ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19) OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) FASCICULE DE BREVET

(11) N° de publication :
MA 35474 B1

(51) Cl. internationale :
H04W 12/06; H04L 9/32

(43) Date de publication :
02.10.2014

(21) N° Dépôt :
35662

(22) Date de Dépôt :
12.02.2013

(71) Demandeur(s) :
DAHMANI ALI, 10 RUE AHMED NACERI QUARTIER PALMIER CASABLANCA (MA)

(72) Inventeur(s) :
DAHMANI ALI ;

(74) Mandataire :
DAHMANI ALI

(54) Titre : **SYSTEME D'AUTHENTIFICATION QUI PREND EN COMPTE LA VITESSE DE FRAPPE LORS DE LA SAISIE DU MOT DE PASSE.**

(57) Abrégé : L'invention concerne un nouveau système d'authentification différent du modèle standard, le mot de passe ne suffit plus pour savoir si l'utilisateur qui se connecte est réellement lui ou pas, on ajoute alors un facteur de temps unique pour chaque personne, qui est la vitesse de frappe, le rythme de saisie, la manière comment un utilisateur entre son mot de passe est prise en considération, les valeurs de la vitesse de frappe sont stockées en toute sécurité pour hausser les politiques de sécurité et baisser le taux de vol d'informations et d'intrusions. Le nouveau système d'authentification permet de s'assurer que les données ne soient pas volées facilement par les pirates informatiques « hackers » et mettre en sécurité les utilisateurs d'internet de tous les périphériques qui peuvent contenir un mot de passe.

Système d'authentification sécurisé qui prend en considération la vitesse de frappe lors de la saisie du mot de passe.

L'invention concerne un nouveau système d'authentification différent du modèle standard, le mot de passe ne suffit plus pour savoir si l'utilisateur qui se connecte est réellement lui ou pas, on ajoute alors un facteur de temps unique pour chaque personne, qui est la vitesse de frappe, le rythme de saisie, la manière comment un utilisateur entre son mot de passe est prise en considération, les valeurs de la vitesse de frappe sont stockées en toute sécurité pour hausser les politiques de sécurité et baisser le taux de vol d'informations et d'intrusions.
Le nouveau système d'authentification permet de s'assurer que les données ne soient pas volées facilement par les pirates informatiques « hackers » et mettre en sécurité les utilisateurs d'Internet de tous les périphériques qui peuvent contenir un mot de passe.

02 OCT 2014

L'invention présentée est une amélioration de tout concept du mot de passe et concerne un procédé d'identification électronique sécurisée, destiné à authentifier l'auteur d'une connexion à un site Internet, d'ouvrir les sessions d'ordinateurs (Windows / Linux / Mac Os etc...) ainsi que les différents périphériques qui peuvent stocker un mot de passe, téléphone mobile, tablette PC, guichets automatiques, coffre-fort, porte électronique etc...
Le système d'authentification bloque toute authentification dès que l'utilisateur arrive à 10 erreurs cumulables.
A partir du moment où le périphérique est bloqué, une solution de récupération de mot de passe est mise en place.

Dans l'état actuel de la technique, les solutions proposées sont de plusieurs types :
-Système d'authentification pour les ordinateurs.
-Système d'authentification pour les téléphones.
-Système d'authentification pour les tablettes PC.
-Système d'authentification pour les sites web.
-Système d'authentification pour les guichets automatiques.
-Système d'authentification pour les coffres-forts.
-Système d'authentification pour les écrans tactiles.
-Système d'authentification pour portes électroniques.
-Système d'authentification pour les Shell.
-Dispositifs mixtes logiciel/matériel de type « Carte SIM », « smartcard ».

Le système d'authentification varie d'un environnement à l'autre mais garde le même algorithme pour enregistrer la vitesse de frappe.
Il demande à l'utilisateur de rentrer son mot de passe 5 fois lors de l'enregistrement ou de la déclaration de l'utilisateur.
Une fois les 5 mots de passe rentrés, le système d'authentification prend les valeurs de chaque caractère des 5 mots de passe, enregistre par la suite la valeur minimale et la maximale de chaque caractère des 5 mots de passe pour ensuite les stocker au niveau de la base de données.
Pour finir, il tolère un décalage de 50ms à chaque caractère, un exemple :

Le mot de passe « Intruders » est tapé 5 fois par l'utilisateur, Il prend la valeur minimale de chaque caractère ainsi que la maximale, la valeur du premier caractère est toujours fixe, un chronomètre est déclenché et l'enregistrement commence, par exemple pour « n », qui est de 80ms, on tolère un décalage de 30ms à 130ms, en rajoutant et enlevant 50ms de la valeur minimale et maximale.
Cet algorithme permet à l'utilisateur de pouvoir s'authentifier avec une toute petite marge de décalage qui ne représente pas une faille de sécurité.

1/ Système d'authentification pour les ordinateurs.

Ce nouveau système d'authentification sera implémenté au niveau des ordinateurs dans trois niveaux différents :

-BIOS.

-Ouverture de session.

-Connexion à un réseau.

Au niveau du bios, une mise à jour devra être appliqué au niveau de la carte mère pour implémenter ce nouveau système d'authentification, le reverse engineering au niveau du Bios est actuellement une faille de sécurité qui permet de pénétrer au bios sans pour autant être obligé d'être le propriétaire de l'ordinateur.

Inconvénient : Récupération du mot de passe en cas d'oubli de la vitesse de frappe, une disquette de secours va permettre d'enregistrer un mot de passe qui va permettre la récupération, c'est l'unique facteur inconvénient au niveau du bios.

Lors de l'ouverture de la session, pour tous les OS (Windows, Linux, Mac Os), l'utilisateur doit rentrer son mot de passe au début 5 fois pour faire démarrer le service de système d'authentification avec la vitesse de frappe, à partir de cet instant, les valeurs de chaque caractère sont stockées à l'intérieur du OS en md5, l'OS correspondant ne pourra que vérifier les valeurs de chaque caractère avec l'intégralité du mot de passe si il est correct.

Pour récupérer le mot de passe, ou pour écraser la vitesse de frappe, il suffit lors de l'entrée des 5 mots de passe d'accepter la récupération de mot de passe, la récupération se fera grâce aux questions secrètes avec ses réponses, l'utilisateur doit répondre à 3 questions sur 10 choisies spécialement par l'utilisateur pour récupérer le mot de passe.

Lors de la connexion à un réseau par l'ordinateur, le routeur va prendre en considération la vitesse de frappe du mot de passe de l'utilisateur pour ensuite la comparer.

Le routeur devra supporter une configuration spécifique, « l'adressage mac », comme chaque ordinateur possède une adresse mac propre à lui, le routeur va vérifier si l'adresse mac est présente dans sa liste d'adresse mac acceptées, si l'utilisateur existe au niveau de la table, la comparaison du mot de passe/vitesse de frappe commencera.

Un tel procédé est obligatoire pour hausser les politiques de sécurité au sein des entreprises pour éliminer les intrusions au niveau du réseau et ainsi limiter les dégâts.

2/ Système d'authentification pour les téléphones.

Au niveau des téléphones mobiles, chaque demande d'authentification sera accompagnée par un mot de passe y compris sa vitesse.

Au niveau du déblocage du mot de passe, l'utilisateur devra utiliser sa vitesse de frappe, la récupération cependant sera plus simple, pour chaque téléphone on pourra utiliser le compte mail de l'utilisateur pour redémarrer le mot de passe, tout comme la reconnaissance d'un symbole spécifique pour récupérer le mot de passe.

Actuellement les pirates informatiques peuvent utiliser des photos personnelles depuis les réseaux sociaux pour permettre la récupération du mot de passe, pour contrer cette méthode, on propose à l'utilisateur de pouvoir utiliser un symbole, un dessin, une image d'un livre pour la récupération du mot de passe dans le cadre ou une connexion internet est impossible.

3/ Système d'authentification pour les tablettes PC.

Au niveau des tablettes pc, l'utilisateur aura le choix de combiner les schémas de déverrouillage avec la vitesse défilement, ou bien utiliser un mot de passe avec la vitesse de frappe.

Les schémas seront stockés au niveau d'une base de données à l'intérieur du système d'exploitation de la tablette PC.

L'utilisateur pourra aussi utiliser un nouveau module d'authentification qui est sous forme de combinaison, la combinaison peut être aussi associée à la vitesse de frappe, tout comme l'utilisateur peut se contenter de la combinaison avec son mot de passe.

Le procédé d'enregistrement d'informations pour la combinaison est similaire aux systèmes vus

précédemment, l'utilisateur doit rentrer sa combinaison de chiffres 5 fois pour que le système d'authentification puisse déterminer un intervalle dans laquelle l'utilisateur peut se connecter.
La récupération est la même que celle du téléphone mobile, sois en utilisant le compte mail d'inscription, sois des réponses secrètes cryptés en MD5.

4/ Système d'authentification pour les sites web.

Le système d'authentification pour les sites web est une des parties les plus cruciales à améliorer.
Au niveau du serveur d'hébergement, le client (l'entreprise) doit installer sous forme d'API le nouveau système d'authentification qui permet :

- La prise en compte de la vitesse de frappe
- La gestion des périphériques (Suppression, ajout)
- Déblocage des périphériques bloqués

En ce qui concerne la vitesse de frappe, le procédé est toujours le même l'utilisateur doit rentrer son mot de passe 5 fois, une barre s'auto-incrémente de 20% à chaque fois que le mot de passe est rentré, pour atteindre finalement 100%, l'utilisateur doit nommer son périphérique.
Après l'authentification de l'utilisateur avec sa vitesse de frappe, une liste est affichée de tous les périphériques enregistrés avec leurs OS, navigateurs et leurs noms.
Pour rajouter un nouveau périphérique, l'utilisateur doit se connecter avec son login et son mot de passe depuis le nouveau périphérique, un email sera envoyé sur son compte mail, l'utilisateur devra entrer depuis son nouveau périphérique à la boîte mail pour ajouter un périphérique.
La suppression d'un périphérique se fait depuis le panneau sans confirmation, ça permet en cas de vol ou de perte de périphérique de sécuriser les données.
Pour sécuriser les données d'avantages, un système d'encryptions sous forme de VPN et de SSL est mise en place par l'hébergeur, l'utilisateur pourra installer un programme de VPN pour chiffrer ses données pour contrer les techniques courantes d'ethical hacking comme par exemple sniffers de paquets http, getform, et de cookies.
Au niveau de l'utilisateur encore une fois, en cas d'échec d'authentification 10 fois, le compte est par la suite bloqué, un mail est envoyé à l'utilisateur pour débloquer son compte, une fois que l'utilisateur accède au lien depuis son compte mail, un nouveau mot de passe est mis en place avec une nouvelle vitesse de frappe, et tous les périphériques sont supprimés, ceci est dans le cadre ou l'utilisateur rate sa vitesse de frappe, on comprendra directement qu'il y a une intrusion.
Le point fort de ce système d'authentification est :
Pour voler le compte d'un utilisateur, on est obligé de se déplacer pour sniffer les cookies, l'authentification est impossible pour un hacker vu qu'il a besoin du login, mot de passe, vitesse de frappe, et rentrer toutes ces données sur un périphérique autorisé par l'utilisateur lui-même.
Ce sont des facteurs qui haussent la sécurité informatique dans tous les domaines, dans le cadre d'une connexion VPN/SSL, mélangée avec ces facteurs difficilement contournables, l'utilisateur est protégé de toute intrusion illégale.

5/ Système d'authentification pour les guichets automatiques.

Au niveau du guichet automatique, les utilisateurs devront procéder de la manière suivante :

- Demander l'authentification avec la vitesse de frappe
- Se présenter dans l'agence, un guichet automatique à l'intérieur de la banque devra être mis en place pour pouvoir taper son mot de passe 5 fois pour que le système d'authentification puisse déterminer la vitesse de frappe.
- Les données seront envoyées en toute sécurité au serveur principal pour que l'implémentation soit faite
- Le serveur principal va par la suite communiquer les données à tous les guichets automatiques pour que la base de données soit mise à jour.
- L'utilisateur pourra après s'authentifier avec sa vitesse de frappe.

Si l'utilisateur se trompe 5 fois au niveau du guichet automatique, la carte sera retirée, la récupération devra être physique pour faire une réinitialisation de la vitesse de frappe avec son mot de passe.

Toutes les données vont être au niveau du serveur, l'utilisateur ne pourra que se connecter et le guichet automatique ne fera que vérifier si les données sont correctes.

6/ Système d'authentification pour les coffres-forts.

Au niveau des coffres-forts, l'utilisateur d'un coffre-fort devra se présenter chez les vendeurs de ce dernier.

Les coffres-forts seront programmés pour deux choses :

- Les 5 premières utilisations seront présentes pour permettre à l'utilisateur de sécuriser à 100% son matériel.
- Un code sera donné à l'utilisateur pour changer la vitesse d'ouverture de la combinaison, la combinaison ne changera pas mais la vitesse changera cependant.

Ces facteurs pourront empêcher les intrusions à un très grand taux sans pour autant présenter des brèches de sécurité.

Avant : connaître la combinaison permet d'ouvrir le coffre.

Après : connaître la combinaison avec sa vitesse permet d'ouvrir le coffre, un code est présent pour réinitialiser la vitesse, mais aucune faille de sécurité n'est disponible pour le moment.

7/ Système d'authentification pour les écrans tactiles.

Au niveau des écrans tactiles, les utilisateurs seront sécurisés d'une manière innovante, à ce jour pour débloquer un écran tactile, il suffit de déverrouiller le schéma ou bien d'entrer son mot de passe.

Pour permettre à un utilisateur de pouvoir se connecter, il aura le choix d'utilisateur le nombre de ses doigts et de faire un mouvement avec une vitesse spécifique.

L'utilisateur pourra par exemple sur l'écran tactile faire sa propre signature avec sa propre vitesse, deux facteurs totalement inconnus pour les hackers.

Tout comme le schéma de déverrouillage pourra être amélioré pour qu'il soit synchronisé avec la vitesse de frappe.

La récupération se fera par compte mail ou 3 questions secrètes avec leurs réponses.

8/

-Système d'authentification pour portes électroniques, les Shell. Dispositifs mixtes logiciel/matériel de type « Carte SIM », « smartcard ».

Ce nouveau système d'authentification peut s'appliquer aux routeurs de sorte à prendre en considération le rythme lors d'un ajout d'ordinateur au sein d'un réseau.
Le processus permettra une authentification sécurisée en limitant les intrusions sur les puces SIM qui concernent grandement les opérateurs téléphoniques de tous les pays du monde.

Type d'authentification	**Matériel requis**
-Système d'authentification pour les ordinateurs.	Ordinateur, clavier, souris, connexion internet
-Système d'authentification pour les téléphones.	Téléphone sous Android/ Ios/ Blackberry os / Windows phone, connexion internet
-Système d'authentification pour les tablettes PC.	Tablette ordinateur, connexion internet
-Système d'authentification pour les sites web.	Serveur d'hébergement, connexion internet
-Système d'authentification pour les guichets automatiques.	Serveur de communication, connexion internet, clavier numérique, carte bancaire.
-Système d'authentification pour les écrans tactiles.	Ecran tactile, connexion internet
-Système d'authentification pour portes électroniques.	Carte mère stockant les données d'authentification.
-Système d'authentification pour les coffres-forts.	Carte mère stockant les données d'authentification.
-Système d'authentification pour les Shell.	Routeur compatible wifi, connexion internet
-Dispositifs mixtes logiciel/matériel de type « Carte SIM », « smartcard ».	Téléphone uni/double SIM, carte SIM, connexion internet

Système d'authentification sous forme d'API :

Le système d'authentification peut se présenter sous forme d'API regroupant plusieurs méthodes d'authentifications et laissant choix à l'utilisateur de pouvoir choisir celle qui lui semble la plus convenable.
L'utilisateur devra installer l'API de ce système d'authentification pour choisir le type d'authentification parmi les listes proposées, cette solution permettrait de séduire les particuliers tout en touchant une part un marché qui cible gros.
Aucune autre entreprise ou toute personne physique ou morale n'aura le droit d'utiliser le système d'authentification avec la vitesse de frappe sans avoir au préalable demandé avis au propriétaire, et uniquement sous son accord signé avec un contrat de confidentialité que cette entreprise pourra uniquement utiliser le système d'authentification.
Aucune modification sans avoir pris en considération l'avis du créateur (Dahmani Ali) entraînera une poursuite judiciaire pour litige et manipulation d'informations.

220

REVENDICATIONS

***

1/Procédé d'authentification individuelle en prenant en compte le rythme et la vitesse de frappe de
225 connexion à une session sur l'ordinateur tout OS confondu, ou bien une connexion distante à un serveur INTERNET utilisant un PC de type xx86, et s'exécutant directement depuis le support amovible à partir d'un système d'exploitation (O.S) courant ou propriétaire, caractérise en ce qu'il comporte les étapes suivantes :

a) Installation sur le disque dur hôte du nouveau système d'authentification pour mettre à jour
230 les composants logiques de la carte mère.
b) Détection de l'état du mode d'administration du système d'exploitation résident.
c) Lancement d'un dispositif de contrôle de mot de passe faisant appel à une saisie par clavier physique ou visuel, il faudra que l'utilisateur qui souhaite s'authentifier puisse rentrer correctement le rythme de frappe pour avoir accès au compte.
235 d) Etablissement d'une connexion avec un ou des sites spécialisés destinés à procéder à un contrôle d'intégrité de la mémoire de la machine utilisée afin de vérifier que la mémoire du périphérique utilisé n'est pas infectée par des virus ou trojans.
e) Vérification que les ports TCP/IP ne sont pas sollicités sans autorisation ;
f) Connexion automatique ou non, à un ou plusieurs périphériques ou un ou plusieurs sites
240 réclamant une authentification.
g) Identification par échange de messages faisant appel à une ou des méthodes de cryptage.
h) Effacement des traces de la session et tout type de fichiers utilisés durant celle-ci, en cas de fonctionnement sous système d'exploitation résident.

245

2/ Procédé selon la revendication 1, caractérisé en ce que l'étape b) entraîne un choix automatique entre l'option d'un fonctionnement sur système d'exploitation résident ou l'option d'un fonctionnement sur système d'exploitation propriétaire embarqué.

250 3/ Procédé selon la revendication 1 caractérise en ce que l'étape c) de vérification de rythme de mot de passe introduit une temporisation systématique de plusieurs secondes avant de valider ou refuser la saisie.

4/ Procédé selon la revendication, caractérise en ce que les effacements de l'étape h) ne concerne
255 pas seulement les fichiers de consultation Internet, mais également toutes autres tâches accomplies durant la session.

5/ Support amovible pour effectuer les étapes du procédé selon la revendication 2, caractérise en qu'il est n'est pas réinscriptible

260

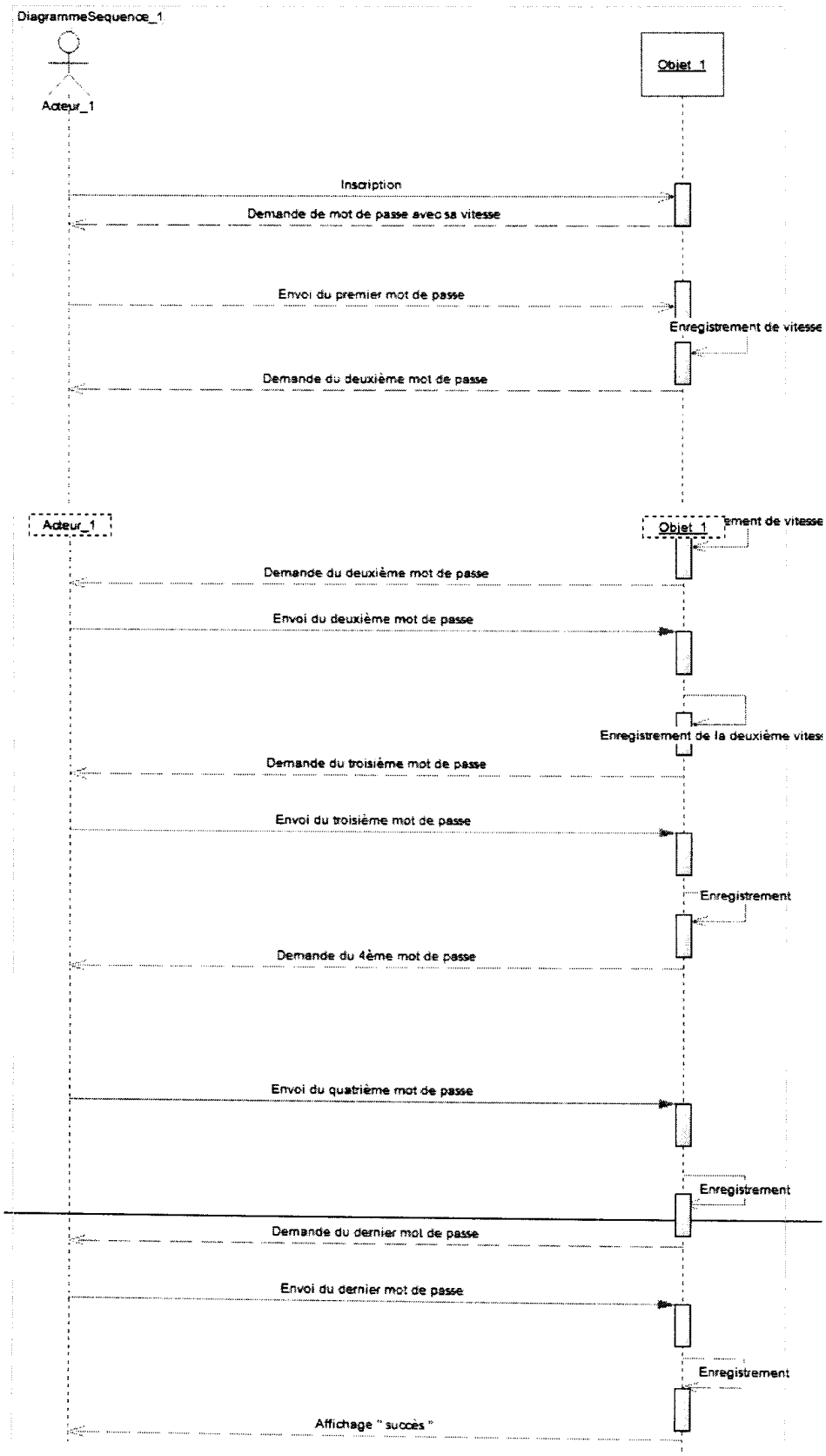
6/ Programme produit comprenant des instructions de code de programme enregistré sur un support utilisable dans n'importe quel ordinateur, tablette PC, ou téléphone selon la revendication 1, 2,3, 4

265

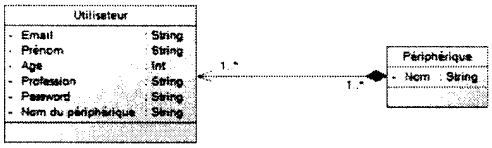
270

Dessins

***


DiagrammeSequence_1
Acteur_1
Objet_1
Inscription
Demande de mot de passe avec sa vitesse
Envoi du premier mot de passe
Enregistrement de vitesse
Demande du deuxième mot de passe
Acteur_1
Objet_1
Demande du deuxième mot de passe
Envoi du deuxième mot de passe
Enregistrement de la deuxième vites
Demande du troisième mot de passe
Envoi du troisième mot de passe
Enregistrement
Demande du 4ème mot de passe
Envoi du quatrième mot de passe
Enregistrement
Demande du dernier mot de passe
Envoi du dernier mot de passe
Enregistrement
Affichage " succès "

275


Utilisateur
- Email : String
- Prénom : String
- Age : Int
- Profession : String
- Password : String
- Nom du périphérique : String
1..*
1..*
Périphérique
- Nom : String