ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية
---

(12) DEMANDE DE BREVET D'INVENTION

(11) N° de publication :
MA 38914 A1

(43) Date de publication :
31.10.2017

(51) Cl. internationale :
G06F 21/30; G06F 21/31; H04K 1/00

(21) N° Dépôt :
38914

(22) Date de Dépôt :
17.03.2016

(71) Demandeur(s) :
KAMAL BENZEKKI, 198 houria, El alia, Mohammedia (MA)

(72) Inventeur(s) :
Kamal BENZEKKI

(54) Titre : **METHODE D'AUTHENTIFICATION ANTI-ESPIONNAGE PAR DESSUS L'EPAULE (SHOULDER SURFING)**

(57) Abrégé : L'invention concerne une manière d'enter un mot de passe pour se prémunir contre l'espionnage par-dessus l'épaule (shoulder surfing). La méthode inventée permet à un utilisateur de s'authentifier en tapant des caractères aléatoires qui contiennent le mot de passe réel. Afin d'extraire le mot de passe réel lors de la saisie sur une interface utilisateur d'une technologie requérant une authentification par mot de passe, nous avons mis en place une fonction qui se base sur une paire de délimiteurs choisis à base d'un ou plusieurs caractères établis au préalable. La fonction exécutée au niveau de l'interface utilisateur permet, d'une part, de détecter les délimiteurs qui identifient le début et la fin du mot du passe inséré dans la chaine de caractères aléatoires, d'autre part, supprimer l'ensemble des caractères aléatoires saisis, y compris les délimiteurs. Après l'extraction du mot de passe, celui-ci est renvoyé au système authentificateur avec l'identifiant associé pour la vérification/identification.

Abrégé

L'invention concerne une manière d'enter un mot de passe pour se prémunir contre l'espionnage par-dessus l'épaule (shoulder surfing). La méthode inventée permet à un utilisateur de s'authentifier en tapant des caractères aléatoires qui contiennent le mot de passe réel. Afin d'extraire le mot de passe réel lors de la saisie sur une interface utilisateur d'une technologie requérant une authentification par mot de passe, nous avons mis en place une fonction qui se base sur une paire de délimiteurs choisis à base d'un ou plusieurs caractères établis au préalable. La fonction exécutée au niveau de l'interface utilisateur permet, d'une part, de détecter les délimiteurs qui identifient le début et la fin du mot du passe inséré dans la chaine de caractères aléatoires, d'autre part, supprimer l'ensemble des caractères aléatoires saisis, y compris les délimiteurs. Après l'extraction du mot de passe, celui-ci est renvoyé au système authentificateur avec l'identifiant associé pour la vérification/identification.

Méthode d'authentification anti-espionnage par-dessus l'épaule (Shoulder Surfing)

Domaine de l'invention

La présente invention concerne une méthode et un système d'authentification permettant d'empêcher et de contrer l'attaque d'espionnage par-dessus l'épaule.

Etat de l'art

La confidentialité est devenue indispensable vu l'apparition de plusieurs types d'attaques qui visent à dérober les informations privées par le vol des mots de passe avec différentes manières. Parmi les méthodes les plus faciles à réaliser, il y a la méthode de l'espionnage par-dessus l'épaule ou « Clonage par distraction » qui requière moins d'effort et d'investissement en temps et argent. Ce type d'attaque peut se produire fréquemment dans les lieux publics où un utilisateur risque d'être exposé aux regards d'une personne malveillante ou curieuse. Cette personne pourrait être un(e) collègue, un(e) conjoint(e), un(e) ami(e), un(e) membre de la famille, ou une personne étrangère. En effet, chaque personne peut avoir une ou plusieurs motivation(s) ou intention(s) pour la violation de la vie privée, qui diffèrent d'un contexte à un autre. Par exemple, un conjoint peut être poussé par la jalousie, un collègue par la curiosité, un inconnu ou concurrent par les recettes secrètes d'un projet ou dossier confidentiel, etc. L'espionnage par-dessus l'épaule peut prendre une autre forme en utilisant un appareil d'enregistrement (e.g., Smartphone) qui permet de filmer les touches appuyées lors d'un processus de saisie. Cette démarche pourrait être plus efficace car, même si elle est moins fréquente, elle permet de réaliser un flashback et ainsi visionner facilement ce qui a été tapé en clavier en ralentissent les captures.

Par ailleurs, une étude menée avec des professionnels en technologie d'information, a révélé ce qui suit :

85% de ces professionnels ont admit avoir regardé, sans permission, des informations confidentiels sur les écrans des utilisateurs.

82% de ces professionnels ont confirmé que des informations affichées sur leurs écrans auraient pu être vu par des tiers non-autorisés.

82% de ces professionnels croient que les employés de leurs organisations ne sont pas ou peu intéressés par la protection de leurs informations privées exposées sur leurs écrans.

En outre, cette étude réalisée a aussi révélé que 98% de ces personnes sont conscientes des menaces que pourrait engendrer l'exposition de leurs informations sur écran.

Description de l'art antérieur

De nombreuses études traitant l'attaque de l'espionnage par-dessus l'épaule ont été effectuées et peuvent être subdivisées en trois catégories selon le mécanisme d'authentification mis en place. La première catégorie traite les méthodes d'authentification basées sur les mots de passe textuels, la deuxième catégorie propose des novelles méthodes d'authentification à base des représentations graphiques. Finalement, dans la troisième catégorie on trouve des méthodes d'authentification à base des PINs.

Dans le brevet américain No. 13/677,078, un system d'authentification graphique est proposé pour limiter l'espionnage par dessus l'épaule. Ce système permet à un utilisateur de sélectionner une image qui, à partir d'un ensemble d'images, sera adoptée pour son authentification dans le future. L'image sélectionnée est segmentée en M*N blocks sous frome de petits carreaux dont un parmi ceux-ci est désigné pour générer un mot de passe. Lors de l'authentification un indice aléatoire de login est créé et sur lequel se basera l'utilisateur pour glisser une barre horizontale et verticale à partir de la position de l'indice vers l'intersection formant le mot de passe. Plusieurs blocks peuvent être choisis respectivement à partir de différentes images pour une meilleure prévention.

Dans le brevet américain No. 13/286,772, l'invention propose un système pour les téléphones mobiles, GAB, tablettes PC qui repose sur une méthode de saisie de mot de passe de l'utilisateur afin de résister à l'espionnage par dessus l'épaule. La technique proposée pour authentifier un utilisateur consiste à sélectionner un chiffre représentant le mot de passe avec un arrière plan cible qui lui est associé. Lorsque l'utilisateur interpelle l'interface d'authentification, qui visualise les caractères en association avec des arrières plan aléatoires (image, couleur, schéma, etc.), il est amené à indiquer une association correcte du couple

chiffre/arrière plan cible pour pouvoir accéder aux ressources. L'authentification peut être personnalisée dans l'unité du control du système selon le niveau requis en sécurité.

Le brevet américain No. 8,789,154, présente un système d'authentification où un utilisateur crée un deuxième de mot de passe à partir d'un mot de passe principale et d'un nombre aléatoire. Ce dernière est généré depuis une fonction f() qui prend comme entrée le nom de l'utilisateur avec le premier mot de passe et le site web visité. Lors de l'authentification l'utilisateur fournit le deuxième mot de passe destiné à un site web avec le nom de l'utilisateur, ensuite le nombre aléatoire est récupéré pour extraire le premier mot de passe en appliquant la fonction inverse $f^{-1}()$. Après, le deuxième mot de passe est remplacé par le mot de passe principale, puis, celui-ci est redirigé vers le serveur pour s'authentifier.

Description du problème technique

La plupart des systèmes proposés reposent sur un ou plusieurs passage(s) de challenge/réponse pour parvenir à authentifier un utilisateur. Toutefois, l'ensemble des processus d'authentification qui leur en sont associés requièrent des efforts mentaux ou intelligence, du temps et une installation d'un système plus ou moins lourd. En outre, ces inventions manquent d'une réelle convivialité et ne sont pas adaptés à tous les types d'utilisateurs qui peuvent rencontrer des problèmes avec le mode d'emploi, manipulation ou carrément ne pas comprendre la méthode mise en place. Un système de protection contre la menace de l'espionnage par-dessus l'épaule doit idéalement établir une balance raisonnable entre la convivialité, la praticabilité, la sécurité et le délai total de l'authentification.

Solution apportée

Dans note invention, nous proposons un système et une nouvelle méthode d'enter un mot de passe. La méthode proposée utilise une technique innovante, facile à implémenter et à comprendre.

Notre système prend en entrée une chaine de caractères **100** incluant le mot de passe réel **105**, deux délimiteurs **101**, **102** et des caractères aléatoirement **103**, **104** tapés par l'utilisateur. L'utilisateur peut choisir n'importe quel type de caractère pour embrouiller une personne malveillante tentant d'observer ou de filmer les touches appuyées lors de la saisie du mot de

passe **100**. L'ensemble des caractères tapé constitue un mot de passe complexe **100** à suivre ou mémoriser vu l'aspect aléatoire des caractères **103, 104** accompagnant le mot de passe réel **105**. La chaine de caractères entrée **100** dans la zone du mot de passe est traitée implicitement au niveau des interfaces utilisateur **200, 300** pour extraire et envoyer le mot passe réel **105** au système authentificateur (serveur distant ou le system local). Le traitement effectué sur la chaine entrée **100** (concaténation des caractères aléatoires, délimiteurs et le mot de passe réel) consiste à extraire le mot de passe réel **105** à l'aide une fonction simple **106** qui permet de détecter les délimiteurs qui séparent le mot de passe orignal **105** et les caractères aléatoires **103, 104**. Lorsque les délimiteurs **101, 102** sont repérés, l'étape suivante consiste à éliminer ces délimiteurs **101, 102** ainsi que les caractères aléatoires **103, 104** et envoyer le nom de l'utilisateur **107** et le mot de passe réel **105** d'une manière transparente vers un système authentificateur pour la vérification.

Le traitement sur la chaine de caractère **100** contenant le mot de passe réel **105** se réalise automatiquement lorsque l'utilisateur valide le nom d'utilisateur **107** et le mot de passe **100** en cliquant sur un bouton de soumission **201**. La technique d'authentification employée dans notre système est très légère et ne demande aucun effort mental et réflexion. En effet, l'utilisateur a l'ample choix de caractère pour cacher le mot de passe réel **105** lorsqu'il est exposé aux regards des personnes éventuellement curieuses ou malintentionnées. La complexité du mot de passe augmente avec le nombre de caractères entrées **103, 104** et cela n'influence en aucun cas la performance du système car la fonction **106** mise en place se focalise uniquement sur les caractères représentant les délimiteurs **101, 102** et non pas les caractères aléatoires **103, 104**. Dans notre méthode, il est préconiser d'entrer plusieurs caractères aléatoires **103, 104** afin de décourager l'espionnage par-dessus l'épaule. Néanmoins, les caractères aléatoires **103, 104** peuvent contenir zéro caractère et/ou de multiples caractères avant le premier délimiteur **101** et/ou après le deuxième délimiteur **102**. Il faut aussi noter que les caractères aléatoires **103, 104** ne doivent pas contenir les caractères choisis pour les délimiteurs **101, 102**.

Les délimiteurs **101, 102** sont généralement au minimum deux caractères qui sont établis au préalable par l'utilisateur et peuvent être changés et personnalisés à tout moment depuis une mini-interface **300**. Un utilisateur peu choisir un ou plusieurs caractères pour désigner les délimiteurs **101, 102** et annoncer à la fonction **106** ou le mot de passe réel **105** commence et

se termine. Les délimiteurs **101**, **102** sont enregistrés localement (e.g., dans le navigateur, disque dur, etc.) et peuvent être définit à partir d'une mini-interface dédiée **300**. Cette interface **300** contient deux champs pour définir respectivement les deux délimiteurs **101**, **102** et un bouton **301** pour soumettre et enregistrer les cataractées représentant les délimiteurs **101**, **102**.

Notre méthode est innovante, efficace, transparente, conviviale et pratique avec un temps de traitement négligeable. Cette méthode proposée est facile à comprendre et à expliquer pour les tous les types d'utilisateurs. La clé de voûte de notre méthode est que notre système est capable d'être implicitement désactivé lorsque l'utilisateur est dans un endroit privé et souhaite directement entrer le mot de passe réel **105**. Effectivement, dans une telle situation la fonction ne détecte aucun délimiteur **101**, **102** et laisse tout simplement le mot de passe **105** transiter vers le système authentificateur. Lorsque l'utilisateur se retrouve dans un endroit publique il est sensé adopter notre système afin d'éviter l'espionnage par-dessus l'épaule. Généralement, les utilisateurs se sentent mal à l'aise lorsqu'ils sont accompagnés et veulent accéder à des ressources qui exigent un accès avec mot de passe, alors cela ne posera aucun souci si notre système est mis en ouvre.

Même si un utilisateur est lent et utilise un ou deux doigts lors de la saisie, ou si le mot de passe entré est court et d'une structure commune, notre méthode permettra intelligemment de camoufler le mot de passe réel saisi **105**.

Applications industrielles possibles

La présente invention peut être appliquée sous différentes plateformes. En effet, note système peut être implémenté dans les technologies Web (HTML, ASP.NET, JavaScript, etc.) et utiliser les différents types de stockage dans le navigateur (e.g., cookies, stockage en local, stockage en session, API, etc.) pour recevoir et enregistrer les délimiteurs **101**, **102**. Notre méthode peut être aussi appliquée aux différents systèmes (e.g., Windows, Linux, MAC, Androïd, iOS, etc.) pour authentifier un utilisateur désirant accéder à son système. Une autre application possible de notre méthode est les GABs (ATMs), dans ce cas, l'utilisateur pourra uniquement utiliser des chiffres pour cacher le PIN réel.

Revendications

Les réalisations de l'invention, au sujet desquelles un droit exclusif de propriété ou de privilège est revendiqué, sont définies comme il suit :

1- Un système d'authentification anti-espionnage par-dessus l'épaule comprenant :

Un module permettant à l'utilisateur d'enter un mot de passe en tout frome de concaténation avec des caractères choisis par l'utilisateur lors de la saisie, et des délimiteurs choisis au préalable.

Un module permettant de définir et d'enregistrer dans une mémoire ou unité de stockage (i.e., disque dur, API, stockage local du navigateur, stockage en session, cookies, serveur, USB) les délimiteurs qui vont cerner, à partir du mot de passe tapé, le mot de passe réel et aideront à déterminer son emplacement lors de l'extraction de celui-ci dans le processus de l'authentification.

Un module permettant de récupérer le mot de passe saisie, après avoir cliqué sur un bouton de soumission, de détecter les délimiteurs et extraire le mot de passe réel à soumettre au système authentificateur (i.e., système local, serveur distant).

2- Un système selon la revendication 1 où l'utilisateur pourrait choisir librement les caractères aléatoires ainsi que les délimiteurs.

3- Un système selon la revendication 1 où le module est implémenté dans un(e) Add-on/extension/plugin, application, un logiciel ou encore une implémentation dans un système d'exploitation.

4- Un système selon la revendication 1 où le module pourrait être désactivé systématiquement si l'utilisateur entre directement son mot de passe réel. Dans ce cas la fonction n'aura aucun effet sur le mot de passe réel et l'authentification fonctionnera normalement.

5- Un système selon la revendication 1 où la technique de concaténation est utilisée pour les mots de passe textuels, à base de PIN ou graphes (images).

6- Un système selon la revendication 2 comportant un module qui se base sur un ou plusieurs délimiteurs pour détecter et extraire le mot de passe réel.

7- Un procédé d'authentification comprenant les étapes suivantes :

Dans l'interface de l'authentification, l'utilisateur tape le nom d'utilisateur et le mot de passe sous forme d'une concaténation du mot de passe réel avec les délimiteurs et les caractères aléatoires.

L'utilisateur valide la combinaison mot de passe/nom d'utilisateur en cliquant sur le bouton soumettre.

La fonction de notre système prend en entrée la combinaison mot de passe/nom d'utilisateur et récupère le mot de passe pour détecter les délimiteurs et les supprimer avec les caractères aléatoires.

La fonction de notre système extrait et renvoie le mot de passe réel vers le système authentificateur.

La combinaison mot de passe/nom d'utilisateur est vérifiée contre une base de données. Si la combinaison est correcte l'accès est garanti aux ressources. Sinon, la demande d'authentification est rejetée. Si uniquement le mot de passe est incorrecte, l'utilisateur est invité à retaper le mot de passe.

Dessins

Dans les dessins qui illustrent l'invention,

La Figure 1 est une représentation de la méthode proposée reposant sur une fonction qui prend en entrée le nom de l'utilisateur et le mot de passe sécurisé. Le nom de l'utilisateur ne subit aucun traitement et son envoi vers le serveur est synchronisé avec le mot de passe ayant subi le traitement nécessaire (i.e., extraction).

La Figure 2 est une prise d'écran d'un exemple d'interface utilisateur. Dans ce cas de figure, l'utilisateur emploi une authentification via une interface WEB.

La Figure 3 illustre une prise d'écran d'une mini interface qui permet de définir les délimiteurs. Dans ce cas d'utilisation, une extension a été développée et insérer dans le navigateur.

La Figure 4 représente un graphe définissant les étapes à suivre pour définir les délimiteurs décrits dans la Figure 3. Les délimiteurs doivent être obligatoirement définit avant toute authentification pour pouvoir utiliser notre système d'authentification. Etape **401** consiste à ouvrir la mini-interface de notre système qui pourrait être développée sous forme d'une extension incarnée dans le navigateur, une configuration système ou application. Dans l'étape **402**, l'utilisateur est invité à entrer des caractères représentant les délimiteurs. Ensuite, les étapes **403** et **404** consistent respectivement à enregistrer les délimiteurs et fermer la mini-interface. Il faut noter que l'utilisateur doit mémoriser ces caractères et en cas d'oubli, il est invité à redéfinir de nouveaux délimiteurs.

La Figure 5 illustre un graphe qui détaille les étapes du processus d'authentification dans notre méthode. Dans l'étape **501** l'utilisateur connait à l'avance la structure du mot de passe. A l'étape **502**, l'utilisateur appelle une interface d'authentification pour enter, dans les étapes qui suivent, le nom d'utilisateur **503** et le mot de passe sous forme d'une concaténation **504** du mot de passe réel avec les délimiteurs et les caractères aléatoires. La combinaison mot de passe/nom d'utilisateur est validée à l'étape **505** en cliquant sur le bouton soumettre. Ensuite, la fonction de notre système prend en entrée ces données et récupère le mot de passe pour

détecter les délimiteurs dans l'étape **506** et supprimer ceux-ci et les caractères aléatoires dans l'étape **507**. A l'étape **508**, la fonction de notre système extrait et renvoie le mot de passe réel vers le système authentificateur. Finalement **509**, si la combinaison de mot de passe/nom d'utilisateur est correcte, l'accès est garanti aux ressources. Sinon, la demande d'authentification est rejetée.

La Table 1 illustre quelques exemples de mot de passes qu'un utilisateur pourrait créer.

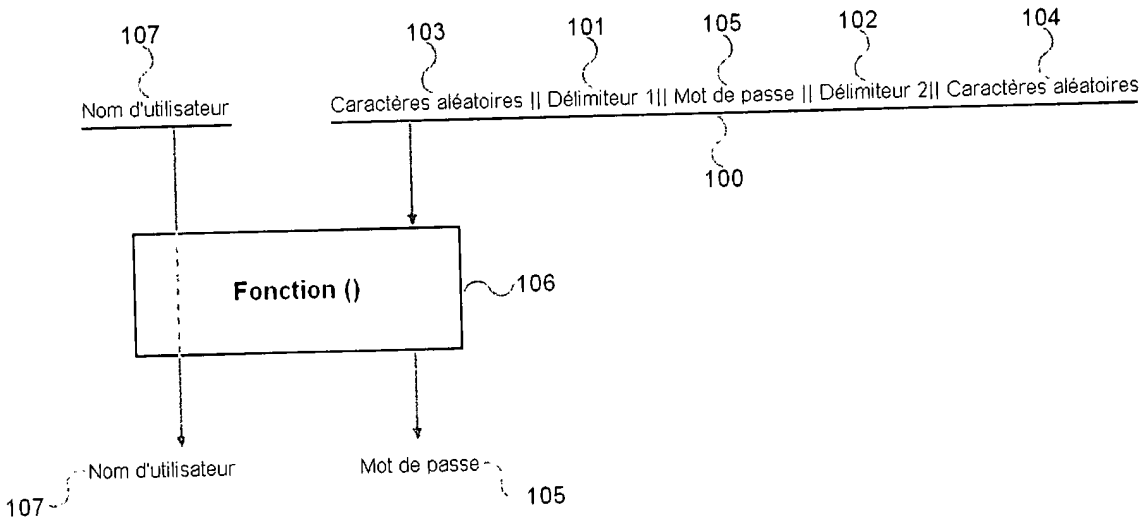

Fig. 1

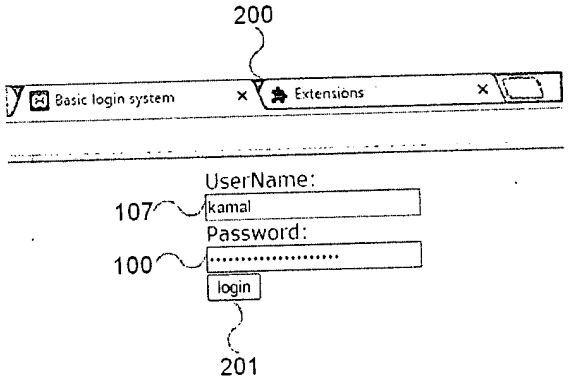

Fig. 2

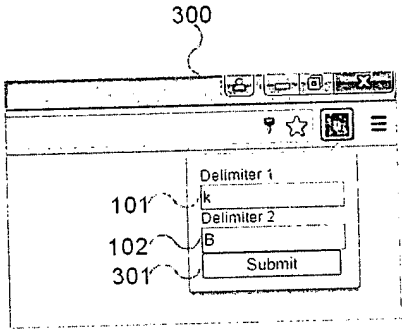

Fig. 3

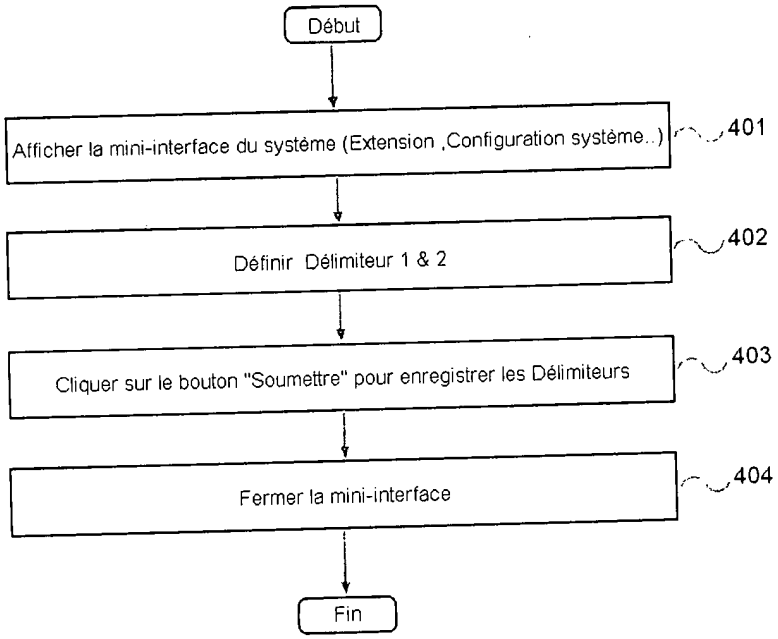
Début
Afficher la mini-interface du système (Extension ,Configuration système..)
401
Définir Délimiteur 1 & 2
402
Cliquer sur le bouton "Soumettre" pour enregistrer les Délimiteurs
403
Fermer la mini-interface
404
Fin

Fig. 4

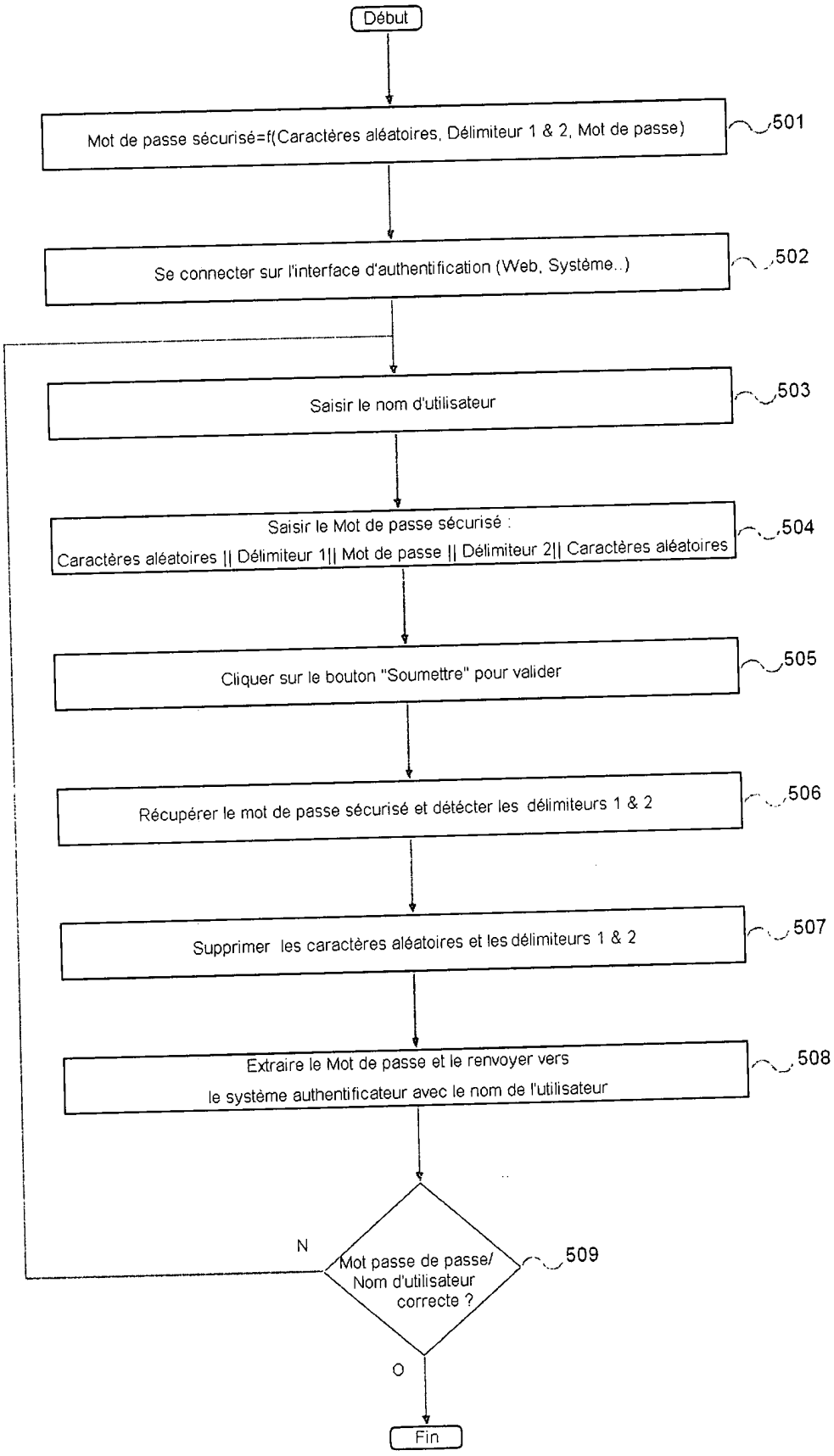
Début
Mot de passe sécurisé=f(Caractères aléatoires, Délimiteur 1 & 2, Mot de passe)
501
Se connecter sur l'interface d'authentification (Web, Système..)
502
Saisir le nom d'utilisateur
503
Saisir le Mot de passe sécurisé :
Caractères aléatoires || Délimiteur 1|| Mot de passe || Délimiteur 2|| Caractères aléatoires
504
Cliquer sur le bouton "Soumettre" pour valider
505
Récupérer le mot de passe sécurisé et détécter les délimiteurs 1 & 2
506
Supprimer les caractères aléatoires et les délimiteurs 1 & 2
507
Extraire le Mot de passe et le renvoyer vers
le système authentificateur avec le nom de l'utilisateur
508
N
Mot passe de passe/
Nom d'utilisateur
correcte ?
509
O
Fin

Fig. 5

Table 1

Mot de Passé Sécurisé	Délimiteur 1	Délimiteur 2	Mot de passé réel
Thisi**ZmyP@s5w0rd**/1230topsecret!	**Z**	**/**	**myP@s5w0rd**
92Dcan**youreveal"it"my**secretn0ws323	**you**	**my**	**Reveal"it"**
IisayDonTtellanybOdy(aboutit)	**I**	**any**	**isayDonTtell**
(Pass$you)HavetoKeepit0**9876privateE**	**9**	**E**	**876private**
NexTtimE?**beready4thebi**ggame/1209!#	**be**	**bi**	**ready4thechange**
Hello:Myname**iskamalmaybeUknowme**	**is**	**me**	**kamalmaybeUknow**

Citations de brevets

Brevet cité	Date de dépôt	Date de publication	Déposant	Titre
US20120110663	1 nov. 2011	3 mai 2012	Electronics And Telecommunications Research Institute	Apparatus and method for inputting user password
US20140053254	14 nov. 2012	20 févr. 2014	Industrial Technology Research Institute	Graphical authentication system and method for anti-shoulder surfing attack
US8789154	30 juin 2011	22 juil. 2014	Qualcomm Incorporated	Anti-shoulder surfing authentication method

Citations hors brevets

Article cité	Date de publication	Auteur
Visual Data Security White Paper	Juil. 2012	European Association for Visual Data Security

MA 38914A1

ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE

المملكة المغربية

المكتب المغربي للملكية الصناعية والتجارية

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 : 38914	Date de dépôt : 17/03/2016 ;
Déposant : KAMAL BENZEKKI	
Intitulé de l'invention : METHODE D'AUTHENTIFICATION ANTI-ESPIONNAGE PAR DESSUS L'EPAULE (SHOULDER SURFING)	

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	**Date d'établissement du rapport :** 28/03/2016
Téléphone: (212) 5 22 58 64 14/00	

ROYAUME DU MAROC ☆ OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE ☆ Unité Brevets, Dessins et Modèles

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
  7 Pages
- Revendications
  1-7
- Planches de dessin
  5 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : G06F21/30, G06F21/31, H04K 1/00,

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	US20050273625 A1 ; International Business Machines Corporation ; 08 Décembre 2005 Tout le document	1-7
X	US6954862 B2 ; Michael Lawrence Serpa ; 11 Octobre 2005 Tout le document	1-7
A	US20130007857 A1 ; Qualcomm Incorporate ; 3 Janvier 2013 Tout le document	1-7
A	WO2014053172 A1 ; Buntinx Bvba ; 10 Avril 2014 Tout le document	1-7

***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 4 : Remarques de clarté

4.1. La revendication 5 ne se fonde pas sur la description, étant donné que sa portée est plus large que celle qui est justifiée par la description et les dessins. En effet, la description et les dessins indiquent que la fonction de concaténation est utilisée uniquement pour les mots de passe textuels ou à base de PIN et qu'aucun autre type n'a été envisagé, en l'occurrence les graphes. Il convient de noter que cette caractéristique n'a pas été prise en compte pour l'examen de nouveauté/Activité inventive.

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

Nouveauté (N)	Revendications aucune Revendications 1-7	Oui Non
Activité inventive (AI)	Revendications aucune Revendications 1-7	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications 1-7 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 : US20050273625 A1

1. Nouveauté (N) et Activité Inventive :

1.1. Le document D1 divulgue un système d'authentification anti-espionnage par-dessus l'épaule (Revendication 11, Figure 1) comprenant :

- Un module permettant à l'utilisateur d'entrer le mot de passe (Figure 1, (102)) ;
- Un module de stockage des informations relatives au mot de passe (Figure 1, (103)), et un moyen permettant à l'utilisateur de définir les délimiteurs (Revendication 24) ;
- Un module permettant de récupérer le mot de passe saisit, de détecter les délimiteurs et extraire le mot de passe réel (Figure 1, (110) ; Revendication 25).

Par conséquent, l'objet de la revendication indépendante 1 n'est pas nouveau au sens de l'article 26 de la loi 17-97 modifiée et complétée par la loi 23-13 et n'implique pas d'activité inventive au sens de l'article 28 de ladite loi.

1.2. Dans le système de D1, l'utilisateur peut entrer librement les caractères aléatoires (Paragraphe [0005]), et définir les délimiteurs (Revendication 24). Ledit système peut être utilisé dans toutes les situations où l'utilisateur est amené à entrer un mot de passe (Paragraphe [0010]), De plus, la concaténation dans le système de D1 est utilisée pour les mots de passe alphanumériques (Paragraphe [0005]), et sera désactivée si l'utilisateur entre uniquement le mot de passe réel sans caractères aléatoires (Paragraphe [0017]) ; l'utilisateur a également la possibilité d'utiliser 1 (Paragraphe [0023]) ou plusieurs délimiteurs (Revendication 23).
Par conséquent, l'objet des revendications 2-6 est entièrement divulgué dans le document D1, d'où l'absence de nouveauté et d'activité inventive.

1.3. Le document D1 divulgue un procédé d'authentification anti-espionnage par-dessus l'épaule (Revendications 1-5, Figure 2) comprenant les étapes suivantes:

- Entre une séquence de caractères aléatoires contenant le mot de passe réel (Revendication 1, figure 1) et valide son entrée (caractéristique implicite);
- Analyser la séquence entrée en vue de déterminer les délimiteurs et extraire le mot de passe réel (Revendications 1,5 ; figure 1) ;
- Vérifier la validité du mot de passe et permettre l'accès si le mot de passe extrait correspond au mot de passe stocké pour l'utilisateur ; et rejeter la demande d'authentification sinon en réinvitant l'utilisateur à entrer le mot de passe correct (Revendications 1 ; Figure 1 ; Paragraphe [0024]).

Par conséquent, l'objet de la revendication indépendante 7 n'est pas nouveau au sens de l'article 26 de la loi 17-97 modifiée et complétée par la loi 23-13 et n'implique pas d'activité inventive au sens de l'article 28 de ladite loi.

2. 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.