Sécurité et Utilisabilité: le cas des mots de passe graphiques

Lilian LE QUERE
Université Paul Sabatier
Toulouse, France
lequere.lilian@gmail.com

Pierre JEANMOUGIN
Université Paul Sabatier
Toulouse, France
pierre@jeanmougin.fr

Matteo MOUGEOT
Université Paul Sabatier
Toulouse, France
matteo.mougeot@gmail.com

Benjamin LACHERAY
Université Paul Sabatier
Toulouse, France
b.lacheray@gmail.com

ABSTRACT
Dans le cadre de systèmes d'authentification par mot de passe graphiques, les notions de sécurité et d'utilisabilité vont difficilement de paire, le renforcement de l'un causant l'affaiblissement de l'autre. Dans ce document, nous recensons plusieurs systèmes d'authentifications graphiques ainsi que leurs avantages et inconvénients en ce qui concerne ces deux notions. Nous proposons de plus une approche permettant d'attribuer des notes en sécurité et en utilisabilité à chaque système, permettant de comparer les systèmes entre eux.

1. INTRODUCTION
La méthode d'authentification la plus commune utilise les noms d'utilisateur et mots de passe alphanumériques. Cette méthode présente des inconvénients importants. Par exemple, les utilisateurs préfèrent choisir des mots de passe courts, identiques sur plusieurs systèmes et préfèrent les conserver le plus longtemps possible. Toutes ces caractéristiques augmentent le risque de découverte des informations d'authentification par des personnes ayant des intentions malveillantes. Pour éviter ceci les administrateurs de systèmes imposent des contraintes sur la composition des mots de passe (lettre, caractères spéciaux, chiffres, …), leur fréquence de renouvellement, … Toutes ces contraintes rendent les mots de passe plus difficiles à mémoriser, à saisir et entraînent des erreurs multiples pouvant conduire au blocage du compte (empêchant complètement l'utilisateur d'effectuer son travail).

Pour remédier à ce problème, des méthodes d'identification utilisant des images comme mots de passe ont été développées. Mais ces nouvelles méthodes permettent-elles d'atteindre le même niveau de sécurité ? Quelles sont les principaux problèmes lors de la conception de mots de passe graphiques ?

Le but de ce rapport est de recenser différents système d'authentifications par mots de passe graphiques et de réaliser une étude comparative du point de vue de leur utilisabilité et du point de vue de la sécurité qu'elles garantissent.

Dans la section suivante, nous allons vous présenter les différentes vulnérabilité en termes de Sécurité (ou Threats), auxquels les différents système d'authentifications peuvent être sensibles ainsi que les différents types d'authentification liés a l'utilisabilité. Dans la section "Les différentes catégories de systèmes d'authentification graphiques" nous allons recenser les différents systèmes d'authentifications en fonction de leurs catégories et lister leurs fonctionnements, leurs avantages et inconvénients en terme de sécurité et d'utilisabilité. Enfin dans la section "Notre approche systématique de comparaison des systèmes d'authentification graphique", nous allons vous présenter la méthode que nous avons utilisé pour comparer les différents système du point de vue de la sécurité et du point de vue de l'utilisabilité.

2. LES ATTAQUES POSSIBLES SUR LES SYSTÈMES D'AUTHENTIFICATION GRAPHIQUES
L'une des attaques possibles est de tester une par une toutes les possibilités pour un mot de passe, c'est ce qu'on appelle la Brute Force Attack. Cette méthode pouvant être extrêmement inefficace si le mot de passe est long, on utilise en général les Dictionary Attack qui utilisent les habitudes des utilisateurs et les patterns pour réduire l'espace de recherche et les tester une a une.
Dans le cas des appareils tactiles, il est aussi possible d'analyser les traces de doigts laissées sur l'écran par l'utilisateur pour découvrir son mot de passe, c'est ce qu'on appelle une Smudge Attack.[1]
Il est possible d'analyser le mouvement des yeux de l'utilisateur pour deviner ce qu'il regarde pendant l'authentification pour deviner son mot de passe, c'est l'Eye Tracking.
Il existe d'autres types d'attaques, comme celles relatives a l'environnement d'exécution (spyware, Keylogger, captures réseau), les Guessing Attack qui consistent à deviner le mot de passe à partir de ce qu'on sait de l'utilisateur, le Phishing et le Social Engineering dont nous ne parlerons pas dans ce TER.

3. LES DIFFÉRENTES CATÉGORIES DE SYSTÈMES D'AUTHENTIFICATION GRAPHIQUES
Nous distinguerons les méthodes d'authentifications selon 3 catégories:

Les systèmes d'authentifications basés sur le rappel pur (pure recall) où l'utilisateur doit se souvenir exactement de son mot de passe (le système d'authentification basé sur les mots de passes alphanumériques en est un bon exemple).

Les systèmes d'authentifications basés sur le rappel indicé (cued recall) où l'utilisateur est aidé pour entrer son mot de passe.

Les systèmes d'authentifications basés sur la reconnaissance (ou recognition), où l'utilisateur doit reconnaître une image. Cette catégorie est considéré plus "user friendly" que les précédentes puisque les humains se souviennent plus facilement d'images que d'une suite de caractères ou de schémas.

3.1 Les systèmes basés sur le rappel pur
Dans cette partie nous allons évoquer trois systèmes d'authentifications basés sur le rappel pur: Draw-A-Secret, Pass-Go et Android Pattern Lock.

3.1.1 Le système Draw-A-Secret

L'utilisateur doit réaliser un dessin sur une grille NxN qu'il a enregistré au préalable comme on peut le voir à la Figure 1. A la différence du Android Lock Pattern et du Pass-Go, le mot de passe ne passe pas par les angles de cette grille mais par les cases. [2]

Il existe plusieurs variantes de DAS, Background Draw a Secret (BDAS), la même grille est utilisée que pour DAS, mais elle est recouverte par une image choisie par l'utilisateur. [2]

Rotationnal Draw A Secret (RDAS): cette variante utilise le même mécanisme que DAS en y incorporant la possibilité de faire tourner le dessin dans un sens ou dans l'autre que ce soit avant, après ou même pendant le dessin. [3]

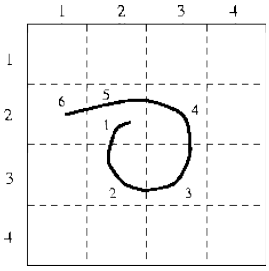

Figure 1. Exemple de mot de passe DAS[4]

3.1.1.1 Avantages en terme de sécurité

Il est possible de rendre DAS résistant au Shoulder Surfing via différentes techniques, le Decoy Strokes où l'utilisateur rentre des traits qui ne font pas parti du mot de passe avec des couleurs de traits différents, le Disappearing Strokes où les traits disparaissent après avoir été entrés par l'utilisateur ou le Line Snaking où le bout d'un trait disparaît au fur et a mesure qu'il est entré par l'utilisateur. [4]

RDAS rend le mot de passe bien plus résistant aux attaques dictionnaires que DAS[3] ainsi qu'aux Smudge Attacks puisque les traces de doigts permettent de retrouver le tracé, mais pas le nombre de rotation effectuées pendant le tracé.

3.1.1.2 Inconvénients en terme de sécurité

En l'état, DAS est sensible au Shoulder Surfing puisque le dessin reste affiché sur l'écran.[4] De plus, plusieurs dessin différents peuvent être acceptés pour un même mot de passe, particulièrement sur des grilles avec peu de cases.[2]

BDAS est plus sensible aux attaques dictionnaire car si l'image permet à un utilisateur de retrouver son mot de passe, elle fournit aussi des indications sur les points les plus susceptibles d'être utilisés.[5]

3.1.1.3 Avantages en terme d'utilisabilité

Le Mot de passe est facile à retenir dans tout les cas. L'entrée du mot de passe se fait rapidement. BDAS rend la mémorisation plus efficace.[2]

3.1.1.4 Inconvénients en terme d'utilisabilité

Les lignes et angles de la grille posent problème puisque si l'on suit une ligne, il est difficile de savoir sur quelle case voisine a cette ligne on est. C'est encore plus vrai pour les angles puisqu'ils ne touchent pas seulement 2 mais 4 cases.[2] Ce problème fait que plus le nombre de cases augmente, plus il est difficile de rentrer un mot de passe, ce qui provoque l'obligation de faire un choix entre utilisabilité et sécurité.

3.1.2 Le système Pass-Go

Inspiré du jeu de Go, c'est un système basé sur une grille (5x5 ou 9x9 dans la version originale). En passant par les intersections des cellules de la grille, l'utilisateur peut dessiner un motif, il est possible de passer par le même point plusieurs fois ou de s'arrêter à un point et reprendre a un autre.[9] En figure 2, un ensemble d'exemples de mots de passe possibles avec Pass-Go.

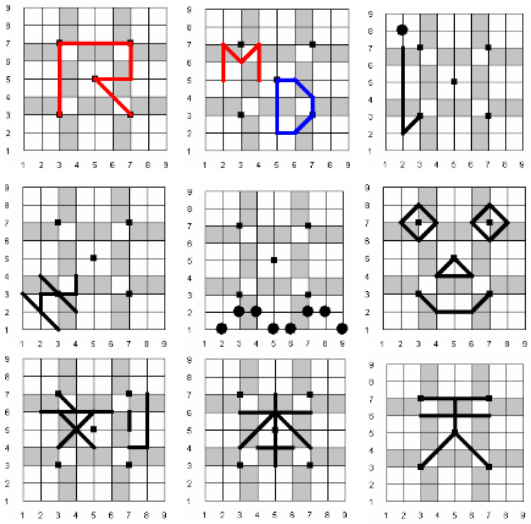

Figure 2, Exemples de mots de passe Pass-Go[9]

3.1.2.1 Avantages en terme de sécurité

L'espace de mot de passe est très grand, ce qui rend les attaques Brute Force et Dictionary compliquées. Il est aussi possible de rajouter des couleurs pour augmenter encore la taille de cet espace. (Pour un mot de passe passant par 19 points sur une grille 9x9 et proposant 8 couleurs, l'espace est d'environ 180 bits, soit 1,5 x 10^{54} possibilités). De plus, les utilisateurs tendent a utiliser des mots de passe longs.[9]

3.1.2.2 Inconvénients en terme de sécurité

Ce système est sensible au Shoulder Surfing, une solution est proposée est de cacher les indicateurs mais les utilisateurs n'utilisent jamais cette fonctionnalité [9] ou d'utiliser le clic droit de la souris pour générer des faux tracés.

En cas d'utilisation sur écran tactile, ce système est sensible aux Smudges Attacks. Les utilisateurs ont tendance à trop se reposer sur les points de repères de la grille, rendant les mots de passe plus prédictifs.

3.1.2.3 Avantages en terme d'utilisabilité:

Présence de repères sur la grille pour orienter l'utilisateur, l'utilisation de couleur permet aussi d'améliorer la mémorisation. Le taux de réussite est élevé et le nombre d'oublis du mot de passe est assez faible.[9]

3.1.2.4 Inconvénients en terme d'utilisabilité

Certains utilisateurs tendent à faire des schémas complexes qu'ils ont du mal a retenir.

3.1.3 Android Pattern Lock

C'est une version modifiée et plus simple de la méthode Pass-go avec une taille de grille de 3x3 et un nombre de mouvements limités.

L'utilisateur dispose d'une grille de taille 3x3 et le mot de passe de l'utilisateur est un dessin sur cette grille par une séquence de lignes reliant les points. Lors du choix du mot de passe, l'utilisateur choisit sa séquence et pour s'authentifier il doit le redessiner sur l'écran. Au moins 4 points doivent être choisis. Aucun point ne peut être réutilisé. Seules les lignes droites sont autorisées. On ne peut pas sauter par-dessus des points non visités.[13]. Des exemples de schémas respectant ces règles sont montrés en figure 3.

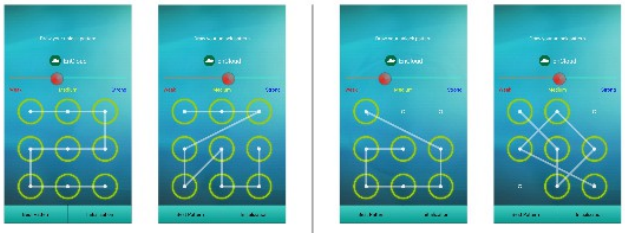

Figure 3. Exemples de mots de passe Android Pattern Lock[13]

3.1.3.1 Avantages en terme de sécurité

Pour éviter les attaques Brute Force et Dictionary, un système de blocage est généralement utilisé. C'est plus sécurisé qu'un code PIN a 4 chiffres.[13]

3.1.3.2 Inconvénients en terme de sécurité

Très sensible aux Smudge Attacks[1] et au Shoulder Surfing.

Les utilisateurs tendent à utiliser les même points pour commencer leur mot de passe comme on peut le voir en figure 4.

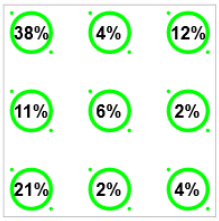

Figure 4. Pourcentages des points de départ des utilisateurs [12]

3.1.3.3 Avantages en terme d'utilisabilité

L'authentification est très rapide et il est difficile de se tromper grâces aux règles imposées.

3.1.3.4 Inconvénients en terme d'utilisabilité

Certains segments sont difficiles a effectuer dans certaines situations et donc rarement voir jamais utilisés. (notamment les longues diagonales comme par exemple de la case en haut a gauche a la case en bas au milieu) [13]

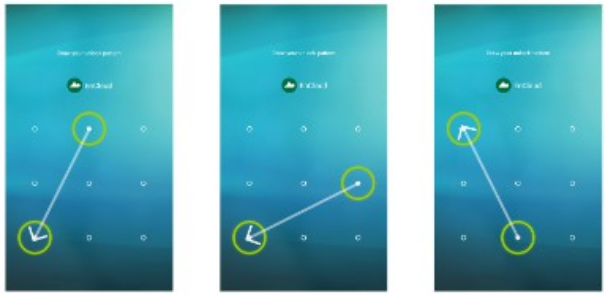

Figure 5. Exemples de segments peu ou pas utilisés[13]

3.2 Les systèmes basés sur le rappel indicé

Dans cette partie nous allons évoquer un système d'authentification basé sur le Cued Recall: Passpoint.

A noter que BDAS que nous avons évoqués dans la section 4.1 appartient plutôt a la catégorie Cued-Recall que Pure-Recall, mais vu ses ressemblances avec DAS nous avons préféré l'évoquer à ce moment.

3.2.1 Le système Passpoint

L'utilisateur choisit une image ainsi que des points à repérer sur cette image; quand il devra se connecter, le système lui demandera de retrouver ces points sur l'image comme on peut le voir sur la figure 5.

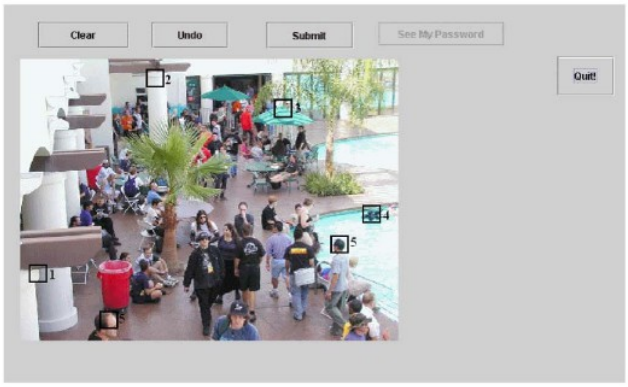

Figure 5. Exemple de mot de passe Passpoint avec l'ordre des points affiché[7]

3.2.1.1 Avantages en terme de sécurité

Résistant aux Brute forces Attacks, si l'image fait 1024x752 pixels, qu'on autorise une marge d'erreur de 20x20 pixels et que l'on demande 5 points, la taille de l'espace du mot de passe est de $2.6x10^{16}$ [7]

3.2.1.2 Inconvénients en terme de sécurité

En cas d'utilisation de Passpoint sur un écran tactile, la taille de la marge d'erreur autorisée doit être bien plus élevée que pour une sélection a la souris. De plus cela rend le système sensible aux Smudges Attacks.

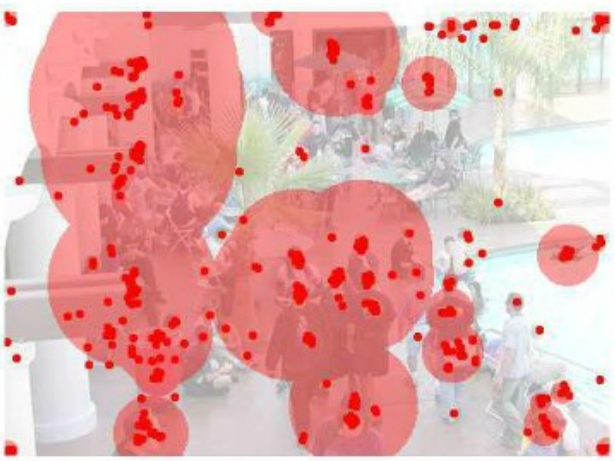

Figure 6. Points les plus utilisés comme mots de passe sur l'image de la figure 5[5]

On sait aussi que les humains ont tendance à choisir les mêmes points sur une image, ce qui peut rendre ce système sensible aux Dictionary Attacks.[5] Voir la figure 6 pour connaître les points les plus utilisés sur une image telle que celle vue en figure 5.

3.2.1.3 Avantages en terme d'utilisabilité

Le taux de réussite est bon (environ 80%), le temps de saisie du mot de passe est acceptable et la pratique améliore la précision.[8]

3.2.1.4 Inconvénients en terme d'utilisabilité

Le choix de l'image peut influencer le taux de réussite.[8] Sur un écran tactile, la sélection est très imprécise et est gênée par le fait que l'utilisateur cache l'image avec son doigt.

3.3 Les systèmes basés sur la reconnaissance

Dans cette partie nous allons évoquer quatre systèmes d'authentification basés sur la "Recognition": Passface, Déjà Vu, Convex Hull Click et ColorLogin Graphical.

3.3.1 Le Système Passfaces

L'utilisateur choisit un ensemble d'images de visages humains et les sélectionne parmi des images leurres pour l'authentification. Il y a 5 phases dans la configuration par défaut, à chaque phase il faut sélectionner un visage parmi une grille de 9 visages (une faisant partie du portfolio, 8 autres aléatoires). Un exemple en noir et blanc est montré en figure 7.

Figure 7. Exemple de grille Passfaces [11]

3.3.1.1 Avantages en terme de sécurité

Comme il est difficile de décrire précisément l'ensemble des visages du portfolio, le mot de passe a peu de chance d'être noté ou transmis à quelqu'un.

3.3.1.2 Inconvénients en terme de sécurité

Si aucun blocage n'est installé sur le nombre de tentatives, très sensible aux attaques Brute Force. En effet la probabilité de s'authentifier au hasard est de $(1/9)^R$ avec R le nombre de phases.

Les utilisateurs tendent à choisir des visages qui leurs plaisent, particulièrement les utilisateurs tendent a choisir des visages de personnes de la même ethnie et en ce qui concerne les visages de femmes, les plus beaux sont utilisés dans la majorité des cas[10], ce qui rend vulnérables aux Guessing Attacks et Dictionary Attacks.

3.3.1.3 Avantages en terme d'utilisabilité

Les utilisateurs se souviennent plus facilement de visages que de textes, le taux d'erreur est trois fois moins élevé pour les mots de passes Passface que pour les mots de passe classiques [11]

3.3.1.4 Inconvénients en terme d'utilisabilité

Le temps d'authentification est plus élevé que pour les mots de passes textuels.

3.3.2 Le système Déjà Vu

L'utilisateur doit faire une sélection d'un nombre défini d'images générées de manière aléatoire pour créer son Portfolio. Pour s'identifier, il devra retrouver les images de son Portfolio dans une plus large sélection d'images générées aléatoirement. En figure 8, un exemple d'interface pour Déjà Vu.

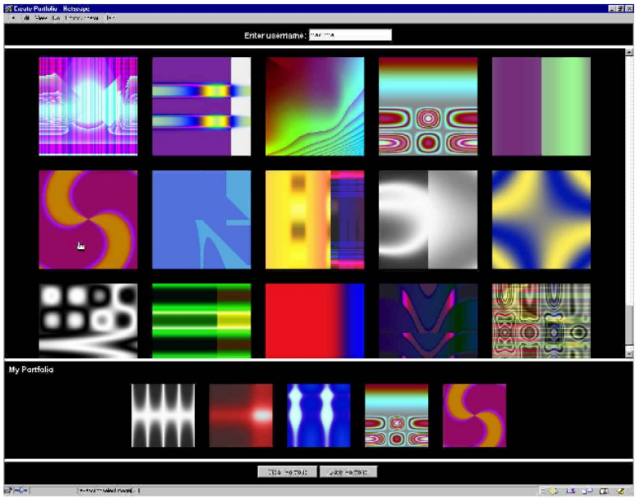

Figure 8. Exemple d'interface d'authentification utilisant Déjà Vu. Le portfolio de l'utilisateur n'est normalement pas affiché.[6]

3.3.2.1 Avantages en terme de sécurité

Déjà Vu est résistant aux attaques Brute Force et Dictionary, en effet le nombre de combinaisons est de $\binom{n}{m}$, avec n le nombre d'images montrées, m le nombre d'images du portfolio affichées. on prend par exemple n = 20 et m = 5, ce qui donne 15504 possibilité par étape.[6].

Il est de plus difficile de partager un mot de passe puisque cela nécessite de montrer toutes les images du portfolio. On peut lutter

contre les Guessing Attacks en utilisant des Random Arts plutôt que des photos.[6]

C'est aussi totalement résistant aux Smudge Attacks puisque la position des images est aléatoire.

3.3.2.2 Inconvénients en terme de sécurité

Bien que Déjà Vu soit résistant au Shoulder Surfing puisqu'une observation ne permet pas de connaître tout le portfolio, des observations répétées du mot de passe permettent de diminuer la sécurité du mot de passe.[6]

3.3.2.3 Avantages en terme d'utilisabilité

L'authentification se fait assez rapidement, environ 30 secondes. [6]

Le pourcentage d'erreur est aussi bien plus faible en utilisant Déjà Vu qu'avec un mot de passe ou un PIN.[6]

3.3.2.4 Inconvénients en terme d'utilisabilité

La création du Portfolio est relativement longue comparée à la création de mots de passes classiques.[6]

3.3.3 Le système Convex Hull Click

La méthode d'authentification Convex Hull Click est une méthode créée pour être résistante face au problème de Shoulder Surfing. Elle consiste à ce que l'utilisateur choisisse plusieurs icônes pour mot de passe (3 ou plus). Lors de la session d'authentification, l'utilisateur verra une fenêtre avec un grand nombre d'icônes disposées aléatoirement. Il devra alors localiser au moins 3 des icônes composant son mot de passe et dessiner mentalement l'enveloppe convexe qu'ils forment (au minimum 3 icônes appartenant à son mot de passe seront présent sur la fenêtre, choisies aléatoirement). Il lui suffit ensuite de cliquer n'importe où dans cette enveloppe convexe. L'authentification se fait en plusieurs sessions pour plus de sécurité, avec à chaque fois une nouvelle position des icônes, et différentes icônes du mot de passe.[14] Les Figures 9 et 10 permettent de montrer des exemples d'authentification selon le système Convex Hull Click.

3.3.3.1 Avantages en terme de sécurité

Résistant, voire invulnérable, au Shoulder Surfing. Résiste aux attaques Brutes Forces et Dictionary. Dans le cas d'une utilisation sur un écran tactile, la génération aléatoire des icônes et de leurs positions rend le système résistant aux Smudges Attacks.

3.3.3.2 Inconvénients en terme de sécurité

Le choix des icônes par l'utilisateur peut amener à une faiblesse face aux Guessing Attacks. Ce problème peut être réglé si un mot de passe aléatoire est donné à l'utilisateur plutôt qu'un mot de passe qu'il choisit.

3.3.3.3 Avantages en terme d'utilisabilité

Facile à retenir, le taux d'erreur est très faible.[14]

3.3.3.4 Inconvénients en terme d'utilisabilité

L'augmentation du nombre de sessions peut rendre le mot de passe long à entrer, il faut en moyenne 10 secondes par session. [14]

Il arrive aussi que le positionnement aléatoire des icônes du mot de passe créent une zone difficilement cliquable par l'utilisateur comme on peut le voir en Figure 11 (problème dit du "narrow triangle" ou Triangle Étroit).

Figure 9. Exemple d'icônes choisies comme mot de passe [14]

Figure 10. Exemples de zones formées par 3(haut) et 5(bas) icônes du mot de passe, les icônes et les zones a cliquer ne sont normalement pas colorées.[14]

Figure 11. Exemple de zone difficilement cliquable.[14]

3.3.4 Le Système ColorLogin Graphical

ColorLogin est une méthode qui utilise les couleurs. Les multiples couleurs sont utilisées pour embrouiller les yeux des attaquants et aider l'utilisateur a s'authentifier plus vite.

Le défi se déroule en R étapes et chaque round produit des icônes aléatoires affichées sur l'écran. Une icône mot de passe est choisie correctement quand l'utilisateur clique sur la ligne qui contient cette icône mot de passe. Les icônes dans cette ligne sont toutes remplacées par des icônes "Lock" pour résister au shoulder surfing. Un round est considéré réussi quand toutes les icônes mot de passe sont correctement choisies. Il n'est pas nécessaire aux utilisateurs de choisir un ordre en particulier. Voir exemple en Figure 12.

Figure 12. Exemple d'une étape complète, les lignes contenant des icônes du mot de passe sur lesquelles l'utilisateur a cliqué sont remplacées par des "Lock" [15]

3.3.4.1 Avantages en terme de sécurité

Résistant au Shoulder Surfing. L'espace du mot de passe est également assez grand (une authentification en 3 étapes sur une grille 9x9 a plus de 46 000 possibilité, si on utilise une grille 15x15 on passe a plus de 1 100 000)[15]

3.3.4.2 Inconvénients en terme de sécurité

Bien que résistant, n'est pas invulnérable au Shoulder Surfing.

3.3.4.3 Avantages en terme d'utilisabilité

L'utilisation de couleur aide à la mémorisation du mot de passe ainsi qu'à l'amélioration du temps pour entrer le mot de passe (2 à 3 fois plus long à entrer si on retire la couleur du fond)[15]

3.3.4.4 Inconvénients en terme d'utilisabilité

Bien que chaque étape ne prenne pas beaucoup de temps a être validée (3 à 5 secondes par étape en moyenne)[15], l'augmentation du nombre d'étapes peut rendre l'authentification longue et laborieuse.

4. NOTRE APPROCHE SYSTÉMATIQUE DE COMPARAISON DES SYSTÈMES D'AUTHENTIFICATION GRAPHIQUE

Afin de pouvoir facilement comparer les systèmes d'authentifications graphiques, nous avons mis en place une approche consistant à appliquer une note sur 5 du point de vue de la sécurité et du point de vue de l'utilisabilité. Pour mieux montrer les écarts, les notes de nos métriques sont 0, 2, 3 et 5.

4.1 Notre approche pour noter la sécurité

Afin d'attribuer une note à la sécurité du système, nous attribuons une note à la résistance aux différentes attaques selon les métriques suivantes. Il y a aussi une note de 0 à 3 sur l'espace de mot de passe. La note globale de sécurité étant la moyenne de toutes ces notes. La figure 13 montre le tableau pour noter la sécurité de tout les systèmes vu précédemment.

4.1.1 Métriques de résistance aux Brute Force Attacks

La note 0 est attribuée si le mot de passe est trouvé rapidement et dans 100% des cas.

La note 2 est attribuée si le mot de passe peut être trouvé mais avec un temps de calcul conséquent (plusieurs jours de calculs).

La note 3 est attribué s'il est possible de trouver le mot de passe mais avec du temps et des moyens conséquents (un temps de calcul de plusieurs mois sur plusieurs machines en parallèle).

La note 5 est attribuée si le nombre de combinaison est trop important pour qu'une Brute Force Attack soit réalisable.

4.1.2 Métriques de résistance aux Dictionary Attacks

La note 0 est attribuée si le mot de passe est trouvé facilement en utilisant un dictionnaire basique.

La note 2 est attribuée si le mot de passe peut être trouvé en fonction de ce qu'on sait sur l'utilisateur ou de statistiques faites sur un groupe d'utilisateurs.

La note 3 est attribuée s'il est difficile de trouver le mot de passe même en ayant des connaissances sur l'utilisateur ou en utilisant des statistiques faites sur un groupe d'utilisateurs.

La note 5 est attribuée si la le système d'authentification fait en sorte qu'aucune statistique ou connaissance sur l'utilisateur ne permette de trouver le mot de passe.

4.1.3 Métriques de résistance au Shoulder Surfing

La note 0 est attribuée si un attaquant peut voir et retenir en une seule fois le mot de passe pendant qu'un utilisateur s'authentifie.

La note 2 est attribuée si un attaquant peut déduire le mot de passe en observant un utilisateur s'authentifier plusieurs fois.

La note 3 est attribuée si même pour un Shoulder Surfer averti, il faut filmer une session d'authentification complète pour déduire le mot de passe.

La note 5 est attribuée si le mot de passe ne peut être déduit même en filmant plusieurs session d'authentification.

4.1.4 Métriques de résistance aux Smudge Attacks

La note 0 est attribuée si les traces conduisent immédiatement à connaître le mot de passe.

La note 2 est attribuée si l'analyse des trace conduit à la connaissance du mot de passe dans 50% des cas.

La note 3 est attribuée si l'analyse des traces conduit à la connaissance du mot de passe dans de rares cas.

La note 5 est attribuée si le système est invulnérable aux Smudges Attacks.

4.1.5 Métriques de résistance à l'Eye Tracking

La note 0 est attribuée si l'observation des mouvement des yeux de l'utilisateur permet de déduire le mot de passe.

La note 2 est attribuée si une observation plus poussée des yeux de l'utilisateur est nécessaire pour déduire le mot de passe.

La note 3 est attribuée si le lien entre le mouvement des yeux de l'utilisateur et le mot de passe est très faible.

La note 5 est attribuée s'il n'y a aucun lien entre le mouvement des yeux de l'utilisateur et le mot de passe.

4.1.6 Métriques de résistance aux attaques relatives à l'environnement d'exécution type Spyware, Keylogger ou capture réseau

La note 0 est attribuée si le mot de passe peut être utilisé dès qu'il est récupéré par l'attaquant.

La note 2 est attribuée si l'attaquant doit effectuer un travail d'analyse pour pouvoir utiliser le mot de passe.

La note 3 est attribuée si l'attaquant peut analyser et déduire le mot de passe en se basant sur l'interception de plusieurs sessions d'authentification.

La note 5 est attribuée si l'attaquant ne peut déduire le mot de passe de l'utilisateur malgré l'interception de plusieurs sessions d'authentification.

4.1.7 Métriques relatives à l'espace de mot de passe

Le cas de l'espace de mot de passe est particulier puisqu'il entre en compte dans la résistance aux attaques Brute Force et Dictionary, pour éviter qu'il n'impacte encore plus la note de sécurité, les métriques correspondent a des notes allant de 0 à 3 (contrairement aux autres qui vont de 0 à 5)

La note 0 est attribuée s'il existe entre 1 et 10^3 possibilités de mots de passe.

La note 1 est attribuée s'il existe entre 10^3 et 10^6 possibilités de mots de passe.

La note 2 est attribuée s'il existe entre 10^6 et 10^{15} possibilités de mots de passe.

La note 3 est attribuée s'il existe plus de 10^{15} possibilités de mots de passe.

4.2 Notre approche pour noter l'utilisabilité

Afin d'attribuer une note à l'utilisabilité du système, nous attribuons une note aux domaines de la norme ISO 9241-11, à savoir une note pour l'efficience, une note pour l'efficacité et une note pour la satisfaction. L'efficacité étant la même pour tous puisque tout les système permettent d'atteindre le même résultat (l'authentification de l'utilisateur) elle n'entre pas en compte dans la note. La note d'efficience est quant à elle partagée en trois domaines: le temps d'apprentissage du mot de passe, le temps de mémorisation du mot de passe et le temps mis pour s'authentifier. La note d'utilisabilité est la moyenne de ces notes. La figure 14 montre le tableau pour noter l'utilisabilité de tout les systèmes vu précédemment.

4.2.1 Métriques liées au temps d'apprentissage du mot de passe

La note 0 est attribuée si l'apprentissage est laborieux et que l'utilisateur a de nombreux échecs d'authentification après la création du mot de passe.

La note 2 est attribuée si l'apprentissage prend un moment et que le nombre d'erreur est faible.

La note 3 est attribuée si l'apprentissage se fait facilement et que les erreurs sont dues à une erreur lors de l'entrée du mot de passe.

La note 5 est attribuée si l'apprentissage est immédiat et qu'aucune erreur n'est faite.

Nom du système	Catégorie	Brute Force Attack	Dictionary Attack	Shoulder Surfing	Smudge Attack	Eye tracking	Spyware, Keylogger	Espace de mot de passe	Indice de sécurité
Alphanumérique	rappel pur	3	3	2	5	5	0	3	3,00
Convex Hull Click	reconnaissance	3	5	5	5	0	5	3	3,71
Draw-A-Secret	rappel pur	3	3	2	2	0	3	3	2,29
Background DAS	rappel Indicé	3	3	2	2	0	3	3	2,29
Rotational DAS	rappel pur	5	3	3	3	3	3	3	3,29
Android Pattern Lock	rappel pur	0	3	0	2	3	0	1	1,29
Passfaces	reconnaissance	0	2	2	5	3	3	1	2,29
Déjà Vu	reconnaissance	0	2	2	5	3	3	1	2,29
Passpoint	rappel indicé	3	3	0	0	3	2	3	2,00
Pass-Go	rappel pur	3	3	2	2	3	2	3	2,57
ColorLogin Graphical	reconnaissance	0	2	3	5	5	3	2	2,86

Figure 13. Tableau d'application de notre approche systématique de notation de la sécurité de différents systèmes.

4.2.2 Métriques liées au temps de mémorisation du mot de passe

La note 0 est attribuée si l'utilisateur oublie son mot de passe dans les jours suivants sa création.

La note 2 est attribuée si l'utilisateur se souvient toujours de son mot de passe plusieurs semaines après sa dernière utilisation.

La note 3 est attribuée si l'utilisateur se souvient toujours de son mot de passe plusieurs mois après sa dernière utilisation.

La note 5 est attribuée si l'utilisateur se souvient toujours de son mot de passe plusieurs années après sa dernière utilisation.

4.2.3 Métriques liées au temps d'authentification

La note 0 est attribuée si l'utilisateur s'authentifie en plus d'une minute.

La note 2 est attribuée si l'utilisateur s'authentifie entre 30 secondes et une minute.

La note 3 est attribuée si l'utilisateur s'authentifie entre 10 et 30 secondes.

La note 5 est attribuée si l'utilisateur s'authentifie en moins de 10 secondes.

4.2.4 Métriques liées a la satisfaction de l'utilisateur

La note 0 est attribuée si l'utilisateur trouve le système inutilisable.

La note 2 est attribuée si l'utilisateur trouve le système assez pratique.

La note 3 est attribuée si l'utilisateur trouve le système pratique.

La note 5 est attribuée si l'utilisateur trouve le système très pratique.

5. CONCLUSION

Les domaines de la sécurité et de l'utilisabilité sont difficilement conciliables dans le cadre d'un système d'authentification graphique, et le fait que ces domaines sont étudiés séparément fait que les développeurs d'un système auront plus tendance à sacrifier un domaine au profit de l'autre.

Nous avons défini les différentes attaques possibles sur les systèmes d'authentification graphiques. Nous avons défini les différentes catégories de systèmes d'authentifications graphiques, classé différents systèmes selon ces catégories et donné les avantages et inconvénients en termes de sécurité et d'utilisabilité de chacun de ces systèmes. Nous avons proposé une approche permettant d'attribuer une note de sécurité et une note d'utilisabilité à un système d'authentification graphique afin de pouvoir les comparer les uns aux autres selon ces critères.

Ce document permet d'obtenir des informations sur les systèmes d'authentifications graphiques les plus connus. Il est aussi possible d'utiliser notre approche de notation afin de comparer un nouveau système à ceux existant déjà.

En ce qui concerne les futurs travaux, des études plus poussées sont nécessaires pour valider ou modifier certaines valeurs des tableaux, notamment des études de tests pour mettre à jour les valeurs concernant la résistance à l'Eye Tracking, la satisfaction des utilisateurs et l'efficience pour chacun des systèmes.

Nom du système	Catégorie	Efficience (efficiency)			Efficacité (effectiveness)	Satisfaction	Indice d'utilisabilité
		Apprentissage	Mémorisation	Temps d'authentification			
Alphanumérique	rappel pur	2	2	3		3	2,5
Convex Hull Click	reconnaissance	2	3	0		3	2
Draw-A-Secret	rappel pur	5	3	5		5	4,5
Background DAS	rappel indicé	5	3	5		5	4,5
Rotational DAS	rappel pur	3	3	3		3	3
Android Pattern Lock	rappel pur	5	3	5		5	4,5
Passfaces	reconnaissance	5	3	3		3	3,5
Déjà Vu	reconnaissance	2	3	3		3	2,75
Passpoint	rappel indicé	3	3	3		3	3
Pass-Go	rappel pur	3	2	3		3	2,75
ColorLogin Graphical	reconnaissance	2	3	3		3	2,75

Figure 14. Tableau d'application de notre approche systématique de notation de l'utilisabilité de différents systèmes.

6. REFERENCES

[1] Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., & Smith, J. M. (2010). "Smudge attacks on smartphone touch screens," *In Proceedings of the 4th USENIX conference on Offensive technologies* (WOOT'10). USENIX Association, Berkeley, CA, USA, 1-7.

[2] Dunphy, P., & Yan, J. (2007). “Do background images improve "draw a secret" graphical passwords?,” *In Proceedings of the 14th ACM conference on Computer and communications security* (CCS '07). ACM, New York, NY, USA, 36-47.

[3] Chakrabarti , S., Landon, G. V., & Singhal, M. (2007). “Graphical passwords: drawing a secret with rotation as a new degree of freedom,” *In Proceedings of the Fourth IASTED Asian Conference on Communication Systems and Networks* (AsiaCSN '07), M. H. Hamza and C. E. Palau Salvador (Eds.). ACTA Press, Anaheim, CA, USA, 114-120.

[4] Zakaria, N.H., Griffiths, D., Brostoff, S., & Yan, J. (2011). “Shoulder surfing defence for recall-based graphical passwords,” *In Proceedings of the Seventh Symposium on Usable Privacy and Security* (SOUPS '11). ACM, New York, NY, USA, , Article 6 , 12 pages. DOI=http://dx.doi.org/10.1145/2078827.2078835

[5] Thorpe, J., & Van Oorschot, P.C. (2007). “Human-seeded attacks and exploiting hot-spots in graphical passwords,” *In Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium* (SS'07), Niels Provos (Ed.). USENIX Association, Berkeley, CA, USA, , Article 8 , 16 pages.

[6] Dhamija, R., & Perrig, A. (2000). “Déjà Vu: a user study using images for authentication,” *In Proceedings of the 9th conference on USENIX Security Symposium - Volume 9* (SSYM'00), Vol. 9. USENIX Association, Berkeley, CA, USA, 4-4.

[7] Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005). “PassPoints: design and longitudinal evaluation of a graphical password system,” *Int. J. Hum.-Comput. Stud.* 63, 1-2 (July 2005), 102-127. DOI=http://dx.doi.org/10.1016/j.ijhcs.2005.04.010

[8] Chiasson, S., Biddle, R., & Van Oorschot, P.C. (2007). “A second look at the usability of click-based graphical passwords,” *In Proceedings of the 3rd symposium on Usable privacy and security* (SOUPS '07). ACM, New York, NY, USA, 1-12. DOI=http://dx.doi.org/10.1145/1280680.1280682

[9] Tao, H. & Adams, C. (2008). “Pass-Go: A proposal to improve the usability of graphical passwords,” Int. J. Net. Secur. 7, 2, 273--292.

[10] Davis, D., Monrose, F., & Reiter, M.K. (2004). On user choice in graphical password schemes. In *Proceedings of the 13th conference on USENIX Security Symposium - Volume 13* (SSYM'04), Vol. 13. USENIX Association, Berkeley, CA, USA, 11-11.

[11] Brostoff, S., & Sasse, M.A. (2000). “Are Passfaces More Usable Than Passwords? A Field Trial Investigation,” In Proceedings of Human Computer Interaction, pages 405–424, 2000.

[12] Uellenbeck, S., Dürmuth, M., Wolf, C., & Holz,T. (2013). “Quantifying the security of graphical passwords: the case of android unlock patterns,” *In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (CCS '13). ACM, New York, NY, USA, 161-172. DOI=http://dx.doi.org/10.1145/2508859.2516700

[13] Song, Y., Cho, G., Oh, S., Kim, H., & Huh, J.H. (2015). “On the Effectiveness of Pattern Lock Strength Meters: Measuring the Strength of Real World Pattern Locks,” *In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15). ACM, New York, NY, USA, 2343-2352. DOI=http://dx.doi.org/10.1145/2702123.2702365

[14] Wiedenbeck, S., Waters, J., Sobrado, L., Birget, J.-C. (2006). “Design and evaluation of a shoulder-surfing resistant graphical password scheme,” *In Proceedings of the working conference on Advanced visual interfaces* (AVI '06). ACM, New York, NY, USA, 177-184. DOI=http://dx.doi.org/10.1145/1133265.1133303

[15] Gao, H., Liu, X., Dai, R., Wang, S., & Chang, X. (2009). “Analysis and Evaluation of the ColorLogin Graphical Password Scheme,” *In Proceedings of the 2009 Fifth International Conference on Image and Graphics* (ICIG '09). IEEE Computer Society, Washington, DC, USA, 722-727. DOI=http://dx.doi.org/10.1109/ICIG.2009.62