De la prolifération des mots de passe : modèle des stratégies des usagers pour l'authentification

Robin Héron

Télécom-Paristech, 75013, Paris, France

robin.heron@telecom-paristech.fr

Stéphane Safin

Télécom-Paristech, 75013, Paris, France

stephane.safin@telecom-paristech.fr

Anne Bationo-Tillon

Université Paris 8, 93200 St-Denis, France

anne.bationo-tillon@univ-paris8.fr

RÉSUME

Dans les environnements numériques, nous sommes confrontés à un nombre toujours croissant de sites et services sécurisés par des mots de passe. Or, si la sécurité informatique nécessite des règles précises et contraignantes de construction de mots de passe, celles-ci ne sont pas toujours respectées par les utilisateurs. Dans cette étude, nous avons conduit onze entretiens pour comprendre les stratégies et ressources que ces utilisateurs développent et mobilisent pour la réussite de l'authentification par mots de passe. Nous modélisons l'activité d'authentification autour de deux sous-composantes - la gestion des identifiants et l'accès aux identifiants. Nous constatons que les utilisateurs réutilisent leurs mots de passe sur différents sites, développent des techniques de création particulières, en fonction de la situation et/ou de leurs habitudes et gardent des traces qu'ils peuvent rechercher lors de la connexion. Nous identifions les différents facteurs influençant l'activité d'authentification et proposons des pistes pour la conception des systèmes d'authentification afin de favoriser l'utilisabilité.

MOTS-CLES

Mots de passe ; Activité d'authentification

1 INTRODUCTION

La prolifération des services en ligne nécessitant la création d'un compte utilisateur pose la question de la sécurisation de l'accès aux données. À l'heure actuelle, l'identification des utilisateurs par mot de passe alphanumérique reste le moyen privilégié de s'assurer de l'authenticité de l'usager pour les interactions avec les services considérés et pour la protection de ses données personnelles.

Cela implique que les utilisateurs se créent un mot de passe pour chaque service en ligne sécurisé, y associent une adresse email ou créent également un nom d'utilisateur et qu'ils gardent par la suite ces paires en mémoire pour accéder aux contenus et services. En suivant les injonctions de sécurité parfois mentionnées sur les sites lors de la création de mots de passe, les utilisateurs devraient posséder un mot de passe unique par site d'au moins 8 caractères avec a minima, un chiffre, un caractère spécial, une majuscule et une minuscule et ne devront en aucun cas les noter.

Or, plusieurs études révèlent que les utilisateurs interagissent au quotidien avec des nombreux sites sécurisés par un mot de passe, avec des moyennes variant entre 8 et plus de 25 sites en fonction sécurité, tant en quantité qu'en variété, les personnes, n'ayant pas forcément une bonne représentation des enjeux liés à la sécurité, ont tendance à limiter les couts en matière de mémorisation grâce à des stratégies de contournement, pas toujours appropriées aux contraintes de sécurité liées à la gestion des données personnelles (Norman, 2009). En effet, de malgré le nombre grandissant de services sécurisés, le nombre de mots de passe reste, quant à lui, limité (Gaw & Felten, 2006 ; Norman, 2009 ; Choong et al., 2014).On comprend donc que l'activité réelle d'authentification des utilisateurs de services en ligne s'éloigne des prescriptions parfois complexes liées à la sécurisation des données personnelles sur Internet. Il apparaît donc nécessaire de mieux comprendre cette activité d'authentification, d'en saisir les déterminants et les enjeux, afin de développer des systèmes de sécurisation des données personnelles pertinents.

Dans cet article, nous interrogeons spécifiquement les stratégies mises en œuvre dans la création, la rétention et la gestion des mots de passe, pour des utilisateurs tout-venants. Il s'agit d'une première étude qualitative préliminaire réalisée dans le cadre du projet HSA®, qui vise à concevoir et tester un nouveau système d'authentification graphique (Salembier et al., 2016). Sur base d'entretiens et d'un questionnaire, nous identifions les modalités et la diversité à l'œuvre dans l'activité de gestion des identifiants de connexions, et proposons un modèle compréhensif. Ce modèle vise à fournir des éléments de réflexion pour la création de nouvelles formes d'identification et de sécurisation des transactions sur Internet.

2 MÉTHODOLOGIE

Afin de recueillir des données sur l'activité d'authentification nous avons interrogé 11 personnes volontaires (5 femmes, 6 hommes) âgés de 20 à 54 ans (moyenne : 35) de différents profils professionnels (étudiants, graphiste, psychologue, chef d'entreprise, etc.). Lors des entretiens, d'une durée moyenne de 35 min (min : 22 ; max : 54), les participants sont invités à verbaliser leurs usages des différents systèmes d'authentification auxquels ils sont confrontés suivant deux thématiques :

- Le recensement des usages « Pourriez-vous me parler des différents services et outils que vous utilisez dans votre quotidien qui nécessitent un mot de passe ou un autre système d'authentification pour y accéder ? »

- Les incidents critiques rencontrés (Flanagan, 1954 ; Hughes, Williamson & Lloyd, 2007). Pourriez-vous me faire part de vos expériences vécues durant lesquelles vous avez été confronté à des difficultés en lien avec vos services et appareils protégés par un système d'authentification ? »

En amont de l'entretien, nous informons les participants sur le sujet de l'étude et leur demandons de retrouver des traces de leur activité (carnet, fichier Excel, Word, documents administratifs, notes informatiques, etc.) auxquels ils peuvent se référer en cours d'entretien, et de commencer à réfléchir à des événements marquants positifs ou négatifs en lien à la gestion de leurs mots de passe afin de faciliter l'évocation des incidents critiques. Lors de l'entretien, qui se déroule au domicile ou sur le lieu de travail du participant, ce dernier est encouragé à utiliser tout support (traces de son activité) aidant à se remettre en situation afin d'illustrer son propos avec des exemples concrets.

Pour permettre des verbalisations au plus près du réel, nous utilisons une panoplie de relances visant à ramener le propos sur des éléments très concrets de l'activité, telles que :« Auriez-vous des

exemples précis? », « Prenez votre temps, laissez l'événement revenir », ou encore « Vous rappelez-vous la dernière fois où vous êtes allé sur... ? », etc. (Vermersch, 1994).

Dans les sections suivantes, nous détaillons les résultats obtenus sur base des entretiens (nous indiquons entre parenthèse le nombre de répondants ayant évoqué chaque sujet) , et illustrons nos analyses par des extraits d'entretien quand approprié.

3 L'ACTIVITÉ D'AUTHENTIFICATION

L'activité d'authentification ne consiste pas uniquement à entrer ses identifiants (couple nom d'utilisateur + mot de passe) et de valider. En nous basant sur les types d'actions et d'activités que les participants évoquent dans la description de leurs stratégies, activités routinière et incidents, nousconstatons que l'activité d'authentification regroupe deux grandes types d'activités que sont la gestion des identifiants et l'accès à ces identifiants., qui peuvent elles-mêmes être subdivisées : création des identifiants, recherche active, création de traces, etc. (voir figure 1)

Ces deux grands types d'activités se déroulent en parallèle et entretiennent des liens mutuels : il n'y a pas d'avant, de pendant ou d'après, c'est lorsque les usagers sont confrontés à une situation d'authentification qu'ils créent, enregistrent et gardent des identifiants. De même, c'est lorsqu'ils sont confrontés à une situation d'authentification qu'ils entrent, vérifient ou modifient leurs identifiants. La gestion et l'accès aux identifiants sont intimement liés, des stratégies de gestion des identifiants influençant les stratégies possibles de récupération, et inversement.

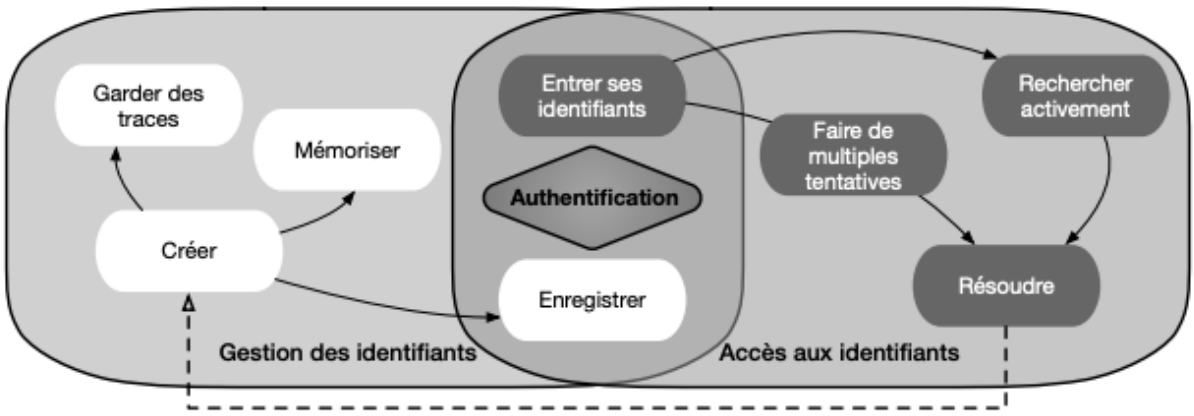

Figure 1. Modèle systémique de l'activité d'authentification

Ci-dessous nous détaillons chacun des éléments u modèle.

3.1 La gestion des identifiants

Comme nous l'expliquions précédemment, le nombre de mots de passe par utilisateur est limité. Un certain nombre de stratégies sous-tendent la gestion de ces identifiants, afin de trouver un bon compromis entre facilité d'accès et contraintes de sécurité.

3.1.1 Créer des identifiants

Lors de la création d'un compte, la première étape consiste à créer un nom d'utilisateur ou, dans la plupart des cas, à choisir une l'adresse e-mail. On constate que la plupart des utilisateurs (6 /11) ont plusieurs adresses e-mail auxquelles sont associés des statuts (poubelle/spam, culture, travail, etc.).

« *Apple, Gmail ou Hotmail. Donc Gmail c'est pour les choses importantes et le Hotmail c'est pour les choses ou il n'y a pas d'importance sur les données sensible*. » (E09)

La deuxième étape consiste à créer le mot de passe. Pour ce faire, quatre stratégies sont évoquées par les participants :

(1) Réutiliser un mot de passe existant

La réutilisation des mots de passe pour plus d'un site est très répandue (9/11), ceci afin de limiter l'impact sur la mémoire. « *Ça va être hyper simple, la plupart de mes mots de passe... j'utilise souvent les 2 mêmes.* » (E05).

(2) Réutiliser un mot de passe existant en le complexifiant légèrement

Lorsqu'ils sont confrontés à des sites dont les contraintes de sécurité sont plus importantes, ou à la suite d'un soupçon de piratage sur le compte concerné. «[Le mot de passe] *est bien parce que c'est un mot de passe avec 5 chiffres, plein de lettres et tu peux mettre une majuscule et un caractère spécial*. » (E04)

(3) Créer un nouveau mot de passe de toutes pièces

Nous observons trois principales techniques des créations : racine (a.) (utilisation d'une base identique), algorithmique (b.) (les mots de passe sont construits de façon similaire) et indicé (c.) et la mémorisation du mot de passe. C'est une manière pour la personne de favoriser l'utilisabilité du système en facilitant la mémorisation via des mécanismes mnémotechniques.

En marge de ces trois stratégies, les participants mobilisent aussi des méthodes de création ad hoc (d.), notamment pour des sites ou applications qu'ils considèrent comme plus sensibles. On constate donc, à l'instar des adresses e-mail, des statuts différents pour des mots de passe, en fonction du type de contenu qu'ils protègent (importance, nature du contenu, etc.) (4/11).

(a.) « *Par exemple pour FB c'est Txxx, pour tout ce qui est de ma boite mail c'est Txxx1 pour Soundcloud c'est aussi des Txxx1 donc tout ce qui est musique. Ma téléphonie c'est Txxxx12 parce que là c'est plus complexe au niveau des demandes pour les mots de passe*. » (E05)

(b.)« *Il faut que ce soit à minima toujours dans le même ordre pour m'y retrouver. Bon, je peux te le dire aussi parce que moi ça me gêne pas, souvent, j'aime bien voyager donc je mets dans mon mot de passe, la prochaine ville dans laquelle je vais aller*. » (E08)

(c.) «*Je prends le nom du site avec la première idée qui me vient parce que quand je ne m'en rappellerais plus ce sera celle-là qui reviendra. Et du coup, je rajoute des chiffres, toujours les mêmes. Mais qui peuvent aller de 2 à 6 en fonction de la longueur du nom du site* ». (E07)

(d.) « *Je le fais à l'instinct, à l'instant t, je réalise pas les conséquences parfois d'un mdp que je creé pas forcément facile à mémoriser*. » (E08)

(4) Utiliser la création automatique de mot de passe par le navigateur

L'utilisation de logiciel prenant en charge les activités de gestion des identifiants et d'authentification n'a été évoquée explicitement par aucune des personnes interrogées. Cependant, en marge des entretiens, plusieurs autres personnes nous ont fait état d'utilisation de ces fonctions.

Les utilisateurs peuvent donc, en fonction de facteurs personnels (habitudes, préférences, connaissances, etc.) et situationnels (types de site, sensibilité des données protéger, éléments de contexte, etc.) créer leurs mots de passe en suivant différentes stratégies (racine, algorithmique, indicée, réutilisation, complexification) afin de s'adapter aux contraintes de sécurité qu'impose l'activité d'authentification tout en poursuivant leur activité en cours de manière fluide.

3.1.2 Garder des traces

Les utilisateurs conservent des traces de certains mots de passe sur des supports externes de différents types (papier, téléphone, ordinateur, etc.) et sous différentes formes (entier, associé au nom

d'utilisateur, un indice). Cette conservation externalisée des identifiants implique un retour aux traces lors de l'authentification, de façon systématique ou lors de difficultés. Ces ressources externes sont donc créées dans cet esprit. Nous constatons deux grands types de fonctionnement : le « sous la main » (a.) (conserver les identifiants de sorte à qu'ils soient accessibles lors de l'activité réalisée) et l'archivage (b.) (conserver les documents ou de noter les mots de passe en les regroupant).

(a.) « *J'ai dû créer mon dossier et du coup ils m'ont demandé si je voulais enregistrer mon mot de passe et j'ai dit non donc du coup je l'ai noté parce que ça génère automatiquement un identifiant et un mot de passe et j'ai mis le papier sur mon pc parce que je vais juste en avoir besoin pour la période d'inscription.* »(E01)

(b.) « *Et tu gardes où tes papiers ? - Dans une mallette qui est cadenassé mais la clé est dans l'armoire.*»(E03). « *Ah oui aussi j'oubliais j'ai aussi un petit carton (…) où il y a un peu tous les mots de passe peu utilisés, genre les impôts, la CAF, AMELI, c'est des trucs déjà pré-faits qu'on t'envoie, donc je les ai notés et planqués* » (E07).

Outre ces deux modes, les utilisateurs, collectionnent également des traces sans tri particulier en conservant un email ou un document, sans y prêter trop d'importance avant d'en avoir l'utilité.

3.1.3 Enregistrer les identifiants

Les utilisateurs ont la possibilité d'enregistrer les identifiants. La majorité des personnes (9/11) enregistrent leurs mots de passe sur le navigateur pour tous les sites sauf ceux permettant d'accéder à de l'argent et 8 d'entre eux utilisent également des applications mobiles où les identifiants sont enregistrés pour un bon nombre de services. « *Oui, la plupart du temps j'enregistre sauf pour des choses sensibles où il faut payer avec sa carte bancaire par exemple*. » (E10)

La distinction entre « garder des traces » et « enregistrer » tient essentiellement aux modes de récupération : en cas d'enregistrement, la personne n'aura pas besoin de rechercher ses traces lors de l'authentification, la connexion étant automatique ou nécessitant tout au plus de sélectionner le remplissage automatique. Il existe plusieurs manières d'enregistrer ses identifiants : grâce au navigateur internet, aux applications, aux sites internet avec la fonction « se souvenir de moi » ou « rester connecté ».

À noter que pour la conservation et l'enregistrement, l'activité qui se déploie est grandement influencée par la situation et les contraintes contextuelles. Par exemple, E07 exprime choisir ses stratégies de conservation et d'enregistrement en fonction de la qualité de services perçue des différents supports (tablettes, smartphone, ordinateur). E08, également, rapporte une séparation très marquée entre le monde professionnel et le monde personnel quant à ses modes de création et de conservation de mots de passe.

3.2 Accès aux identifiants

3.2.1 Entrer ses identifiants

Lorsque confronté au service concerné, l'utilisateur doit retrouver ses identifiants et les encoder.

Il va dès lors soit se rappeler les identifiants mémorisés, soit les retrouver dans les traces préalablement construites. Certains participants évoquent le caractère incarné et automatique du rappel de certains mots de passe : les personnes se souviennent du « pattern » sur le clavier.

« On nous impose d'avoir 8 chiffres pour le code d'accès et donc là, j'utilise une date clef pour moi et je mets les chiffres à l'envers mais c'est tout le temps le même. [...] Mais bon c'est étonnant parce qu'à la fin tu ne regardes même pas ce que tu fais, tu tapotes le code ». (E08)

Néanmoins, lorsque les identifiants sont incorrects, les usagers développent des stratégies pour se connecter.

L'analyse des 37 incidents critiques montre que les problèmes portent tous sur la difficulté de se souvenir de l'association entre le mot de passe, l'identifiant et le site internet, mais les stratégies de résolution mobilisées diffèrent en fonction des personnes et des situations. Nous identifions 3 types de réactions face aux difficultés d'authentification. Généralement, l'utilisateur va dans un premier temps explorer plusieurs combinaisons d'identifiants (faire de multiples tentatives), puis cherchera dans ses papiers, ses emails, auprès de proche (recherche active), ou réinitialisera son mot de passe, contactera le service client si ses tentatives restent infructueuses (résoudre).

3.2.2 Faire de multiples tentatives

Lorsque la première combinaison nom d'utilisateur/mot de passe ne fonctionne pas, les utilisateurs peuvent essayer différentes combinaisons, en commençant par la plus plausible pour le service concerné. « *Euh, le mot de passe de mon pc là-haut vu que j'y vais plus beaucoup du coup je galère et je me dis c'est quoi le mot de passe, j'arrive je commence à faire le mot de passe habituel et puis je me dis mais non, parce qu'en fait celui-là c'est pas moi qui l'ai créé parce que c'était l'ordinateur de ma mère et donc c'est devenu instinctif mais vu que je l'utilise de moins en moins vu que j'ai mon nouveau pc, donc j'ai des petits moments de bugs, mais ça dure pas bien longtemps.* » (E01)

3.2.3 Chercher activement

S'ils n'arrivent pas à se connecter ou s'ils n'ont pas mémorisé leurs identifiants par choix, les utilisateurs vont s'investir activement dans leur recherche, dans leur espace physique (papier, carnet, proches, etc.) ou numérique (email, logiciel de notes, galerie photo, répertoire de contacts, etc.). Il y a alors une mobilisation des ressources externes développées en amont.« *Bah c'est con, mais il y a 2-3 jours, un pote m'a demandé comment se connecter à la plateforme de l'école donc j'ai dû retourner tout mon appartement pour trouver le papier. Ses identifiants ne marchaient pas, il était pas sûr d'avoir noté les bons. Donc du coup je lui ai donné les miens. Mais les papiers sont soit là [une table] soit là-bas [une commode].* » (E05)

3.2.4 Résoudre

En fonction des situations, si les personnes sont pressées ou qu'elles n'ont pas envie de se lancer dans des investigations, elles vont alors réinitialiser leur mot de passe en répondant à des questions secrètes ou par l'envoi d'un e-mail sur l'adresse correspondante. Dans certains cas, les personnes appellent un service client ou un responsable du système informatique. Ce genre de comportements est aussi observé après que les utilisateurs aient essayé pendant un temps relativement long de se connecter par leurs propres moyens. Ici, ce sont les ressources proposées par le système qui sont mobilisées.

« *Donc la dernière fois il fallait que je revoie le papier, entre deux j'avais oublié le mot de passe que j'avais déclaré donc là j'ai pris mon téléphone et j'ai dit à la nana que j'avais plus aucune idée de ce qu'était mon mot de passe et qu'il fallait que je revoie le doc et elle m'a envoyé le doc.* » (E08)

4 L'AUTHENTIFICATION COMME UN COMPROMIS ENTRE SÉCURITE ET UTILISABILITÉ

Nous l'avons vu, les utilisateurs déploient un large nombre de stratégies et ressources au cours de l'activité d'authentification. Bien qu'il n'y ait pas de liens déterministes sur le choix d'une stratégie ou d'une autre pour la construction des identifiants, leur stockage et la résolution des problèmes d'authentification, nous pouvons identifier, à la lumière des entretiens, un ensemble de facteurs influençant l'activité d'authentification.

Fréquence d'utilisation du service

Il est possible de distinguer deux groupes de comptes qui impliquent des usages différents : les comptes utilisés fréquemment et les comptes utilisés plus occasionnellement. Pour le premier groupe, les utilisateurs seront plus enclins à utiliser des stratégies particulières de création de mot de passe et auront moins tendance à consulter des traces pour réussir leur connexion.

Type de service

Dans le même ordre d'idées, on constate que les utilisateurs distinguent deux types de services numériques : des services qui leurs sont "imposés" (services administratifs notamment) et des services qu'ils décident spontanément d'utiliser (réseaux sociaux, sites d'e-commerce, etc.), avec un investissement moins important dans la sécurité des services « imposés ».

La sensibilité perçue des données protégées

Pour tous les utilisateurs interrogés, les données bancaires sont les plus sensibles et donc demandent une plus grande protection. De plus, certains perçoivent comme particulièrement sensibles, leurs adresses e-mails car au cœur d'une grande partie de leur réseau, ou encore les réseaux sociaux car ils véhiculent leur image. Ils créent donc des mots de passe plus complexes ou limitent la conservation de traces de leurs identifiants quand ils considèrent les données comme sensibles.

Les caractéristiques propres à chaque service numérique

Premièrement, certains services numériques disposent de mécanismes de sécurité supplémentaires. Ces contraintes supplémentaires imposées par les dispositifs ajoutent une perception de la sécurité. Les utilisateurs, compte tenu de ces garanties de sécurité, ont tendance, de leur côté, à générer des mots de passe plus simples, plus faciles à mémoriser et récupérer.

Deuxièmement, les utilisateurs vont également considérer les possibilités de réinitialisation de mot de passe offertes par le système. Aussi, quand la réinitialisation est aisée et automatisée, cette stratégie de résolution va être plus rapidement privilégiée.

Enfin, Les exigences des systèmes d'authentification quant à la création du mot de passe (minuscule, majuscule, caractères spéciaux, etc.) conduisent les personnes à complexifier leurs mots de passe existants. Ces contraintes peuvent les obliger à créer des mots de passe inhabituels, s'écartant de leurs routines de création, et étant de ce fait plus difficiles à mémoriser.

La perception de ses capacités mnésiques

Les utilisateurs ont conscience des limites de leurs capacités mnésiques, ils intègrent donc ce facteur dans leur choix en matière de création et conservation de mots de passe. De fait, ils privilégient des mots de passe facilement mémorisables et conservent des traces en cas de mots de passe trop complexes, notamment les mots de passe imposés auxquels il est difficile d'attribuer un sens pour faciliter la mémorisation.

L'objet de l'activité future ou présente

Les stratégies de conservation sont influencées par les projections que font les utilisateurs des activités dans lesquelles ils seront engagés quand ils auront besoin de leurs identifiants. Ceci est particulièrement perceptible avec l'idée du "sous la main" décrite au point 3.2.1 (garder des traces). L'activité présente influence également le comportement des utilisateurs. Ceux-ci, lors d'achats en ligne sur un nouveau site par exemple, passent rapidement l'étape de création de compte en décidant d'un mot de passe dans l'instant afin de continuer l'activité dans laquelle ils étaient lancés.

5 DISCUSSION

Bien qu'il existe des standards relativement bien définis en matière de règles de création et de conservation des identifiants (complexité des mots de passe, utilisation d'un mot de passe par site ou service, non-conservation ou protection importante des traces, etc.), et bien que ces règles soient régulièrement rappelées lors de la création d'identifiants, l'activité réelle des utilisateurs s'éloigne de ces prescriptions. Nos résultats sont cohérents avec ceux rapportés par Stobbert & Biddle (2014).

Nous montrons d'une part qu'il existe plusieurs stratégies complémentaires de création, de rétention et de rappel des identifiants. Les utilisateurs, dans une volonté de garder le contrôle sur leur sécurité, mobilisent des stratégies circonstancielles ou habituelles, dans la création et la réutilisation de leurs identifiants. D'autre part, nous constatons qu'un faisceau de déterminants influencent le choix de ces stratégies, et que ces facteurs s'organisent autour d'un compromis entre sécurité et utilisabilité. Ce compromis est consciemment pris en compte par les utilisateurs. Cependant, tout en s'inquiétant de la sécurité de leurs données, la majorité des utilisateurs ne définissent pas clairement la menace et n'apprécient pas les différences existant en matière de menace en fonction des services utilisés (Norman, 2010 ; Stobbert & Biddle, 2014). Ceci permet, en partie, d'expliquer la faible adoption des dispositifs de gestions d'identifiants (Gaw & Felton, 2006 ; Alkaldi et al. 2018) ou d'alternative comme la biométrie (Florencio and Herley, 2007), au privilège des mots des passe, malgré les contraintes.

Nos résultats nous permettent de penser certaines recommandations pour l'amélioration de l'utilisabilité des systèmes d'authentification que nous détaillerons dans l'article.

Contexte similaire de création et d'authentification

Pour soutenir la stratégie de création « indicée » décrite plus haut, nous suggérons de proposer des indices lors de la création du mot de passe (sons, images, etc.) et de les présenter de nouveau lors de l'authentification. De la même manière, présenter les contraintes de création des mots de passe lors de l'authentification (caractères spéciaux, nombre de caractère, etc.) permettrait de faciliter le rappel des conditions qui ont guidé la création du mot de passe et de simplifier le rappel pour chaque site.

Regroupements des sites.

On observe des comportements différents suivant la sensibilité perçue des données, l'importance ou le type du service. Ceci est intrinsèquement lié aux difficultés de compréhension et de confiances qu'on les utilisateurs dans ces système. Nous suggérons donc de proposer plusieurs intermédiairessécurisés d'authentification permettant de regrouper les services numériques en fonction de critères pertinents pour les utilisateurs, et sur leurs exigences de sécurité (i.e. plus de sécurité pour les sites stockant des données bancaires, donc plus de contrainte pour la connexion). Ceci contrairement aux systèmes actuels d'authentification uniques (single sign-on) (e.g. Facebook ou Google) se confrontant directement au problème de confiance des utilisateurs.

Double authentification

La réinitialisation du mot de passe, bien qu'utilisée la plupart du temps en dernier recours, peut néanmoins être mobilisée de manière systématique. Ceci est notamment le cas pour les sites dont la sensibilité perçue est faible. Cependant, la réinitialisation met en péril l'utilisabilité du système, un changement de mot de passe impose un nouvel investissement dans la création, et peut entrer en interférence avec les anciens identifiants (Chiasson et al., 2007). Nous encourageons la double authentification, comme le propose certains services (e.g. paiements bancaires). L'utilisateur associe une adresse email (par exemple) à son compte, au moment de la connexion, l'utilisateur entre son nom d'utilisateur et reçoit un e-mail. Il se connecte en cliquant sur un lien dans le message.

La gestion des identifiants de connexion est le résultat d'un compromis entre l'utilisabilité des systèmes et les contraintes de sécurité. La présente étude, et les recommandations ci-dessus, adressent essentiellement la première partie de cette équation, mais doivent évidemment être discutées et affinées en regard des contraintes spécifiques à la sécurité informatique.

6 BIBLIOGRAPHIE

Alkaldi, N., & Renaud, K. (2019, January). Encouraging Password Manager Adoption by Meeting Adopter Self-Determination Needs. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Chiasson, S., Biddle, R., & van Oorschot, P. C. (2007, July). A second look at the usability of click-based graphical passwords. In Proceedings of the 3rd symposium on Usable privacy and security (pp. 112). ACM.

Choong, Y.-Y., Theofanos, M. & Liu, H.-K. (2014). United States Federal Employees' Password Management Behaviors : a Department of Commerce Case Study. National Institue of Standards and Technology.

Norman, D. A. (2010). THE WAY I SEE IT When security gets in the way. Interactions, 16, 6 : 60-63.

Flanagan, J. C. (1954). The critical incident technique. Psychological bulletin, 51(4), 327.

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. In Proceedings of the 16th international conference on World Wide Web (pp. 657-666). ACM.

Gaw, S., & Felten, E. W. (2006, July). Password management strategies for online accounts. In Proceedings of the 2nd symposium on Usable privacy and security (SOUPS 2007) (pp. 44-55). ACM. Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with computers*, *23*(3), 256-267.

Hughes, H., Williamson, K., & Lloyd, A. (2007). Critical incident technique. Exploring methods in information literacy research, 28, 49-66.

Riley, S. (2006). Password security: What users know and what they actually do. Usability News, 8(1), 2833-2836.

Salembier, P., Zouinar, M., Héron, R., Mathias, C., Lorant, G., & Wary, J. P. (2016, Octobre). Etudes expérimentales d'un système d'authentification graphique basée sur la catégorisation sémantique. Dans Actes de la 28ième conférence francophone sur l'Interaction Homme- Machine (IHM 2016) (pp. 134-143). ACM.

Stobert, E., & Biddle, R. (2014). The Password Life Cycle: User Behaviour in Managing Passwords. In 10th Symposium On Usable Privacy and Security (SOUPS 2014) (pp. 243-255). Usenix.

Vermersch,P.(1994).L'entretiend'explicitation(Vol.2003).Paris:Esf.