ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) BREVET D'INVENTION

(11) N° de publication :
MA 38593 B1

(43) Date de publication :
30.04.2018

(51) Cl. internationale :
G06F 21/00; G06F 21/22; H04L 29/06; G06F 7/04; G06F 21/24

(21) N° Dépôt :
38593

(22) Date de Dépôt :
16.11.2015

(71) Demandeur(s) :
UNIVERSITE MOHAMMED V, Angle avenue Allal El Fassi et Mfadel Cherkaoui, Al Irfane 8007.N.U, Rabat Rabat-Chellah (MA)

(72) Inventeur(s) :
DIOURI OUAFAE ; BEN MESSAOUD EL HIOUSSAIN

(74) Mandataire :
FATIMA ZAOUI

(54) Titre : **SYSTEME AUTO-ADAPTATIF DE REGULATION DYNAMIQUE DE LA SECURITE APPLICATIVE DES SYSTEMES A BASE DE WEB SERVICES**

(57) Abrégé : La présente invention concerne un Système auto-adaptatif de régulation dynamique de la sécurité applicative des systèmes à base de Web services. Ce système est caractérisé par: • Une protection dynamique et intelligente contre les nouvelles menaces qui peuvent affecter un système d'information à base de Web service, à travers un moteur intelligent (E) permettant d'adapter et rehausser les exigences de la politique de sécurité (PS) d'un fournisseur de service de manière automatique et de la déployer auprès des clients/partenaires de manière dynamique. • Capacité d'apprentissage au fil du temps pour capitaliser sur les attaques précédentes afin de fournir de nouvelles réponses à des menaces non inconnues auparavant et ce de manière autonome. • Faculté d'isoler le système à protéger en cas d'incapacité à trouver et déduire une solution optimale et ce après qualification de la gravité de l'attaque afin d'éviter la contre-productivité (ex: fausse alerte). Ceci permet de diminuer la portée des dommages pour une attaque inévitable.

ABREGE

La présente invention concerne un **Système auto-adaptatif de régulation dynamique de la sécurité applicative des systèmes à base de Web services.**

Ce système est caractérisé par :

- Une protection dynamique et intelligente contre les nouvelles menaces qui peuvent affecter un système d'information à base de Web service, à travers un moteur intelligent (E) permettant d'adapter et rehausser les exigences de la politique de sécurité (PS) d'un fournisseur de service de manière automatique et de la déployer auprès des clients/partenaires de manière dynamique.
- Capacité d'apprentissage au fil du temps pour capitaliser sur les attaques précédentes afin de fournir de nouvelles réponses à des menaces non inconnues auparavant et ce de manière autonome.
- Faculté d'isoler le système à protéger en cas d'incapacité à trouver et déduire une solution optimale et ce après qualification de la gravité de l'attaque afin d'éviter la contre-productivité (ex : fausse alerte). Ceci permet de diminuer la portée des dommages pour une attaque inévitable.

Titre: Système auto-adaptatif de régulation dynamique de la sécurité applicative des systèmes à base de Web services

DESCRIPTION

La sécurité des systèmes information connectés est devenue une préoccupation opérationnelle généralisée. Les services de sécurité de pointe et les relations de confiance sont actuellement les caractéristiques les plus recherchées de ces systèmes.

Le besoin croissant d'échanges d'informations sécurisées au sein de l'entreprise et au-delà de ses frontières, la création de nouveaux espaces reposant sur la collaboration entre partenaires internationaux, la mutation vers une économie numérique généralisée... autant de préoccupations qui ont transformé la sécurité de l'information en un enjeu stratégique.

Seulement et de manière parallèle, les dangers entourant cette transformation se développent à rythme soutenu notamment sur le volet sécurité.

La prise de conscience en matière de sécurité amène toute entreprise, à décrire les axes à suivre dans un document de contrôle appelé politique de sécurité, recueillant la nature des objectifs de sécurité à garantir ou à atteindre. La mise en œuvre de la politique de sécurité doit permettre de répondre aux besoins d'intégrité, de disponibilité, de confidentialité, et de traçabilité, qui forment en plus des concepts de gestion des identités et des accès, un moyen de protéger les systèmes d'information des organisations en garantissant les objectifs de sécurité. Notre invention concerne le domaine de la **sécurité informatique des systèmes à base de Web services.**

ETAT DE LA TECHNIQUE ANTERIEURE

Les politiques de sécurité statiques pour les web services, ne sont clairement plus adaptées pour gérer le risque lié aux ressources critiques dans les systèmes d'information d'aujourd'hui. Il faut réaliser une personnalisation précise pour garantir une protection complète en fonction des vulnérabilités présentes. Même cela n'est pas suffisant dans le temps, car nous ne sommes alors protégés que pour une période donnée, et ce jusqu'à ce qu'un changement intervienne dans le système (nouvelle attaque, nouvelles vulnérabilités découvertes...). Il faut donc « tunner » et optimiser sa politique de sécurité et sa configuration technique résultante, continuellement pour conserver un niveau de sécurité acceptable et maintenu.

Jusqu'à présent les procédés de sécurisation des web services actuels offrent uniquement :

- **Une sécurité statique dans le temps apportant une protection limitée aux menaces connues d'avance.**
- **Manque de capacité de prise de décision (intelligence) intrinsèque au service Web, afin de cantonner une nouvelle attaque ou déclencher une réaction adaptée à celle-ci de manière autonome.**
- **Nécessité d'intervention manuelle pour ajuster la politique de sécurité et gérer son redéploiement.**

DESCRIPTION DU PROCEDE

La présente invention introduit la notion de sécurité adaptative capable de protéger un système d'information à base de Webservice continuellement dans le temps. En effet, Les mécanismes de sécurité conventionnels offrent une détection parfois tardive des menaces — quand celles-ci ne passent pas carrément inaperçues — et un délai de résolution relativement long. Le concept que nous introduisons repose sur le fait d'au lieu de tenter de prévenir la moindre attaque, nous proposons plutôt de mettre en œuvre un modèle adaptatif capable de réagir par de nouvelles mesures de protection suite à la confirmation d'une attaque sur le systéme Web service à sécuriser. Nous proposons en effet, un mécanisme ayant un double objectif : celui de détecter rapidement les attaques, de les catégoriser et d'y répondre de façon vigoureuse, rapide et efficace et surtout automatique afin d'éviter des conséquences néfastes.

Or, face aux menaces multiples et rapides de nos jours, l'objectif étant de renforcer la détection et réduire le délai de correction. Pour cela les entreprises doivent pouvoir s'adapter à l'évolution des techniques utilisées par les cybercriminels. Elles doivent pouvoir compter sur une architecture de sécurité à la fois agile et intelligente. Cette architecture doit également pouvoir être capable d'anticiper les attaques, de manière proactive, et non se contenter de les examiner après-coup. Il est aussi important de répondre rapidement et efficacement aux attaques que de les bloquer.

En réponse aux limitations indiquées dans la section « Etat de la technique antérieure». La présente invention permet de fournir un degré plus élevé de protection continue dans le temps, grâce à :

- Un mécanisme de réponse **automatisée et intrinsèque** (E) face aux vulnérabilités d'une application Web service pas forcément connues à l'avance
- La possibilité de maintenir un haut degré de sécurité Web en se basant sur la **capacité d'apprentissage artificiel** qui capitalise la connaissance et l'expérience du système au fil du temps de manière automatique

En effet, le système doit pouvoir à la publication/détection d'une nouvelle vulnérabilité (D), renforcer les exigences de sécurité de manière **autonome** (sans intervention humaine) afin de la contrer (E). Le système doit également d'historier et tracer tous les événements nouveaux sur l'architecture (K) en vue de les utiliser pour **l'apprentissage** et la **prédiction** de nouvelles solutions à de nouvelles menaces (E).

La valeur ajoutée de l'invention, concerne la capacité à adapter la politique de sécurité du web service à protéger de manière autonome et dynamique, suite à l'identification d'une menace nouvelle inconnue auparavant.

DESCRIPTION TECHNIQUE

COMPOSANTES DE LA SOLUTION

Notre système se décompose en trois modules. Nous distinguons un module responsable de s'interfacer avec les scanners appelé module de détection (D), un module intelligent (E) qui permet d'interpréter les notifications générées à travers le module (D) et d'y associer les traitements correspondants, et une base

de connaissances (K) d'où le module intelligent (E) puise la savoir nécessaire pour prendre la décision adéquate. Le module intelligent (E) comporte une unité d'apprentissage (Ea) capable de déduire et d'injecter automatiquement de nouvelles solutions, une unité (Eu) qui permet d'appliquer les recommandations de la solution d'une attaque donnée par la mise à jour de la politique de sécurité encours d'exécution dynamiquement et finalement une unité (Q) de qualification et de gestion de la réputation afin d'éviter de bloquer le Web services pour de fausses attaques, dont le degré de gravité ne justifie pas l'isolation :

Détection proactive (D)

Le système propose la détection de menace par analyse probabiliste de **ressemblances avec des attaques déjà catégorisées dans la base de connaissance combinée avec les scanners web du marché**. Cette composante permet la traduction d'une alerte en fait (existant ou nouveau) dans la base de connaissance (K).

Base de connaissance (K)

Une composante de base de connaissance qui concentre la savoir autours des nouvelles menaces mais également intègre les solutions adaptées.

Il s'agit d'un Système de veille capable de stocker, traiter et mettre à une base de données des vulnérabilités et des solutions possibles.

Moteur de Réaction (E)

Le système fournit la capacité de choisir la meilleure mesure parmi celles possibles pour palier à la menace détectée. En se basant sur son moteur de règles intrinsèque et sur la base de connaissance (K).

En cas d'absence de mesure corrective, le système doit lancer un processus de **Contention de l'attaque** afin de limiter les dégâts et ce après consultation de l'unité (Q)

Le module (E) se compose en plus de trois unités :

- **Unité Ea :** Unité d'apprentissage (Ea) capable de déduire et d'injecter automatiquement de nouvelles solutions à la suite de la capitalisation sur l'historique de traitement du système. Cette unité permet de produire et d'enrichir le système de base de connaissance (K) de manière automatique sans intervention manuelle.
- **Unité Eu :** Unité d'update qui permet d'appliquer les recommandations de la solution d'une attaque donnée, puisée dans la base de connaissance (K) et ce par la mise à jour de la politique de sécurité en cours d'exécution dynamiquement et d'en informer les clients du Web service à protéger.
- **Unité de qualification (Q) :** Module (Q) de qualification et de gestion de réputation (scoring) permettant la qualification des comportements douteux afin d'éviter les faux positifs et réduire les actions d'isolation sur fasses alertes.

DESCRIPTION FONCTIONNELLE

Le système proposé correspond à **une architecture auto-adaptable et intelligente, dépassant la protection périmétrique statique par la capacité de contrer dynamiquement avec de nouvelles menaces, à travers la possibilité de prise de décision autonome, afin de rehausser le niveau d'exigence de la politique de sécurité** en cours d'exécution du web service. Celle-ci pouvant ne pas tenir compte des nouvelles menaces arrivantes.

Le systéme agit essentiellement au niveau des **politiques de sécurité** des Web service exprimés (mais pas uniquement) grâce aux standards WS-Policy et WS-SecurityPolicy qui permettent d'exprimer des politiques de sécurité au niveau des messages échangés entre services, c'est-à-dire servent à spécifier quelles accréditations doivent accompagner le message, et quel mécanisme de protection des données doit être mis en œuvre dans les messages. Tous les besoins de sécurité du serveur sont couverts par les "obligations minimales" définies à l'intérieur de la politique de sécurité.

ALGORITHME DE FONCTIONNEMENT DU SYSTEME :

Le système auto-adaptatif (voir **figure 1**), initie son module de détection (D) qui supervise régulièrement le système à protéger et notifie le module intelligent (E) en cas de comportement douteux. A la détection d'une menace, le module intelligent (E) consulte la base de données des connaissances (K) pour vérifier l'existence ou non d'une solution de protection possible. Si c'est le cas, celle-ci est appliquée grâce à unité (Eu) en mettant à jour la politique de sécurité en cours d'exécution dynamiquement et lançant le processus de son redéploiement. Dans le cas contraire, le moteur intelligent (E) demande à l'unité d'apprentissage et de raisonnement (Ea) de lui proposer une solution possible et optimale à la menace en cours en lui transmettant sa description ainsi que l'ensemble du contexte et des indicateurs qui l'entourent. Celle-ci se basant sur l'historique de la connaissance et l'expérience des attaques précédentes, essaye de catégoriser cette menace et d'en déduire une solution adéquate. Si le résultat de cette unité est positif (solution produite), celle-ci est insérée dans la base de connaissance pour une réutilisation ultérieure, puis transmise à l'unité (Eu) pour mettre à jour la politique de sécurité de manière dynamique en conséquence. Si l'unité (Ea) échoue à produire une solution à cette nouvelle menace, le moteur (E) va consulter l'unité de qualification et de gestion de la réputation (Q) pour statuer sur le degré de danger représenté par cette menace et s'il mérite d'isoler le système en vue de limiter les dégâts éventuels. Ce mécanisme permet de se prémunir contre la détérioration de la productivité du système à protéger sur fausses alertes. Si l'isolation du système est décidée par le moteur (E), ceci déclenchera en parallèle la notification d'un administrateur système sur ce fait.

EXPOSE DU MODE DE REALISATION

Une implémentation possible de ce système, peut être faite grâce à l'utilisation des briques suivantes :

- **Tripwire :** un logiciel permettant de s'assurer que les fichiers sensibles sur un ordinateur ne sont pas modifiés sans que cela ne déclenche une alerte
- **Le langage AVDL :** le langage AVDL (Application Vulnerability Description Language) fournit un mécanisme pour importer les résultats d'un test de pénétration de l'application directement dans une passerelle de contrôle des transactions Web
- **Moteur de règles Drools** (www.drools.org) : (ou JBoss Rules) est un logiciel gérant les règles utilisant un raisonnement déductif se basant sur des prémisses définies par l'utilisateur. C'est un système capable de définir des règles et de les appliquer à des faits.

APPLICATIONS INDUSTRIELLES

Le procédé objet du brevet permet d'offrir, entre autres, les avantages suivants :

- Sécurité accrue et maintenu dans le temps pour les systèmes critiques à base de Web services
- Capacité de réduire ou atténuer les effets néfastes d'une attaque informatique
- Possibilité d'isolation du système infecté en cas de non disponibilité de réponse efficace.
- Meilleure confiance dans les architectures Webservice et réduction de la charge de travail des administrateurs système et de sécurité de SI.

L'invention objet de la présente, est susceptible d'applications industrielles dans les domaines suivants (parmi d'autres), cette liste n'est pas exhaustive :

- Le e-gouvernement : tous les services e-gov à base de WS sont concernés, surtout là ou ilya des données sensibles à échanger
- Applications militaires et sensibles
- Les échanges Webservices commerciaux faisant appel à des données stratégiques ou des montants importants

REVENDICATIONS D'INNOVATION

Les revendications portent sur :

1. **Système de sécurité informatique, applicative, auto-adaptative, intelligent, et autonome pour les Web services, caractérisé en ce qu'il comprend au moins un moyen (K) de consolidation de la connaissance et des règles de sécurité et de la gestion de leur éditions, un moyen (D) de détection permettant de s'interfacer et agréger plusieurs types de détecteurs d'intrusions et de vulnérabilités, un moteur intelligent de régulation dynamique de la sécurité applicative (E) capable d'orchestrer, de raisonner, de sélectionner et de prendre des décisions de mise à jour de la politique de sécurité, de manière dynamique, en gérant son déploiement et ce de manière automatique.**

2. **Système conforme à la revendication 1, dans lequel le moteur intelligent de régulation dynamique de la sécurité applicative (E), comprend un moyen de sélection des règles adéquates à appliquer et/ou une unité d'apprentissage (Ea) pour déduire et injecter de nouvelles règles de sécurité, par raisonnement artificiel, de manière automatique, et/ou un moyen d'intégrer automatiquement les nouvelles solutions produite par l'unité d'apprentissage (Ea), à la base de connaissance (K) pour les utiliser dans le traitement des nouvelles attaques non répertoriées, et/ou un moyen (Eu) de mise à jour de la politique de sécurité en cours d'exécution, dynamiquement, en temps réel et la gestion de son déploiement automatique.**

3. **Moyen conforme à la revendication 2 comportant un moyen de qualification et de gestion de la réputation (Q) des comportements douteux et de la gestion de la réputation de ces comportements (scoring)**

4. **Système conforme à la revendication 1, 2 et 3, dans lequel une opération d'isolation du Web service attaqué, est déclenchée en cas d'absence de mesure adéquate identifiée par le moteur intelligent de régulation dynamique de la sécurité applicative (E) et ce après consultation automatique du moyen de qualification et de gestion de la réputation (revendication 3), afin d'éviter les fausse alertes et réduire ainsi les actions d'isolation inutiles. La notification des administrateurs est également déclenchée en cas d'isolation.**

DESSIN

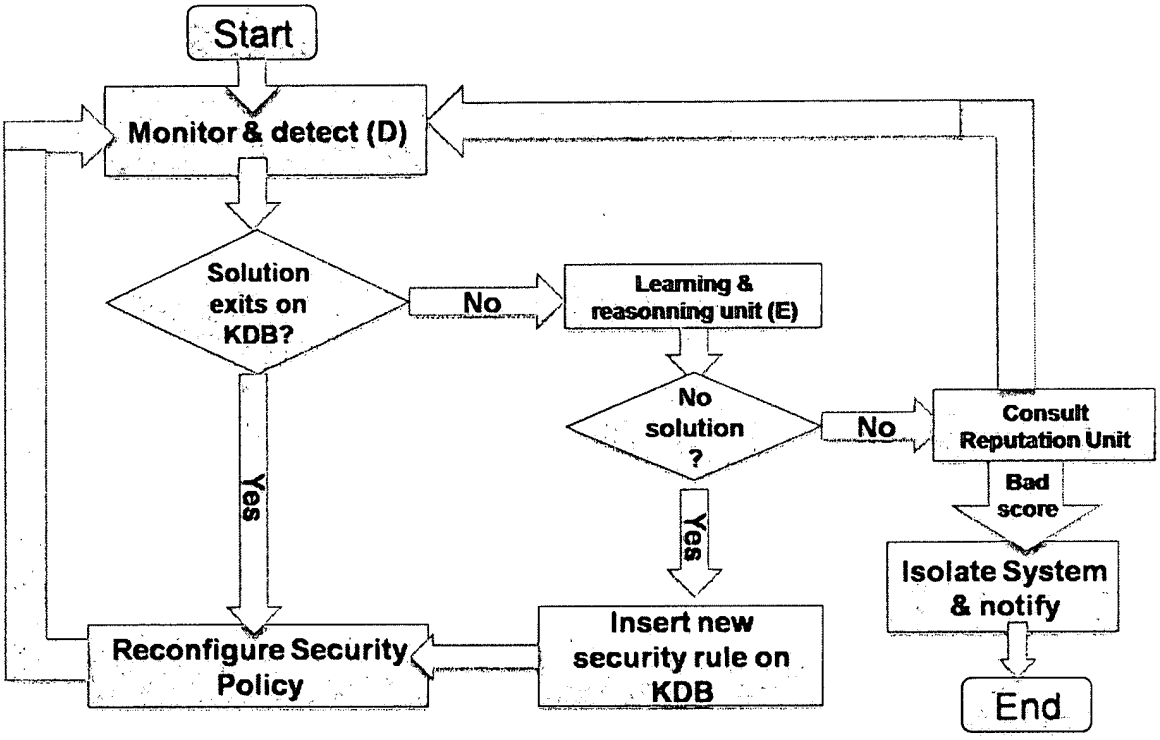

Figure 1 – Algorithme de fonctionnement du Système auto-adaptatif de régulation dynamique de la sécurité applicative des systèmes à base de Web services

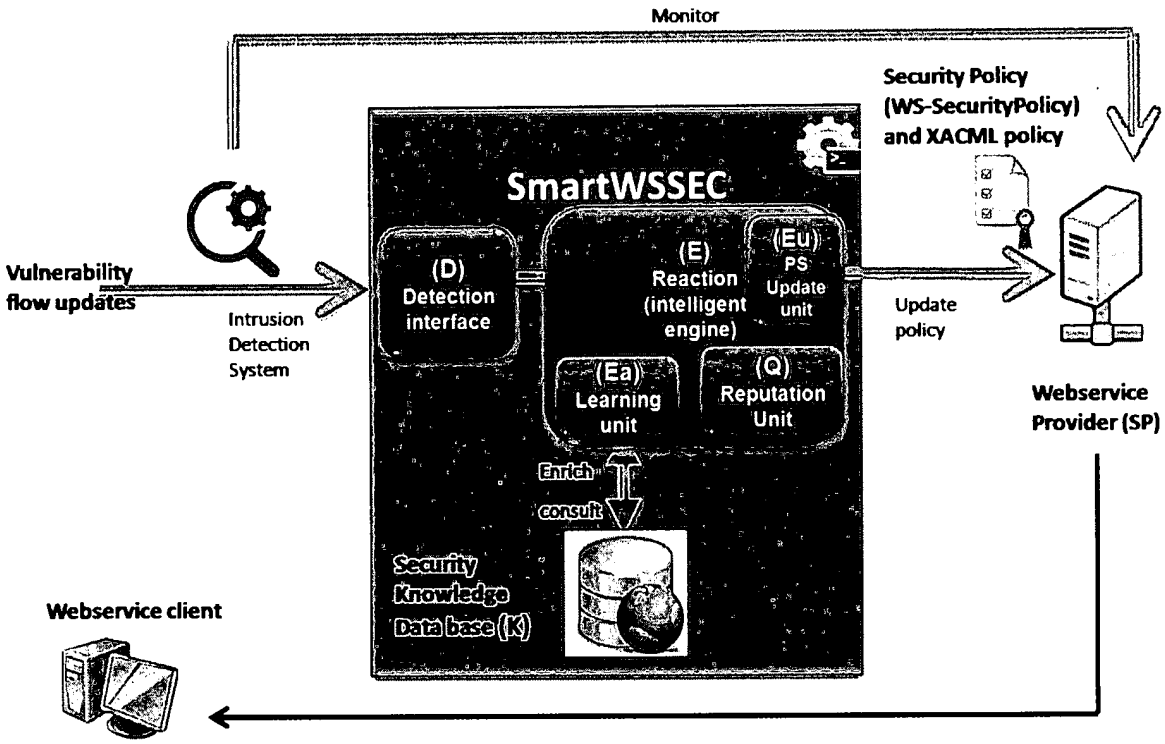

Figure 2 – Composantes du Système auto-adaptatif de régulation dynamique de la sécurité applicative des systèmes à base de Web services

MA 38593B1

ROYAUME DU MAROC
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE

OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle)

Renseignements relatifs à la demande	
N° de la demande : 38593	Date de dépôt : 16/11/2015
Déposant : UNIVERSITÉ MOHAMMED V DE RABAT	
Intitulé de l'invention : SYSTEME AUTO-ADAPTIF DE REGULATION DYNAMIQUE DE LA SECURITE APPLICATIVE DES SYSTEMES A BASE DE WEB SERVICES	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents cités par l'examinateur dans la partie rapport de recherche sont joints au présent document

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☐ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☐ Cadre 4 : Remarques de clarté
- ☒ Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle
- ☐ Cadre 6 : Observations à propos de certaines revendications dont aucune recherche significative n'a pu être effectuée
- ☐ Cadre 7 : Défaut d'unité d'invention

Examinateur: F.Belafkih
Téléphone: **+(212) 5 22 58 64 14/00**
Email : **fbelafkih@ompic.ma**

Date d'établissement du rapport : 27/11/2015

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  5 Pages
- Revendications
  4
- Planches de dessin
  2 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : G06F21/24, G06F21/22, G06F7/04, G06F21/00, H04L29/06
CPC : H04L63/12, H04L63/1433, G06F21/577

Bases de données électroniques consultées au cours de la recherche :

EPOQUE, Orbit

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
X	**US7000247 B2 ; Citadel Security Software, Inc. ; 14 Février 2006** Tout le Document	1-2
A	**US 20100082803 A1 ; Microsoft Corporation ; 1 Avril 2010** Tout le Document	1-4
A	**US20130133076 A1 ; Nec Corporation ; 23 MAI 2013** Tout le document	1-4

***Catégories spéciales de documents cités :**

-« **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
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« **P** » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« **E** » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

Partie 3 : Opinion sur la brevetabilité

Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté (N)	Revendications 3-4 Revendications 1-2	Oui Non
Activité inventive (AI)	Revendications 3-4 Revendications 1-2	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications 1-4 Revendications aucune	Oui Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : **US7000247 B2**
D2 : **US 20100082803 A1**

1. Nouveauté (N) :

1.1. Le document D1 divulgue un système autonome de sécurité informatique (D1 : colonne 2, lignes 3-6) contenant, entre autres, les éléments suivants :

- Un moyen de consolidation de la connaissance (D1 : Elément 16 de la figure 1, colonne 5, lignes 22-28) ;
- Un moyen de détection permettant de s'interfacer et d'agréger plusieurs types de détecteurs d'intrusions et de vulnérabilités (D1 : Elément 15 de la figure 1; colonne 4, lignes 22-30) ;
- Un moteur intelligent de régulation dynamique de la sécurité (D1 : Elément 12 de la figure 1; colonne 5, lignes 2-12 ; colonne 4, lignes 46-57).

Par conséquent, l'objet de la revendication 1 n'est pas nouveau au sens de l'art. 26 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

1.2. Le système décrit dans le document D1 comprend également un moyen pour la génération automatique de solution corrective qui est le module 18, et qui permet de remédier à une vulnérabilité (D1 : colonne 4, lignes 46-57). L'historique des vulnérabilités et des actions pour y remédier sont sauvegardés pour utilisation ultérieure dans la résolution de futures vulnérabilités (D1 : Revendication 20).
Le système comprend également un module de déploiement chargé de l'application des solutions consistant en la mise à jour des politiques de sécurité (D1 : Revendication 1).

Par conséquent l'objet de la revendication 2 est entièrement divulgué dans le document D1 d'où l'absence de nouveauté

1.3. Aucun des documents cités ci-dessus ne divulgue l'ensemble des caractéristiques techniques énoncées dans les revendications 3 et 4. Par conséquent, l'objet desdites revendications est nouveau au sens de l'article 26 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

2. Activité inventive (AI) :

2.1. N'étant pas nouveau, l'objet des revendications 1 et 4 n'implique pas une activité inventive au sens de l'art. 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

2.2. L'objet de la revendication 3 implique une activité inventive au sens de l'article 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

En effet, l'objet de ladite revendication diffère de l'état de la technique le plus proche D1 en ce que le système de sécurité informatique de la présente demande comporte également un moyen de qualification et de gestion de la réputation des comportements douteux.

L'effet technique lié à cette différence est de permettre l'évaluation du degré de la gravité des vulnérabilités avant l'isolation du service attaqué, en cas d'absence de mesures pour les contrer.

Le problème que la présente invention se propose de résoudre peut être considéré comme la gestion des vulnérabilités dans un système de détection et de correction automatiques, en cas d'absence de mesures adéquates pour y remédier.

La solution proposée par la présente demande peut être considérée comme impliquant une activité inventive. En effet, l'utilisation d'une unité de qualification qui permet l'appréciation de la gravité de l'attaque avant d'isoler le système, lorsqu'aucune solution n'a été produite pour remédier à une vulnérabilité donnée, n'est pas connue de l'état de la technique.

Quoique le document D2 décrive un système de sécurité informatique qui permet l'isolation d'un système non conforme aux règles de sécurité en cas d'absence de mesures pour remédier aux vulnérabilités (Abrégé), ledit document n'anticipe pas la gestion des fausses alertes par un système de qualification pour éviter l'isolement d'un service critique sur la base d'un comportement douteux.

Par conséquent, l'homme du métier n'aurait pas parvenu à l'objet de la revendication 3 sans faire preuve d'activité inventive.

2.3. La revendication 4 dépend de la revendication 3 dont l'objet est considéré inventif pour les raisons énoncés ci-dessus, ainsi elle satisfait également, en tant que telle, aux exigences de l'article 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13 concernant l'activité inventive.

3. Possibilité d'application industrielle (PAI) :

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible.