plurality of users (U_1-U_4), this method comprising the following steps:- analyzing data relating to at least one content or service accessed by at least one of said users (U_1-U_4) through said network (R); - as a function of said analysis, determining data relating to the behaviour of said user (U_1-U_4), said data making up a so-called behavioural signature (SCU_1-SCU_4) of said user (U_1-U_4); - comparing said behavioural signature (SCU_1-SCU_4) with at least one so-called référence signature (SR_1-SR_n), said référence signature comprising data representing a predefined model behaviour; and - triggering at least one so-called security action as a function of said comparison.

[Suite sur la page suivante]

WO 2007/144504 A3

— *avec revendications modifiées*

(88) Date de publication du rapport de recherche internationale: 20 mars 2008

Date de publication des revendications modifiées:
15 mai 2008

(57) Abrégé : Procédé de traitement de données de sécurité d'un réseau informatique (R) comportant une pluralité d'utilisateurs (U_1-U_4), ce procédé comprenant les étapes suivantes: - analyse de données relatives à au moins un contenu ou un service accédé par au moins un desdits utilisateurs (U_1-U_4) au travers dudit réseau (R); - en fonction de ladite analyse, détermination de données relatives au comportement dudit utilisateur (U_1-U_4), lesdites données composant une signature (SCU_1-SCU_4) dite comportementale dudit utilisateur (U_1-U_4); - comparaison de ladite signature comportementale (SCU_1-SCU_4) à au moins une signature (SR_1-SR_n), dite de référence, ladite signature de référence comprenant des données représentant un comportement modèle prédéfini; et - déclenchement d'au moins une action, dite de sécurisation, en fonction de ladite comparaison.

REVENDICATIONS MODIFIÉES

reçues par le Bureau international le 18 mars 2008 (18.03.2008)

1. Procédé de traitement de données de sécurité d'un réseau informatique (R) comportant une pluralité d'utilisateurs (Ui-U_4) se trouvant au sein dudit réseau (R), ce procédé comprenant les étapes suivantes:

- analyse de données relatives à au moins un contenu ou un service accédé par au moins un desdits utilisateurs (Ui-U_4) au travers dudit réseau (R) ;
- en fonction de ladite analyse, détermination de données relatives au comportement dudit utilisateur (Ui-U_4), lesdites données étant internes audit réseau (R) et composant une signature (SCUi-SCU_4) dite comportementale dudit utilisateur (Ui-U_4) ;
- comparaison de ladite signature comportementale (SCUi-SCU_4) à au moins une signature (SRi-SR_n), dite de référence, ladite signature de référence comprenant des données représentant un comportement modèle prédéfini ; et
- déclenchement d'au moins une action de sécurisation dudit réseau (R), en fonction de ladite comparaison.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comprend en outre une définition d'une politique de sécurité (PSi-PS_3) pour au moins un utilisateur (U_1-U_4), ladite politique de sécurité (PSi-PS_3) comprenant des données relatives à au moins une règle d'accès dudit utilisateur (Ui-U_4) à au moins un contenu et/ou service au travers du réseau informatique (R).

3. Procédé selon l'une quelconque des revendications 1 ou 2, caractérisé en ce que l'action de sécurisation est fonction d'au moins une politique de sécurité (PSi-PS_3) associée à au moins un utilisateur (Ui-U_4).

4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'une action de sécurisation comprend une modification dynamique d'une politique de sécurité (PSi-PS_3).

5. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'une action de sécurisation comprend un envoi de données à au moins un utilisateur (Ui-U_4).

6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'une action de sécurisation comprend une modification d'accès d'un utilisateur (U_1-U_4) au réseau informatique (R).

7. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend en outre une définition d'au moins une signature de référence (SR_1-SR_n) pour au moins un utilisateur (U_1-U_4) et/ou un groupe d'utilisateurs.

8. Procédé selon la revendication 7, caractérisé en ce que la définition d'une signature de référence (SR_1-SR_n) est relative à une activité d'au moins un utilisateur (U_1-U_4).

9. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'une signature comportementale (SCU_1-SCU_4) comprend des données statistiques relatives à au moins un contenu et/ou service accédé par au moins un utilisateur (U_1-U_4).

10. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'une signature comportementale (SCU_1-SCU_4) comprend des données statistiques relative à au moins une catégorie de contenus et/ou services accèdes par au moins un utilisateur (Ui-U_4), ladite catégorie étant prédéfinie.

11. Procédé selon l'une quelconque des revendications 9 ou 10, caractérisé en ce que les données statistiques comprennent des données relatives à un nombre d'accès d'un utilisateur (U_1-U_4) à au moins un contenu et/ou service.

12. Procédé selon l'une quelconque des revendications 9 à 11, caractérisé en ce que les données statistiques comprennent des données relatives au

moment de l'accès d'un utilisateur ($Ui\text{-}U_4$) à au moins un contenu et/ou service.

13. Procédé selon l'une quelconque des revendications 9 à 12, caractérisé en ce que les données statistiques comprennent des données relatives à un temps d'accès d'un utilisateur ($Ui\text{-}U_4$) à au moins un contenu et/ou service.

14. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend en outre une représentation graphique (30) d'une signature comportementale ($SCUi\text{-}SCU_4$).

15. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que les données relatives à au moins un contenu ou service comprennent des données relatives à une catégorie ou famille dans laquelle ledit contenu à été au préalable classé en fonction de l'information qu'il représente.

16. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend en outre un classement dans au moins une catégorie d'un contenu et/ou d'un service, ledit classement étant réalisé en fonction d'une analyse des données relatives audit contenu et/ou service.

17. Procédé selon la revendication 16, caractérisé en ce qu'il comprend en outre une mise à jour dudit classement, ladite mise à jour état effectuée par connexion à un serveur distant.

18. Utilisation du procédé selon l'une quelconque des revendications précédentes, pour la gestion d'accès d'au moins un utilisateur ($Ui\text{-}U_4$) à des contenus au travers d'un réseau de type Internet (11).

19. Système mettant en œuvre le procédé selon l'une quelconque des revendications précédentes.