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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
6 septembre 2013 (06.09.2013)

WIPO | PCT

(10) Numéro de publication internationale
WO 2013/127619 A1

(51) Classification internationale des brevets :
H04L 12/24 (2006.01) *H04L 29/06* (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2013/052691

(22) Date de dépôt international :
11 février 2013 (11.02.2013)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1251858 29 février 2012 (29.02.2012) FR

(71) Déposant : **AMOSSYS** [FR/FR]; 4 bis allée du Bâtiment, F-35000 Rennes (FR).

(72) Inventeur : **HENN, Thibaut**; La Douve, F-35750 Geveze (FR).

(74) Mandataire : **LE SAUX, Gaël**; 90333, B, Technopole Atalante, 16B, rue de Jouanet, Bretagne, F-35703 Rennes Cedex 7 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

(54) **Title** : NETWORK INVENTORY METHOD

(54) **Titre** : MÉTHODE D'INVENTAIRE DE RÉSEAU

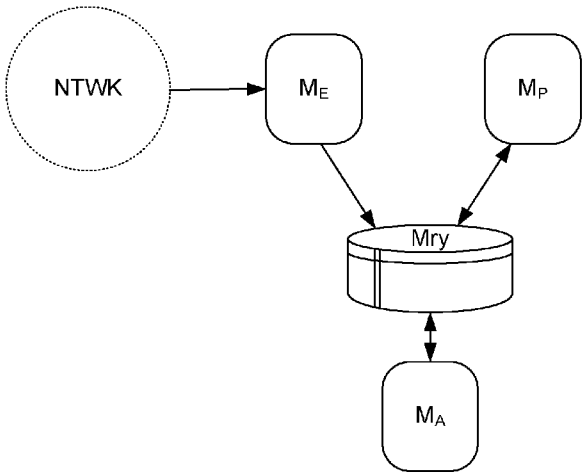

Figure 1

(57) **Abstract** : The invention relates to an inventory method for a communication network, said network comprising at least one host *h* exchanging data with other equipment of said network. According to the invention, said method comprises the following phases: a phase of obtaining at least one imprint *E* associated with said host h, said at least one imprint E comprising at least one notification of detection representative of at least one activation of at least one detection rule r by at least one element exchanged over said network and associated with said host *h*; a phase of obtaining, on the basis of said at least one imprint *E*, at least one probability p of presence of at least one service *s* within said host *h*, on the basis of at least one probabilistic database associating said at least one detection rule *r* with at least one predetermined probability.

(57) **Abrégé** : L'invention se rapporte à un procédé d'inventaire d'un réseau de communication, ledit réseau comprenant au moins un hôte *h* échangeant des données avec d'autres équipements dudit réseau. Selon l'invention, ledit procédé comprend les phases suivantes : une phase d'obtention d'au moins une empreinte *E* associée audit hôte h, ladite au moins une empreinte E comprenant au moins une notification de détection représentative d'au moins une activation d'au moins une règle de détection r par au moins un élément échangé sur ledit réseau et associé audit hôte *h*;

une phase d'obtention, à partir de ladite

[Suite sur la page suivante]

WO 2013/127619 A1

au moins une empreinte *E*, d'au moins une probabilité *p* de présence d'au moins un service *s* au sein dudit hôte *h*, à partir d'au moins une base de données probabiliste associant ladite au moins une règle de détection *r* à au moins une probabilité prédéterminée.

Méthode d'inventaire de réseau.

1 DOMAINE DE L'INVENTION

L'invention se rapporte à la surveillance de réseaux. L'invention se rapporte plus particulièrement à la surveillance de réseaux comprenant des terminaux de communication. De tels terminaux de communication peuvent prendre la forme d'ordinateurs personnels, d'assistants personnels, de tablettes ou de téléphones intelligents. Plus spécifiquement encore, l'invention concerne l'inventaire de tels réseaux de communication.

L'inventaire d'un réseau de communication consiste d'une part à lister les hôtes présents sur ce réseau, et d'autre part pour chacun de ces hôtes, à obtenir la liste des logiciels qui y sont installés, ainsi que leurs versions. Il s'agit de trouver les systèmes d'exploitation utilisés, les serveurs installés et disponibles, mais aussi des clients utilisés. Un tel inventaire prend tout son sens dans les réseaux de communications modernes, particulièrement les réseaux locaux d'entreprises, dans lesquels de plus en plus de terminaux de nature différentes sont connectés.

La connaissance de l'inventaire d'un réseau est importante, autant pour un administrateur que pour un attaquant car elle donne un aperçu de la sécurité du réseau. En effet, connaître les versions des logiciels présents permet de savoir, via des bases de données publiques, les vulnérabilités potentielles de ces logiciels, et donc, des machines vulnérables.

Maintenir un inventaire précis et à jour nécessite l'utilisation de logiciels dédiés. D'une part, la taille croissante des réseaux ne permet plus d'établir de liste manuellement. D'autre part la possibilité, pour les utilisateurs, d'installer leurs propres logiciels, ainsi que les mises à jours constantes des logiciels ne permet pas de maintenir ces listes à jours manuellement.

2 SOLUTIONS DE L'ART ANTÉRIEUR

Depuis de nombreuses années, l'inventaire de réseau de communication est au centre des préoccupations tant de la part d'éditeurs de logiciels, qui tentent

de fournir des solutions permettant de réaliser un tel inventaire de la manière la plus simple et la plus efficace possible, qu'au centre des préoccupations de groupes de personnes dont les intentions sont nettement moins louables, et pour lesquels l'obtention d'un inventaire de réseau permet de préparer des attaques destinées à récupérer des données confidentielles ou à mettre à mal un service de communication.

La méthode historique d'obtention d'inventaire consiste à se connecter manuellement aux serveurs du réseau de communication et à observer des bannières transmises par ces derniers. En effet, les différents logiciels de l'époque transmettaient au client leur nom, leur numéro de version, mais également le système d'exploitation les faisant fonctionner ainsi que sa version.

Depuis, et pour éviter que des attaquants ne devinent trop facilement les versions des logiciels installés, les services et logiciels sont moins verbeux et il est nécessaire d'utiliser des méthodes d'inventaire plus élaborées. Ainsi, on utilise des méthodes qui utilisent les protocoles de communications existants, par exemple à base de paquets (IP, pour « Internet Protocol », TCP pour « Transmission Control Protocol », UDP pour « User Datagram Protocol », etc.) pour réaliser l'inventaire. Parmi ces méthodes, on distingue les trois typologies d'approche suivantes :

1. les méthodes par agents : ces méthodes utilisent des agents logiciels installés sur chacun des postes surveillés et remontent les configurations de ces derniers vers un serveur central.
2. les méthodes actives : ces méthodes transmettent des paquets spécialement forgés vers les hôtes et analysent les réponses (ou l'absence de réponse) de ces derniers. On subdivise généralement les méthodes actives en deux catégories:
    a. les méthodes à balayage de ports, consistant à découvrir les ports ouverts chez le destinataire des paquets transmis;

b. la prise d'empreinte de systèmes, consistant à découvrir les systèmes d'exploitation hébergés sur les hôtes en fonction de règles de détection de systèmes et/ou de services.

3. les méthodes passives : ces méthodes ne transmettent pas de paquet sur le réseau mais effectuent une analyse du trafic capturé pour déterminer les services utilisant le réseau. On réalise alors un prise d'empreinte du ou des systèmes en appliquant sur des évènements et/ou des paquets des règles de détection qui délivrent un résultat.

Récemment, une technique hybride a été proposée, elle utilise une première phase d'inventaire passif et une deuxième phase d'inventaire actif. Lors d'une requête d'un utilisateur en vue de construire un inventaire, si la connaissance de l'outil (qui met en œuvre la méthode hybride) ne permet pas d'y répondre, une phase active est instanciée pour tenter de compléter la base.

On ne détaille pas dans la présente divulgation, ces différentes méthodes qui sont considérées comme étant bien connues de l'homme du métier.

Pour ce qui est des méthodes à base d'agents, c'est l'approche la plus intrusive pour le réseau car elle nécessite d'installer des agents logiciels sur tous les postes surveillés. Ces derniers ont pour charge d'extraire la configuration du poste pour l'envoyer ensuite vers un serveur central. Bien que fiables, ces méthodes sont parfois jugées trop intrusives. Il est parfois impossible d'intervenir sur tous les postes du réseau (impossibilité technique, organisationnelle ou juridique). C'est pour répondre à ces problèmes que les méthodes actives ou passives ont été mises au point.

La méthode active du balayage de ports (« scan de ports ») regroupe les techniques consistant à découvrir les ports TCP et UDP ouverts sur un hôte et d'en déduire les services qui y fonctionnent. Initialement, les scans de ports étaient effectués en tentant de se connecter aux ports des serveurs. Une deuxième technique, moins lourde consistait à n'envoyer que le premier paquet TCP (le SYN) et d'attendre la réponse (qui dépend de l'ouverture du port). Cependant, les

systèmes actuels comprennent en général des pare-feu (« firewall ») installés de manière standard qui limitent l'utilisation de telles techniques.

Les techniques actives de détection de systèmes et de services sont les premières à avoir été publiées. Elles faisaient suite à un besoin de détection des équipements présents sur le réseau. Toutes ces techniques fonctionnent sur le même principe : transmettre des paquets spécialement forgés et utiliser des signatures pour déduire le système en fonction des réponses reçues. Les différentes approches se focalisent plus sur les champs intéressants (des paquets transmis et reçus) que sur les techniques mises en œuvre. Elles mettent en œuvre des bases de données de règles de détection permettant de déterminer un système à l'aide des observations réalisées.

Les techniques passives ont été développées après les techniques actives. Elles font suite à un besoin de furtivité dans la phase de découverte des systèmes d'exploitation. En effet, suite à la publication des techniques actives, les outils de surveillance ont commencé à intégrer des règles de détection et des mécanismes pour détecter l'utilisation de ces outils.

Les techniques passives, bien que similaires dans leur démarche (déduire le système d'après les changements dans la valeur de certains champs), sont plus prolifiques en typologies de méthodes employées et la littérature propose plus d'originalité. Parmi les méthodes employées, certaines utilisent également des bases de données de règles de détection permettant de déterminer un système à l'aide des observations réalisées (c'est par exemple le cas du logiciel « p0f »). D'autres méthodes utilisent une classification naïve bayésienne à la place de règles de détection statiques.

Dans le cadre de la prise d'empreinte de système d'exploitation, il est parfois nécessaire de choisir entre plusieurs possibilités. Que ce soit lors d'une observation, ou après une série d'observations. En effet, les règles de détection ou les systèmes utilisés proposent parfois plusieurs solutions différentes pour expliquer leurs observations.

Au niveau atomique, c'est à dire après une seule observation, les systèmes à base de règles de détection choisissent le premier système listé (c'est par exemple le cas dans le logiciel *« p0f »*), les systèmes statistiques choisissent celui ayant la meilleure probabilité (exemple de Robert Beverly. *"A robust classifier for passive tcp/ip"*. In Fingerprinting, in PAM, 200). Ces méthodes ne gèrent pas les suites d'observations et des contradictions peuvent apparaître (dans *« A robust classifier for passive tcp/ip »*, ces contradictions sont interprétées comme plusieurs machines partageant la même adresse IP, ce qui n'est évidemment pas forcément le cas, et donc génère une fausse interprétation).

D'un autre côté, les méthodes actives, de par leur nature, gère nativement les séries d'observations. Deux approches différentes sont alors utilisées :

1. Dans une première approche, les requêtes (transmises par le dispositif en charge de réaliser l'inventaire) sont choisies à la manière d'un arbre de décision.Le dispositif sélectionne une requête permettant de supprimer des systèmes possibles jusqu'à ce qu'il n'en reste qu'un seul système possible. Cette approche pose problème puisque l'on élimine automatiquement, avec un arbre de décision, un ensemble de possibilités sur la base de la concordance d'une requête avec une seule règle de détection, concordance qui peut s'avérer fausse.
2. Dans une deuxième approche, les systèmes se voient attribuer un score (initialement 0). Chaque fois qu'une règle de détection est validée, le score des systèmes concernés augmente (de 1 dans le cas du logiciel « nmap », d'un coefficient déterminé par un expert dans le cas du logiciel « Xprobe »). Le système choisi est celui ayant le meilleur résultat (exprimé en pourcentage du score maximal possible).Là encore, cette approche pose problème car le résultat obtenu n'a pas de réalité mathématique. Il s'agit plutôt d'une sélection arbitraire du système qui présente le meilleur score.

3 RÉSUMÉ DE L'INVENTION

L'invention ne pose pas ces problèmes liés aux méthodes de l'art antérieur. En effet, la présente divulgation propose un système d'inventaire d'un réseau, fournissant une probabilité associée à ses déductions et une capacité d'apprentissage.

Plus particulièrement, l'invention se rapporte à un procédé d'inventaire d'un réseau de communication, ledit réseau comprenant au moins un hôte *h* échangeant des données avec d'autres équipements dudit réseau.

Selon un mode de réalisation, ledit procédé comprenant les phases suivantes :

- une phase d'obtention d'au moins une empreinte *E* associée audit hôte *h,* ladite au moins une empreinte *E* comprenant au moins une notification de détection représentative d'au moins une activation d'au moins une règle de détection *r* par au moins un élément échangé sur ledit réseau et associé audit hôte *h* ;
- une phase d'obtention, à partir de ladite au moins une empreinte *E*, d'au moins une probabilité *p* de présence d'au moins un service *s* au sein dudit hôte *h*, à partir d'au moins une base de données probabiliste associant ladite au moins une règle de détection *r* à au moins une probabilité prédéterminée.

Ainsi, à la différence des méthodes de l'art antérieur, dans lesquelles des scores en pourcentage sont affectés aux hôtes et équipements du réseau de communication, l'invention permet d'obtenir un ensemble de probabilités associé aux règles déclenchées lors de la reconnaissance.

Selon un mode de réalisation particulier, ledit procédé comprend en outre une phase préalable d'apprentissage comprenant une étape de remplissage de ladite base de données probabiliste à l'aide d'un réseau de communication comprenant des équipements connus.

Selon un mode de réalisation particulier, ladite phase d'obtention de ladite au moins une empreinte E dudit hôte h comprend au moins une itération des étapes suivantes :

- réception d'un élément en provenance dudit réseau de communication et associée audit hôte h ;
- application, audit élément, d'au moins une règle de détection r parmi une base de données de règles de détection R, délivrant une notification de détection ;
- sauvegarde, au sein d'une liste de notification de prise d'empreinte A, de ladite notification de détection lorsque ladite notification de détection est au moins partiellement positive, ladite liste de notification de prise d'empreinte A représentant ladite empreint E.

Selon un mode de réalisation particulier, ladite notification de détection délivrée lors de ladite application de ladite au moins une règle de détection délivre un résultat binaire.

Selon un mode de réalisation particulier, ladite notification de détection délivrée lors de ladite application de ladite au moins une règle de détection délivre un résultat probabiliste.

Selon un mode de réalisation particulier, ladite phase d'obtention d'au moins une probabilité p de présence d'au moins un service s au sein dudit hôte h comprend, pour chaque notification de ladite empreinte de détection E :

- une étape d'obtention, à partir de ladite au moins une base de données probabiliste, d'au moins une probabilité p_s associée à ladite notification ;
- une étape de calcul d'une probabilité résultante p_r telle que :

$$p_r = p_a + p_s - p_a p_s$$

dans laquelle p_a désigne une probabilité antérieure associée dans une itération préalable ou 0 lorsque qu'aucune itération préalable n'a été mise en œuvre ;

- une étape de sauvegarde de ladite probabilité résultante p_r.

Selon un mode de réalisation particulier, lors du calcul de ladite probabilité résultante p_r, ladite probabilité antérieure p_a est affecté d'un coefficient c^{dt} dont la valeur est fonction du temps écoulé entre lesdites notifications de ladite empreinte de détection et/ou d'un coefficient ayant une valeur prédéterminée.

L'invention concerne également un dispositif d'inventaire d'un réseau de communication, ledit réseau comprenant au moins un hôte h échangeant des données avec d'autres équipements dudit réseau.

Selon un mode de réalisation particulier, ledit dispositif comprend :

- des moyens d'obtention d'au moins une empreinte E associée audit hôte h, ladite au moins une empreinte E comprenant au moins une notification de détection représentative d'au moins une activation d'au moins une règle de détection r par au moins un élément échangé sur ledit réseau et associé audit hôte h ;
- des moyens d'obtention, à partir de ladite au moins une empreinte E, d'au moins une probabilité p de présence d'au moins un service s au sein dudit hôte h, à partir d'au moins une base de données probabiliste associant ladite au moins une règle de détection r à au moins une probabilité.

L'invention concerne également un produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, et comprenant des instructions de code de programme pour la mise en œuvre de la méthode précédemment décrite.

4 LISTE DES FIGURES

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation préférentiel, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- la figure 1 présente un synoptique d'un mode de réalisation de l'invention ;
- la figure 2 présente schématiquement un dispositif de mise en œuvre de l'invention.

5 DESCRIPTION DÉTAILLÉE DE L'INVENTION

5.1 Rappel du principe de l'invention

La méthode présentement décrite ne présente pas les inconvénients de l'art antérieur. Au contraire, la méthode décrite permet de prendre compte pour l'identification d'un système, les résultats précédemment obtenus. À la différence des techniques antérieures, cette prise en compte est effectuée de manière récursive et non discriminatoire : cela signifie par exemple que les inconvénients liés aux arbres de décision ne sont pas présents avec la méthode décrite. Cela signifie également que les inconvénients liés au scoring (attribution d'un pourcentage) n'est pas présent dans la méthode décrite.

Par ailleurs, la méthode décrite offre la possibilité de corriger des résultats erronés en mettant à jour la base de connaissance qui est utilisée pour obtenir les résultats d'identification de règles de détection.

Le principe général repose sur un calcul probabiliste récursif. Ce calcul permet, à la différence des techniques antérieures, d'obtenir une suite de probabilités d'appartenance ou de non appartenance. Ce calcul permet également d'éviter que certaines possibilités de concordance soient purement et simplement éliminées, comme cela est le cas d'autres systèmes.

Plus particulièrement, l'invention met en œuvre une technique dans laquelle une base de données probabiliste est utilisée. Cette base de données probabiliste répertorie, pour une règle de détection donnée, des probabilités associées à des systèmes (et/ou des services). L'invention utilise cette base de données de probabilités pour associer un hôte donné à une certaine quantité de services possibles, cette quantité de services possible étant fonction du

déclenchement des règles de détection par rapport aux paquets « écoutés » sur le réseau.

Ainsi, de manière générale, l'invention se rapporte à une méthode d'inventaire d'un réseau de communication, ledit réseau comprenant au moins un hôte *h* échangeant des données avec d'autres équipements dudit réseau, ledit procédé comprenant les phases suivantes :

- une phase d'obtention d'au moins une empreinte *E* associée audit hôte *h,* ladite empreinte *E* comprenant au moins une notification de détection représentative d'au moins une activation d'au moins une règle de détection *r* par au moins un élément échangé sur ledit réseau et associé audit hôte *h* ;
- une phase d'obtention, à partir de ladite au moins une empreinte *E*, d'au moins une probabilité *p*de présence d'au moins un service *s* au sein dudit hôte *h*, à partir d'au moins une base de données probabiliste associant ladite au moins une règle de détection *r* à au moins une probabilité prédéterminée.

En d'autres termes, l'invention comprend les phases suivantes :

1. une phase d'observation a lieu, au cours de laquelle les données exploitables qui transitent sur le réseau (par exemple des paquets TCP, des paquets IP, etc.) sont utilisées pour former une empreinte et être injectées dans un module de prise d'empreinte.
    a. ce module de prise d'empreinte fonctionne de manière itérative et tente, au moins pour une portion des règles de détection de la base de données de règles de détection, d'appliquer ces règles de détection sur les données exploitables ;
    b. lorsqu'une donnée exploitable active une règle de détection *r* (le résultat binaire de l'activation est « 1 »), cette activation est conservée en base de données (ainsi que son

association avec l'hôte h à l'origine de la donnée exploitable) pour être utilisée par la suite.

c. le module de prise d'empreinte poursuit la prise d'empreinte tant que des données exploitables lui sont fournies.

d. Pour un hôte donnée h, l'empreinte E, obtenue à l'issue de cette phase de prise d'empreinte, est constituée de la suite ordonnée ou non des règles de détection activées (r_i), et est enregistrée en base de données.

2. Lorsqu'une ou plusieurs empreintes sont disponibles, elles peuvent être utilisées par un module de calcul probabiliste. Ce module utilise une empreinte E pour calculer récursivement la probabilité de découverte d'un ou plusieurs systèmes (services) s_i qui pourraient être associés à cette empreinte :

a. pour chaque règle de détection r_i activée d'une empreinte E, on identifie, au sein de la base de données, la liste des systèmes associés et leurs probabilités de présence respectives.

b. ces probabilités sont combinées aux probabilités précédentes (ou à une probabilité 0 s'il s'agit de la première itération récursive) pour délivrer une probabilité résultante.

c. ce processus récursif est mis en œuvre tant qu'il reste des règles de détection (associées à des probabilités) à traiter.

Le résultat obtenu à l'issue de cette phase de calcul probabiliste, pour un hôte h donné, est un ensemble de probabilités associées à un ou plusieurs systèmes (services).

On peut noter que selon l'invention, l'utilisation d'une base de données probabiliste permet d'obtenir un résultat mathématique qui représente une réelle

connaissance. Ceci est bien différent des systèmes de l'art antérieur. En effet, il est très rare que la validation d'une règle puisse à coup sûr permettre l'identification d'un système. Il est plus logique (et plus intuitif) de considérer qu'un résultat donné représente une certaine probabilité.

Par la suite, on présente notamment un mode de réalisation de l'invention. Il est clair cependant que ce mode de réalisation ne limite en rien la portée de l'invention, et que d'autres modes de réalisation peuvent être envisagés sans sortir du cadre de l'invention.

5.2 Description d'un mode de réalisation

On présente dans ce mode de réalisation, une mise en œuvre de la méthode précédemment décrite.

Ce mode de réalisation s'articule autour de quatre éléments complémentaires. La figure 1 schématise l'architecture globale de ce mode de réalisation et liste les quatre principaux éléments :

- la mémoire (*Mry*), volatile ou non : stocke les connaissances à priori*(les probabilités)*, les paramètres du modèle et les résultats intermédiaires ;
- le module de prise d'empreinte (M_E) : écoute le réseau et notifie (enregistre dans la mémoire *Mry*) lorsque des règles de détection valident des paquets réseau ;
- le module d'estimation des probabilités (M_P) utilise les notifications (issues du module de prise d'empreintes M_E) et communique avec la mémoire (*Mry*) pour estimer la probabilité d'hébergement des services ;
- le module d'apprentissage des paramètres : communique avec la base de données(*Mry*) pour mettre à jour les paramètres du modèle.

Les modules de ce mode de réalisation peuvent être déployés sur des machines différentes, ou regroupés, totalement ou partiellement sur une seule et même machine et/ou dans un seul et même composant logiciel sans en changer les principes.

La description de ce mode de réalisation suit les modules listés sur le schéma de la figure 1.

5.2.1 Mémoire

La mémoire permet d'accéder et de modifier les éléments suivants :

1. des listes :
   a. La liste des services et/ou systèmes informatiques à prendre en compte (*S*) ;
   b. La liste des hôtes observés (*H*) ;
   c. La liste des règles de détection(*R*) ;
   d. La liste des notifications de la prise d'empreinte (*A*) ;
2. des compteurs :
   a. le nombre de fois qu'une règle de détection a été validée pour un hôte hébergeant un service, sous la forme d'une table d'enregistrements de la forme *(r, s, c)* où « *r* » est une règle de détection, « *s* » est un service, et « *c* » est le compteur ; ces compteurs sont regroupés dans *C*.
   b. le nombre de validation d'une règle de détection, ce nombre se calcule comme la somme des compteurs pour une règle de détection donnée, ces compteurs sont regroupés dans *V*.
3. des résultats intermédiaires :
   a. les probabilités, pour les hôtes *(h)*, que les services *(s)* y soient hébergés (notés $P_h(s)$), elle peut prendre la forme d'une table contenant des éléments de la forme d'enregistrements $(h, s, P_h(s))$; ces probabilités sont regroupées dans *P*.

Dans ce mode de réalisation, pour économiser l'espace mémoire, seul les enregistrements dont la probabilité est strictement positive sont stockés.

Au démarrage de l'outil, les listes des règles de détection et des services sont valorisées d'après des bases de connaissances à priori. Pour tout service qu'une règle de détection est capable de détecter (d'après les connaissances à

priori), le compteur correspondant est initialisé à 1 (il est à 0 sinon). Les autres éléments sont vides et seront valorisés pendant l'exécution de l'outil.

5.2.2 Prise d'empreinte passive à base de règles de détection

La prise d'empreinte passive est réalisée par le module de prise d'empreinte M_E. La prise d'empreinte passive utilise une approche par règle de détection binaire. Ces règles de détection prennent en entrée un paquet réseau et fournissent en sortie un booléen (décision vrai/faux). Le principe d'obtention d'un résultat associé à une règle de détection est donc simple.

D'une manière générale, tout système de règles de détection binaires est utilisable dans le cadre de ce mode de réalisation, la seule contrainte étant de fournir une indication binaire pour les éléments du trafic observé (« vrai » ou « 1 » pour une application de la règle de détection à un paquet et « faux » ou « 0 » pour une non-application de la règle de détection à un paquet).

Note : dans ce mode de réalisation de l'invention, l'indication binaire est privilégiée pour des raisons de simplicité. Bien entendu, une indication probabiliste est également envisagée. On obtiendrait alors un double système probabiliste. L'avantage d'un tel double système probabiliste est bien entendu le fait qu'une probabilité plus « affinée » sera obtenue au final.

À titre d'exemple, deux systèmes de règles de détection ont été utilisés : des règles de détection syntaxiques des paquets TCP/SYN (tirées des règles de détection de l'outil p0f), et des règles de détection par expression régulière portant sur les en-têtes du protocole HTTP.

Lorsqu'une règle de détection valide un paquet observé, le module de prise d'empreinte M_E transmet (soit directement, soit sous la forme d'une création d'un enregistrement en base de données) une notification vers le module d'estimation de la probabilité M_P. Cette notification comprend un horodatage, l'identifiant de la machine source du paquet et l'identifiant de la règle de détection qui a été validée.

5.2.3 Estimation de la probabilité d'hébergement par le module d'estimation

L'estimation de la probabilité d'hébergement (i.e. d'un service ou d'un système donné sur un hôte donné) par le module d'estimation des probabilités (M_P)utilise la suite (ordonnée ou non) des notifications du module de prise d'empreinte M_E précédent pour fournir une estimation de la probabilité qu'un service soit présent sur un hôte.

Une des difficultés de cette estimation réside dans les contraintes suivantes :

- une règle de détection ne détecte pas toujours le même service, mais un ensemble (une classe) de services qui partagent certaines propriétés dans les paquets qu'ils transmettent (par exemple, les systèmes Linux avec un noyau 2.6) ;
- plusieurs services équivalents peuvent être hébergés simultanément au sein d'un hôte. Il peut s'agir de services compatibles (des navigateurs webs par exemple), ou incompatibles (des systèmes d'exploitations), les différents systèmes partageant la même adresse, par exemple par l'intermédiaire d'un système de translation d'adresse (NAT).

Il est donc nécessaire de proposer une méthode qui tienne compte de ces difficultés tout en réalisant un calcul probabiliste qui tienne compte de la réalité.

5.2.3.1 Modélisation mathématique

Soit donc une suite de notifications $N = \{n_i = (h, r, t)\}$. Ces notifications sont remontées par les sondes passives et contiennent l'information qu'une règle de détection r donnée à validé le trafic d'un hôte h à un instant t donné.

Par commodité, nous définissons les fonctions $h(n)$ et $r(n)$ fournissant respectivement l'hôte et la règle de détection relative à une notification n. Une séquence de notification vide (ne contenant aucune notification) est notée ε. Pour

une suite non vide de notification $N = n_0...n_k$, on note $N_0 = n_0$ son premier élément et $N_{1..k} = n_1...n_k$ la suite privée de son premier élément.

La probabilité qu'un hôte h héberge un service s est notée $P_h(s)$ et se calcule en fonction de la suite des notifications : $P_h(s) = P_h(s|N)$.

Intuitivement, l'événement *"le service est à l'origine d'une notification"* correspond à l'événement *"le service est à l'origine de la première, ou à l'une des suivantes"*. La probabilité se calcule récursivement de la manière suivante :

$$P_h(s|N) = \begin{cases} 0 & N = \varepsilon \\ P_h(s|N_0) + P_h(s|N_{1..k}) - P_h(s|N_0) \times P_h(s|N_{1..k}) & sinon \end{cases}$$

La probabilité $P_h(s|N_0)$ (c'est-à-dire la probabilité que le service soit à l'origine de la notification) ne dépend pas de l'hôte considéré *(h)* et peut donc s'exprimer plus simplement $P_h(s|n) = P(s|r)$, c'est à dire la probabilité qu'un service soit à l'origine du trafic validé par une règle de détection.

Cette probabilité est estimée dans une phase d'apprentissage préalable (décrite ci-après).

5.2.3.2 Mise en œuvre de la méthode de calcul de probabilité

La méthode de calcul de probabilité au sens de l'invention est mise en œuvre au sein d'un module spécifique de calcul de probabilité. Ce module utilise, en entrée, les notifications de la prise d'empreinte passive, une notification et notée *(h, r, t)* par la suite.

Avant de débuter les calculs, la liste des hôtes est actualisée ; si un hôte n'a pas encore été vu (c'est-à-dire qu'aucune probabilité n'a été calculé à son égard), le module de calcul de probabilité ajoute cet hôte dans la liste H des hôtes. La notification est ajoutée à la liste des traces A.

Pour estimer les probabilités, le module de calcul de probabilité effectue, dans ce mode de réalisation, les opérations suivantes :

1. Récupérer le nombre de validation de la règle de détection dans V (nombre qui est nommé v dans la suite).

2. Pour chaque compteur concernant la règle de détection r dans la liste C, effectuer les étapes suivantes :
   (a) Extraire le service concerné (nommé s dans la suite)
   (b) Extraire la valeur du compteur (nommé c par la suite)
   (c) Calculer le coefficient $p_s = \frac{c}{v}$, c'est-à-dire le rapport entre le nombre de validations de la règle de détection concernant ce service et le nombre de validations totale de la règle de détection.
   (d) Extraire l'ancienne probabilité $P_h(s)$ dans P, si elle n'existait pas encore, l'initialiser à 0 (nommé p_a par la suite)
   (e) Calculer la nouvelle probabilité résultante $p_r = p_a + p_s - p_a p_s$
   (f) Mettre à jour probabilité $P_h(s) = p_r$, et si p_r vaut 0, ne plus stocker cette probabilité.

Notons que le calcul de probabilité en se basant sur des valeurs de compteur est une approcha parmi d'autres pour calculer la probabilité. Dans d'autres modes de réalisation, la probabilité associée à un service ou à un système peut déjà être présente dans la base de données probabiliste sans qu'il soit nécessaire d'effectuer le calcul du ratio p_s.

5.2.3.3 Introduction d'un coefficient temporel

Afin de tenir compte du temps qui s'écoule entre les notifications de la prise d'empreinte (lorsque cet écoulement temporel a une signification), et donc d'obtenir un résultat qui a encore plus de sens, les inventeurs ont eu l'idée d'introduire deux caractéristiques complémentaires qui peuvent ou non être combinées.

La première caractéristique est l'insertion d'un ordonnancement dans la prise d'empreinte. Plus particulièrement, les notifications sont ordonnancées afin de tenir compte de la survenance réelle des évènements (paquets, traces) qui ont déclenché les notifications.

Selon une deuxième caractéristique, qui peut être couplée à l'ordonnancement, le calcul tient compte de l'ordonnancement.

L'idée générale est la suivante : l'inventaire n'est pas figé. À tout moment, des machines démarrent, s'arrêtent et les systèmes présents derrière une adresse peuvent changer (changement d'attribution des adresses via DHCP ou dual boot). Le procédé est alors amélioré pour pouvoir "oublier" ses précédentes déductions.

Concrètement, la formule de calcul de probabilité est modifiée de la manière suivante :

$$p_r = c^{dt}.p_a \times (1 - p_s) + p_s$$

c^{dt} signifie "*c exposant dt*" où *dt* est le temps écoulé entre la précédente mise à jour et la mise à jour courante (en secondes) et *c* est un coefficient. Le coefficient est adapté en fonction des besoins. Quand le coefficient *« c »* vaut "1", le système n'oublie rien. Quand il vaut 0, il oublie tout. Plus on va de 0 à 1, plus on garde en mémoire des vieux événements et donc plus les probabilités « anciennes » conservent de la valeur.

Dans les systèmes très dynamiques (c'est-à-dire dans les systèmes ou le parc évolue vite), le coefficient *c* peut être proche de 0, puisque dans ce cas, les anciennes prévisions n'ont pas forcément de sens.

Dans ce cas, l'ordonnancement des traces et leur horodatage prend tout son sens. Il faut également stocker, dans la mémoire, le moment où les résultats stockés ont été calculés.

Dans un autre mode de réalisation, il est également possible d'affecter un coefficient *c* aux anciennes probabilités, sans qu'il soit conditionné à un temps écoulé entre la précédente mise à jour et la mise à jour courante. Dans ce cas la formule ne tient pas compte du temps.

5.2.3.4 Exemple numérique d'application

Pour cet exemple, nous considérons deux règles de détection (r_1, r_2) qui permettent de détecter chacune deux systèmes, dont l'un est en commun (soit au total trois systèmes s_1, s_2 et s_c– *système commun*). Le tableau 1 donne les probabilités de détection de ces deux règles de détection pour les trois systèmes.

$P(s\|r)$	s_1	s_2	s_c
r_1	½	0	½
r_2	0	½	½

Tableau 1

Si les deux règles de détection génèrent des notifications pour un hôte *h* donné, l'estimation des probabilités engendre une probabilité plus grande pour le système en commun s_c. Le tableau 2 montre un exemple de progression des probabilités associées aux trois services pour une suite arbitraire de notifications.

règle de détection	s_1	s_2	s_c
r_1	50%	0	50%
r_2	50%	50%	75%
r_1	75%	50%	87%
r_1	87%	50%	94%
r_2	87%	75%	97%
r_2	87%	87%	98%
r_2	87%	93%	98%

Tableau 2

Plus les notifications sont nombreuses, plus les probabilités augmentent asymptotiquement vers 1, mais le système commun aux deux règles de détection conserve une probabilité supérieure aux deux autres (il converge plus vite). De ce tableau on déduit que, dans la mesure où les deux règles de détection permettent de qualifier deux systèmes, la reconnaissance, pour un hôte *h* donné, d'une activation tantôt de la règle de détectionr_1 et tantôt de la règle de détectionr_2 fait plutôt pencher la balance en faveur du système commun. La méthode de

l'invention permet ainsi de corroborer un résultat que l'on pourrait qualifier d'intuitif.

Notons qu'il n'est pas assuré que le système commun s_c soit effectivement le système à l'origine des notifications. Il se pourrait fort bien qu'en définitive ce soit le système $s_1$ou le système s_2 qui soit à l'origine des notifications. En effet, dans la mesure où ce sont bien des *probabilités* de détection qui servent de point de départ au calcul. Ainsi, par exemple, au regard des résultats du tableau 2, il y a à l'issu du calcul, 2% de chance que ce ne soit pas le système s_c qui soit à l'origine des notifications.

5.2.4 Apprentissage des paramètres

L'apprentissage permet d'estimer le coefficient p_s mentionné dans la section précédente via le calcul des compteurs. L'apprentissage prend en entrée une trace *(A)* de détection, et un inventaire explicite (fournis par un expert par exemple), sous la forme d'une table d'association entre les services et les hôtes *(*$I \subset H \times S$*)*.

Une première étape facultative d'initialisation peut être effectuée. Cette phase consiste à remettre l'ensemble des compteurs à 0. Lorsque cette étape n'est pas effectuée, les phases d'apprentissages consécutives se cumulent.

Ensuite, et pour chaque notification *(h, r, t)* dans la liste de notifications, l'apprentissage effectue les opérations suivantes :

1. Extraire de l'inventaire *I*, toutes les associations concernant l'hôte *h*. Pour chaque association *(h, s)*, effectuer les étapes suivantes :
   (a) Ajouter 1 au compteur *C* pour la règle de détection *r* et le service *s* ;
   (b) Ajouter 1 au compteur *V* pour la règle de détection *r*.

5.3 Apport de ce mode de réalisation

Le calcul des probabilités fournies par ce mode de réalisation permet de mieux qualifier l'existence ou non d'un service derrière un hôte particulier. En effet, les systèmes actuels ne proposent que deux possibilités : proposer plusieurs

résultats plus ou moins contradictoires sans possibilité pour l'utilisateur de trancher, ou choisir arbitrairement le système ayant la meilleure note.

Comme cela a été démontré dans l'exemple numérique, la méthode décrite est capable de quantifier la présence d'un système, et lorsque plusieurs solutions sont possibles, elle permet de les classer de la plus probable à la moins probable.

La probabilité fournie a un réel sens mathématique : elle quantifie la probabilité, au vu des observations, que le système concerné soit présent sur l'hôte. De faibles probabilités indiquent que le service a peu de chance d'être présent, mais qu'il peut être à l'origine de certaines observations réseaux. Une grande probabilité indique, à l'opposé, que le service à de grande chance d'être présent.

L'utilisation d'un cadre probabiliste permet également d'utiliser des règles de détection pour la prise d'empreinte très différentes dans leur nature et de corréler leurs résultats de manière homogène. Chaque règle de détection validée apportant de nouvelles connaissances sur le réseau surveillé et augmentant d'autant la précision de l'outil.

Cette augmentation s'est montrée significative lors de tests. En plus d'améliorer la précision générale de la méthode de l'invention, la phase d'apprentissage permet aussi d'améliorer la précision et la pertinence des règles de détection de la base. En effet, la base de données des règles de détection de p0f contient nombre d'erreurs (par exemple, des règles de détection sont référencées comme détectant les systèmes de la famille Windows Vista alors qu'elles détectent les systèmes de la famille XP). Sans apprentissage, l'outil est susceptible de détecter des systèmes erronés. Une fois la phase d'apprentissage effectuée, la base de connaissance se corrige et les détections sont, par voie de conséquence, plus précises.

5.4 Autres caractéristiques optionnelles et avantages

On présente, en relation avec la figure 2, un mode de réalisation d'un dispositif de d'inventaire au sens de l'invention.

Ce dernier comprend une mémoire M 21, une unité de traitement 22, équipée par exemple d'un microprocesseur, et pilotée par le programme d'ordinateur Pg 23. À l'initialisation, les instructions de code du programme d'ordinateur 23 sont par exemple chargées dans une mémoire RAM avant d'être exécutées par le processeur de l'unité de traitement 22. L'unité de traitement 22 reçoit en entrée les données 24 émises par les différents hôtes du réseau au sein duquel il faut réaliser l'inventaire (il s'agit par exemple de paquets TCP, IP ou d'entêtes HTTP). Le microprocesseur μP de l'unité de traitement 22 réalise une ou plusieurs empreintes passives de ces données 24, selon les instructions du programme Pg 23. L'unité de traitement 22 délivre en sortie des probabilités 25 (par exemple des listes de probabilités associées à différents services/systèmes), destinés à permettre de réaliser un inventaire du réseau.

REVENDICATIONS

1. Procédé d'inventaire d'un réseau de communication, ledit réseau comprenant au moins un hôte *h* échangeant des données avec d'autres équipements dudit réseau, ledit procédé comprenant les phases suivantes :

- une phase d'obtention d'au moins une empreinte *E* associée audit hôte *h,* ladite au moins une empreinte *E* comprenant au moins une notification de détection représentative d'au moins une activation d'au moins une règle de détection *r* par au moins un élément échangé sur ledit réseau et associé audit hôte *h* ;
- une phase d'obtention, à partir de ladite au moins une empreinte *E*, d'au moins une probabilité *p* de présence d'au moins un service *s* au sein dudit hôte *h*, à partir d'au moins une base de données probabiliste associant ladite au moins une règle de détection *r* à au moins une probabilité prédéterminée.

2. Procédé d'inventaire selon la revendication 1, caractérisé en ce qu'il comprend en outre une phase préalable d'apprentissage comprenant une étape de remplissage de ladite base de données probabiliste à l'aide d'un réseau de communication comprenant des équipements connus.

3. Procédé d'inventaire selon la revendication 1, caractérisé en ce que ladite phase d'obtention de ladite au moins une empreinte *E* dudit hôte *h* comprend au moins une itération des étapes suivantes :

- réception d'un élément en provenance dudit réseau de communication et associée audit hôte *h* ;
- application, audit élément, d'au moins une règle de détection *r* parmi une base de données de règles de détection *R,* délivrant une notification de détection *;*

- sauvegarde, au sein d'une liste de notification de prise d'empreinte *A*, de ladite notification de détection lorsque ladite notification de détection est au moins partiellement positive, ladite liste de notification de prise d'empreinte *A* représentant ladite empreint *E*.

4. Procédé d'inventaire selon la revendication 3, caractérisé en ce que ladite notification de détection délivrée lors de ladite application de ladite au moins une règle de détection délivre un résultat binaire.

5. Procédé d'inventaire selon la revendication 3, caractérisé en ce que ladite notification de détection délivrée lors de ladite application de ladite au moins une règle de détection délivre un résultat probabiliste.

6. Procédé d'inventaire selon la revendication 1, caractérisé en ce que ladite phase d'obtention d'au moins une probabilité p de présence d'au moins un service s au sein dudit hôte h comprend, pour chaque notification de ladite empreinte de détection E :

- une étape d'obtention, à partir de ladite au moins une base de données probabiliste, d'au moins une probabilité p_s associée à ladite notification ;
- une étape de calcul d'une probabilité résultante p_r telle que :

$$p_r = p_a + p_s - p_a p_s$$

dans laquelle p_a désigne une probabilité antérieure associée dans une itération préalable ou 0 lorsque qu'aucune itération préalable n'a été mise en œuvre ;

- une étape de sauvegarde de ladite probabilité résultante p_r.

7. Procédé d'inventaire selon la revendication 6, caractérisé en ce que, lors du calcul de ladite probabilité résultante p_r, ladite probabilité antérieure p_a est affecté d'un coefficient c^{dt} dont la valeur est fonction du temps écoulé entre lesdites notifications de ladite empreinte de détection et/ou d'un

coefficient ayant une valeur prédéterminée.

8. Dispositif d'inventaire d'un réseau de communication, ledit réseau comprenant au moins un hôte *h* échangeant des données avec d'autres équipements dudit réseau, ledit dispositif comprenant :

- des moyens d'obtention d'au moins une empreinte *E* associée audit hôte *h,* ladite au moins une empreinte *E* comprenant au moins une notification de détection représentative d'au moins une activation d'au moins une règle de détection *r* par au moins un élément échangé sur ledit réseau et associé audit hôte *h* ;
- des moyens d'obtention, à partir de ladite au moins une empreinte *E*, d'au moins une probabilité *p* de présence d'au moins un service *s* au sein dudit hôte *h*, à partir d'au moins une base de données probabiliste associant ladite au moins une règle de détection *r* à au moins une probabilité.

9. Produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution du procédé de d'inventaire selon l'une au moins des revendications 1 à 7, lorsqu'il est exécuté sur un ordinateur.

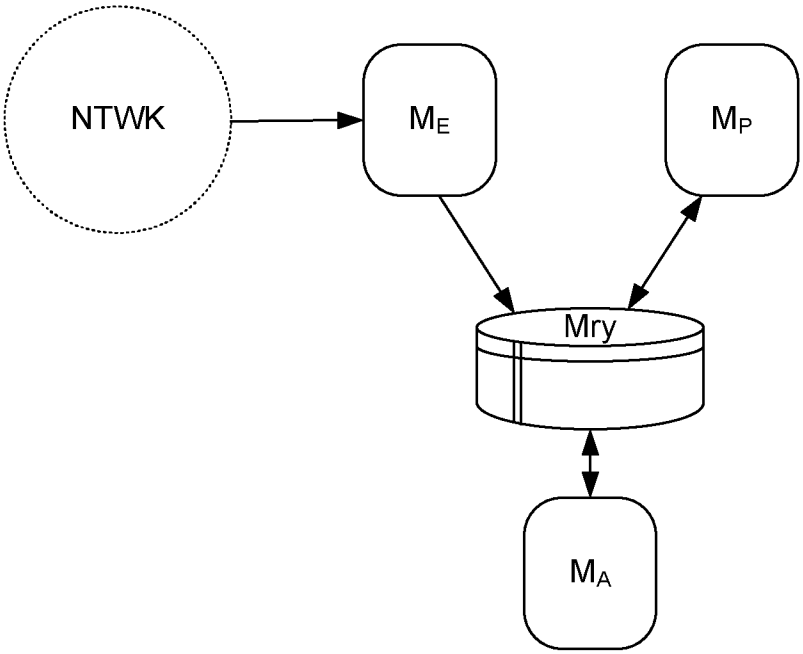

Figure 1

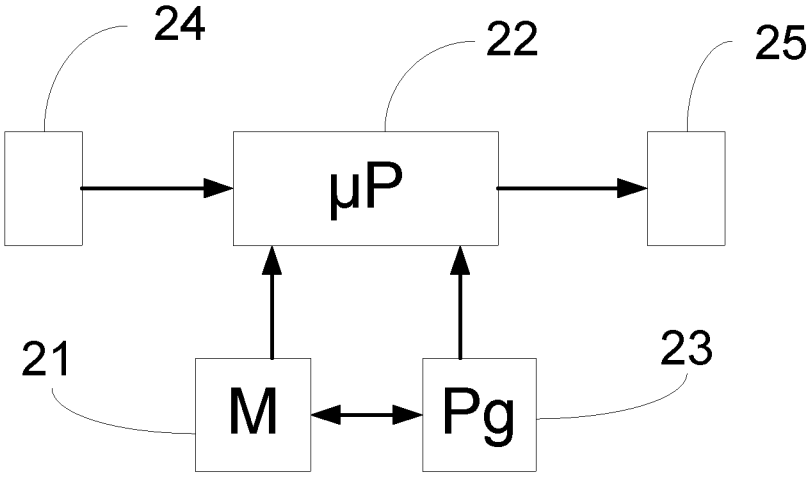

Figure 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/052691

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/24 H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/314143 A1 (VOGEL III WILLIAM ANDREW [US] ET AL) 22 December 2011 (2011-12-22) paragraphs [0002], [0004] paragraphs [0055], [0058] paragraphs [0082] - [0101] figures 1-8	1-9
X	US 7 519 954 B1 (BEDDOE MARSHALL [US] ET AL) 14 April 2009 (2009-04-14) column 11, line 52 - column 12, line 26 column 15, lines 29-61	1-9
X	US 2003/200304 A1 (THORPE JOHN ROBERT [US] ET AL) 23 October 2003 (2003-10-23) paragraphs [0085] - [0131] page 1; figures 1-19C	1-9

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 April 2013	10/05/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Ghomrasseni, Z

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/052691

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/182864 A1 (KHAN FAUD [CA] ET AL) 16 July 2009 (2009-07-16) paragraphs [0043] - [0070] figures 1-7	1-9
A	US 2009/037353 A1 (GREENWALD LLOYD G [US] ET AL) 5 February 2009 (2009-02-05) paragraphs [0022], [0027] - [0050], [0062]	1-9

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/052691

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011314143 A1	22-12-2011	CA 2795847 A1	29-12-2011
		EP 2585912 A1	01-05-2013
		US 2011314143 A1	22-12-2011
		WO 2011162879 A1	29-12-2011
US 7519954 B1	14-04-2009	NONE	
US 2003200304 A1	23-10-2003	US 2003200304 A1	23-10-2003
		US 2006248187 A1	02-11-2006
US 2009182864 A1	16-07-2009	US 2009182864 A1	16-07-2009
		WO 2009093226 A2	30-07-2009
US 2009037353 A1	05-02-2009	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2013/052691

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L12/24 H04L29/06
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2011/314143 A1 (VOGEL III WILLIAM ANDREW [US] ET AL) 22 décembre 2011 (2011-12-22) alinéas [0002], [0004] alinéas [0055], [0058] alinéas [0082] - [0101] figures 1-8	1-9
X	US 7 519 954 B1 (BEDDOE MARSHALL [US] ET AL) 14 avril 2009 (2009-04-14) colonne 11, ligne 52 - colonne 12, ligne 26 colonne 15, ligne 29-61	1-9
X	US 2003/200304 A1 (THORPE JOHN ROBERT [US] ET AL) 23 octobre 2003 (2003-10-23) alinéas [0085] - [0131] page 1; figures 1-19C	1-9

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
29 avril 2013	10/05/2013

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Ghomrasseni, Z

1

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2009/182864 A1 (KHAN FAUD [CA] ET AL) 16 juillet 2009 (2009-07-16) alinéas [0043] - [0070] figures 1-7	1-9
A	US 2009/037353 A1 (GREENWALD LLOYD G [US] ET AL) 5 février 2009 (2009-02-05) alinéas [0022], [0027] - [0050], [0062]	1-9

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2013/052691

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2011314143 A1	22-12-2011	CA 2795847 A1	29-12-2011
		EP 2585912 A1	01-05-2013
		US 2011314143 A1	22-12-2011
		WO 2011162879 A1	29-12-2011
US 7519954 B1	14-04-2009	AUCUN	
US 2003200304 A1	23-10-2003	US 2003200304 A1	23-10-2003
		US 2006248187 A1	02-11-2006
US 2009182864 A1	16-07-2009	US 2009182864 A1	16-07-2009
		WO 2009093226 A2	30-07-2009
US 2009037353 A1	05-02-2009	AUCUN	