Mots de passe, le mieux est l'ennemi du bien.

1. Les bases

Passage obligatoire, rappelons l'ensemble des exigences d'un mot de passe fort :

1 - au moins 8 caractères (10 recommandés) ;

2 - au moins un élément de chaque groupe de caractères (minuscules, majuscules, numériques, spéciaux) ;

3 - aucun rapport psycho-social évident avec le propriétaire (prénom, nom du chien, etc.), l'endroit où il est utilisé (AdminERP, Facebook01, etc.) ou bien l'entreprise (NSA2k15, AdminCodeNucleaire, etc.) ;

4 - aucun mot issu d'un dictionnaire, même sous forme dégradée (l33t, langage SMS, etc.) ;

5 - n'est pas réutilisé ailleurs ;

6 - n'est inscrit nulle part.

Note : Si le mot de passe doit parfois être utilisé depuis une machine tierce (et possiblement à l'étranger), évitez d'y inclure des caractères absents du clavier international (é, ù, ç, etc.).

Exemples :

Ty6?/K32vE

_Hjk[20%2/

2. La théorie

La sécurité d'un mot de passe est liée à la difficulté qu'éprouvera un attaquant pour le découvrir. Pour calculer le nombre théorique de mots de passe que l'attaquant devra essayer, on utilise la formule :

XN+ X(N-1)+ X(N-2)+⋯+ X + 1

Où X est le nombre de caractères autorisés et N la longueur du mot de passe.

Ainsi un mot de passe de 4 caractères, composé uniquement de minuscules (26 lettres), demande 264+263+262+26+1 essais au maximum (si le mot de passe est *zzzz*).

Cependant, comme un attaquant essaiera probablement des mots de passe à partir d'une certaine longueur et que ça ne change pas réellement l'ordre de grandeur, on considère que le nombre de combinaisons à calculer est de l'ordre de X^N.

Analysons la complexité « théorique » de nos mots de passe forts. Ils utilisent 4 ensembles :

1 - les minuscules (26 éléments) ;

2 - les majuscules (26 éléments) ;

3 - les chiffres (10 éléments) ;

4 - les caractères spéciaux (considérons que l'on utilise les caractères suivants : &"-)'=#{[|@]`+}_~$%*,?;.:/!§) (28 éléments).

Pour chacun des 10 caractères, il y a 90 symboles possibles (26+26+10+28), soit : 9010 mots de passe pouvant être générés. Cela représente, pour un attaquant, 34 867 844 010 000 000 000 possibilités à tester (35 trillions) dans une attaque par force brute*****. Dans le cas d'une attaque en ligne, sur un site Web distant, pouvant tester 1000 mots de passe/seconde. Il faut à l'attaquant environ 35 billiards de secondes (1 milliard d'années) pour essayer toutes les possibilités.

Note : ******* *Bien sûr, rien ne dit que l'attaquant ait pu avoir connaissance de la taille du mot de passe, des symboles qu'il utilise, etc. Mais nous utilisons toujours l'approche de la borne inférieure (*lower bound*) dans cet article. Elle consiste à évaluer la sécurité dans le pire des cas : on sait que l'attaquant pourrait connaître moins de choses sur le mot de passe, mais dans tous les cas, il ne pourrait en savoir plus sans connaître le mot de passe lui-même. Or, comme le dit Karl Wiberg, dans un ascenseur il est plus utile de connaître le nombre de personnes transportables en sécurité que le nombre de personnes nécessaires pour faire rompre le câble* **[13]**.

3. La vraie vie

Mais il existe au moins deux raisons pour lesquelles la théorie c'est bien surtout en théorie.

3.1 Raison 1 : La mémoire

Une fois le mot de passe ultime créé, encore faut-il s'en souvenir. Or les mots de passe suivants sont très difficilement mémorables...

Ty6?/K32vE

_Hjk[20%2/

Lorsqu'une personne créera un mot de passe fort selon les règles énoncées plus haut, elle tentera de le rendre mémorisable en dérogeant, en partie, aux exigences 3 et 4. Ainsi, dans les faits, nos mots de passe « forts » ressemblent plutôt à ceci :

S4ng0ku-89

Must4ng/31

Dans une large majorité des cas **[1][12]**:

1 - la majuscule est au début ;

2 - le(s) chiffre(s) à la fin, souvent basés sur une date de naissance, un chiffre fétiche ou un code postal ;

3 - le caractère spécial juste avant ;

4 - il s'agit d'un mot existant, mais dégradé (ici Sangoku, Mustang).

3.1.1. Les motifs

Les mots de passe sont le plus souvent constitués d'un « motif » reconnaissable. Ils sont bien connus des attaquants :

1 - les séquences : agencement du clavier, alphabet, etc. (CDEFG, 45678) ;

2 - les spatiaux : agencement des touches sur le clavier (3EDC, Azerty) ;

3 - les dictionnaires : mots connus, variantes avec majuscules ou substitution lettre/chiffres, noms propres, etc. (M4m4n, Z1danE) ;

4 - les dates (1979, 98).

Ces motifs s'agencent suivant un nombre relativement limité de schémas***** (exemple : séquence + caractère spécial + date). Dès lors, en combinant ces motifs connus avec un minimum de force brute, l'entropie des mots de passe chute significativement.

*Note: ******L'outil suivant analyse les motifs présents dans le mot de passe soumis : http://www.takecontrolbooks.com/resources/0148/zxcvbn/ (basé sur un dictionnaire anglais)*

Ce type d'attaque ne permet pas de découvrir les rares mots de passe qui échappent à ces schémas, mais découvre beaucoup plus rapidement ceux qui y sont soumis (la majorité).

On estime que la présence de motifs fait chuter l'entropie à 28 bits **[2][3][13]** (chiffre en grande partie empirique). Le nombre d'essais à tester est donc d'environ 1 milliard (3 jours avec 1000 mots de passe testés par seconde).

De manière globale, les statistiques sur les mots de passe sont des armes particulièrement efficaces pour les hackers. Par exemple, il est très intéressant de relever des informations macroscopiques **[4][7][8]** : la taille moyenne des mots de passe, la distance de Hamming moyenne entre les mots de passe et les mots du dictionnaire, etc.

3.1.2 La racine

En fait, les briseurs de mots de passe actuels n'utilisent quasiment jamais la force brute pure. Ils privilégient autant que possible les approches intelligentes.

Le mot de passe typique contient toujours une « racine » qui est un mot prononçable (afin d'être mémorisable), plus ou moins déformé, auquel on attache un suffixe (dans 90% des cas) et/ou un préfixe (dans 10% des cas) **[1]** :

Tonnerre => T0NnR => T0NnR/90

Une approche efficace consiste à utiliser une base de 1000 mots de passe communs (123456, bradpitt, iloveyou, etc.) à laquelle on attache les 100 suffixes les plus communs (1, 69, abc, !, etc.).

Des études, menées dans des entreprises, montrent qu'il est déjà possible de briser ¼ des mots de passe avec ce procédé qui ne coûte pourtant que 100 000 essais (soit 100 secondes dans notre scénario d'attaque) **[1]**.

En ajoutant des techniques de dérivation de la racine (tonnerre => T0NnR) et d'autres astuces similaires, il est possible de briser entre 90 et 60% des mots de passe, et ce, en quelques heures **[1]**.

L'approche par force brute (qui sert d'étalon de mesure dans cet article) n'est que l'attaque la moins efficace.

Comme le dit Bruce Schneier, tout ce qui peut être mémorisé, peut être craqué. Pour vous remémorer votre mot de passe, vous suivez une logique dans sa construction. « Logique » entraîne « absence d'aléa » et donc perte d'entropie.

Si vous utilisez des mots de passe réellement forts, générés aléatoirement, vous aurez 65 bits d'entropie et serez à l'abri des attaques. Mais vous pourrez difficilement mémoriser un tel mot de passe, encore moins plusieurs.

3.2 Raison 2 : Les canaux auxiliaires

Admettons que vous soyez un utilisateur chevronné, qui génère aléatoirement des mots de passe forts. Si nous admettons également que vous n'avez pas le syndrome d'Asperger alors vous rencontrez le fameux problème de la mémoire explicité plus haut et devenez vulnérable aux attaques par canaux auxiliaires.

L'attaquant doit essayer tous les mots de passe jusqu'à en trouver un qui produise le même condensat que le vôtre… Ou bien il peut le lire sur le post-it que vous avez collé sur votre écran pour vous en rappeler.

3.2.1 L'entreprise

Vous êtes recruté dans une grande entreprise (qui n'est pas à la pointe de l'état de l'art en matière de SSO), on vous a créé 7 comptes desquels vous devez changer les mots de passe associés (par ex. l'ERP, le mail, quelques applications métiers, etc.). Enfer et damnation, ils ont des exigences différentes (8 caractères pour l'un, 12, avec 2 chiffres minimum pour l'autre, etc.).

Le coup de grâce intervient lorsque ces mots de passe arrivent à expiration…de façon décalée (expiration tous les 60 jours, pour d'autres tous les 90, etc.). Raffinement suprême : interdiction que le nouveau mot de passe soit trop proche du précédent (pour les petits malins qui utilisent un chiffre incrémental à la fin).

Qui pourrait se voir reprocher de ne pouvoir retenir autant de mots de passe sans les noter sur un joli fichier mot_de_passe.xls ?

3.2.2 La sphère privée

Qui n'a pas ressenti l'énervement légitime occasionné lorsqu'un site ne nous laisse PAS utiliser notre mot de passe ultra-sécurisé (parce qu'il n'accepte pas certains caractères spéciaux ou bien qu'il demande au moins deux chiffres). On se retrouve alors à le défigurer pour le faire coller aux attentes (hélas, on l'oublie assez vite, nous obligeant à utiliser la fonction d'oubli du mot de passe à chaque connexion).

Heureusement nos navigateurs les retiennent aussi pour nous. Mais sachant que cette base de mots de passe est consultable via les paramètres du navigateur, ils sont accessibles à tous si vous ne verrouillez pas votre session et ne chiffrez pas votre disque dur (la vieille technique du Live-CD).

Cela concerne aussi ceux qui sauvegardent leurs mots de passe en se les envoyant par mail (ou en enregistrant un brouillon).

3.2.3 La délégation de confiance

Chaque fois que vous vous enregistrez sur un site, vous lui faites confiance implicitement pour protéger votre mot de passe. Si le site stocke ce dernier de façon non sécurisée, un vol de cette base permettra aux attaquants de le connaître directement. S'il est stocké de façon sécurisée (condensat), il leur faudra (seulement) des semaines/mois pour y parvenir*****.

*Note : ***** En effet dans une attaque distante depuis Internet, l'attaquant pouvait tester 1000 mots de passe/seconde. S'il possède les condensats « chez lui », il n'est plus soumis à la vitesse du réseau et du serveur distant, on parle alors d'ordre de grandeur de 3-30 milliards de mots de passe/seconde **[5] [6]**.*

3.2.4 L'effet boule de neige

Sachant que la plupart des sites stockent votre adresse mail et votre mot de passe (de façon sécurisée ou pas), que votre adresse mail fait souvent office de login (Facebook, PayPal, etc.) et que vous utilisez généralement le même mot de passe partout **[8]**, le pirate ayant pu exfiltrer des données contenant votre mot de passe et votre adresse e-mail, peut alors très probablement :

1- accéder à votre boite mail avec le mot de passe volé ;

2- accéder aux sites où vous utilisez votre adresse mail comme login et votre mot de passe habituel ;

3- accéder aux autres sites en profitant de la fonction de réinitialisation du mot de passe.

De surcroît, le pirate n'est pas le seul à craindre. Lorsque vous vous inscrivez sur un site douteux (téléchargement, moyen révolutionnaire pour gagner de l'argent avec une méthode très simple et en très peu de temps, etc.) vous renseignez votre adresse mail et un mot de passe sans moyen de savoir ce qu'en fera le propriétaire du site. Qu'est-ce qui l'empêche lui-même d'aller consulter votre compte ? L'altruisme ?

3.2.5 La question « secrète »

Sur certains sites, une question secrète permet de réinitialiser votre mot de passe si vous l'avez perdu. Si votre mot de passe est « _73GHd5,djh », mais que votre question secrète est « Quel est mon signe astrologique ? » n'importe quel bélier comprendra qu'il ne faudra pas plus de 12 essais à un attaquant pour accéder à votre compte.

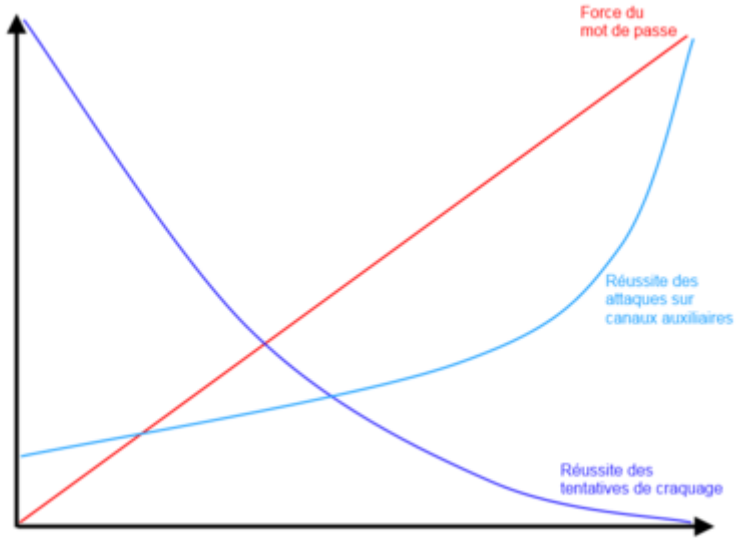
Ce comportement tend à décliner au profit des fonctions de réinitialisation du mot de passe, mais il est loin d'avoir disparu.

4. Constat

K04l498! est mémorisable, mais n'est pas un mot de passe fort. 0-fjq;7J!HF0jn est un mot de passe fort, mais n'est pas mémorisable.

K04l498! peut être découvert en utilisant des attaques malignes basées sur la racine (ici koala) en quelques jours. 0-fjq;7J!HF0jn peut être découvert en fouillant vos tiroirs ou votre bureau.

Donc plus un mot de passe est fort, moins il est exposé au craquage de mot de passe, mais plus il est exposé aux attaques par canaux auxiliaires :



Dans les faits, aucun niveau de complexité ne permet de rendre votre mot de passe inviolable.

5. Que faire ?

5.1 Les sphères de criticité

Première réelle bonne pratique, trop largement sous-estimée : les sphères de criticité. Le principe étant que : « Surtout, si vous avez créé un très bon mot de passe, NE L'UTILISEZ PAS PARTOUT !!! ».

5.1.1 Le principe

Regroupez vos comptes par ordre de criticité et utilisez un mot de passe différent pour chaque groupe. Ainsi la divulgation d'un mot de passe (forum en ligne par exemple) ne compromet pas les autres sphères plus sensibles (banque en ligne, mail, etc.).

Trois niveaux peuvent par exemple être définis :

5.1.1.1 Niveau 3 : mots de passe cloud non sensibles

Destiné aux services en ligne communs : forums, blogs, réseaux sociaux, etc. Utilisez-le si vous n'êtes pas sûr que le site ne lise/utilise pas vos mots de passe. Ou bien, si le site est tellement important qu'il subit de nombreuses attaques (PlayStation network, etc.) et qu'il y a donc une probabilité non négligeable que vos mots de passe soient un jour dérobés.

5.1.1.2 Niveau 2 : mots de passe cloud sensibles

Destiné aux services en ligne sensibles : mail, paiement, réseaux sociaux, stockage en ligne... Votre boite mail permettant de réinitialiser tous vos autres comptes (Facebook, Twitter, etc.) doit obligatoirement avoir un mot de passe différent de ceux-ci. Le mot de passe du site sur lequel vous effectuez un achat (eBay, etc.) ne doit pas être le même que votre moyen de paiement (PayPal, etc.).

5.1.1.3 Niveau 1 : mots de passe « offline »

Destiné aux supports physiques : compte utilisateur de votre ordinateur, mot de passe de chiffrement de votre disque dur, etc. L'objectif : qu'il se trouve uniquement dans la mémoire de votre machine et ne soit jamais présent sur des bases de données en ligne. Ainsi un attaquant doit pouvoir accéder physiquement à votre matériel pour le dérober.

Le milieu professionnel doit disposer de ses propres mots de passe (obligatoirement différents de ceux du privé) et ses propres sphères de criticité :

1 - offline ;

2 - services cloud internes (hébergés dans l'entreprise : interfaces métiers, de maintenance, mail, ERP, etc.) ;

3 - services cloud externes***** (hébergés sur Internet ou par un prestataire : possiblement mail, ERP, etc.).

Note : *******Il est évidemment du ressort de l'entreprise de communiquer à ses employés les services hébergés en interne et ceux qui sont externalisés. Il est également possible d'éviter que le service externe ait connaissance du mot de passe grâce aux mécanismes de* Single Sign On *(SSO).*

5.2 Les coffres forts numériques

Ces gestionnaires (appelés « trousseaux de clés » ou « coffres-forts ») retiennent tous vos mots de passe et sécurisent cette liste avec un mot de passe maître. Il ne vous reste donc qu'un seul mot de passe à mémoriser. Virtuellement, vous avez ainsi un niveau de sécurité quasi-parfait. L'ennui majeur réside dans le fait qu'il faut « faire confiance » à un gestionnaire de mots de passe pour protéger le sésame de toute votre vie numérique (risque de piratage, Patriot Act, etc.). L'ANSSI a certifié un certain nombre de solutions pour lesquelles le niveau de sécurité est important: http://www.ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/.

Saluons une initiative très intéressante de Manoé Zwhalen : Pa$$ware (ou Pa55ware) **[10]**.

Il s'agit d'un dispositif physique protégé par un code PIN (bloqué après 3 essais) et qui tape virtuellement les mots de passe pour vous (le projet est open source). Cette approche mériterait d'être plébiscitée et approfondie.

5.3 Les passe-phrases

Les passe-phrases répondent à un constat qui est que « complexité » ne signifie pas automatiquement « force » et vice-versa.

Par exemple :

gj8(&KsP05_, est plus complexe que ....Pouet....

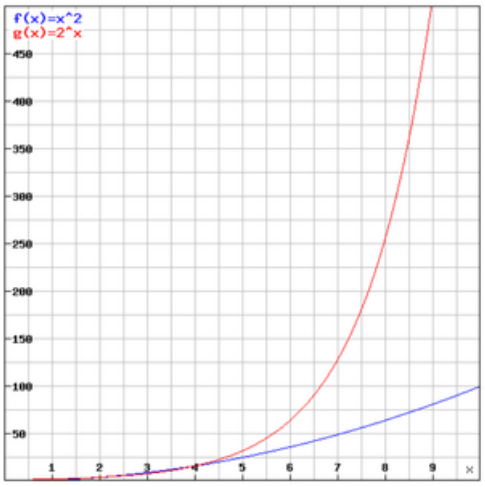
Pourtant ce deuxième mot de passe est 20 fois***** plus difficile à percer que le premier.

*Note : ***** Le premier contient tous les ensembles de symboles (90) et 12 caractères, soit 9012 possibilités : 282 429 536 481 000 000 000 000. Le second ne possède pas de chiffre, donc seulement 80 symboles possibles, mais 13 caractères de long, soit 8013 possibilités : 5 497 558 138 880 000 000 000 000 (19,47 fois plus).Même si ce second mot de passe est beaucoup moins complexe, qu'il possède moins d'entropie, l'attaquant n'en sait rien a priori. Ce mot de passe ne fait pas partie de la liste des plus fréquents, il ne fait pas partie du dictionnaire. Il possède bien un motif, mais il n'est pas commun du tout. «* Close only counts in horseshoes and hand grenades *». Aucune des attaques habituelles n'ayant réussi, l'attaquant est obligé d'utiliser une attaque exhaustive **[9]**.Bien entendu, si tout le monde se met à utiliser des mots de passe avec ce format, les attaquants adapteront les attaques par motifs.*

5.3.1 Quelques notions

Nous avons vu que l'on calcule la complexité d'un mot de passe avec la formule : X^N où X est le nombre de caractères autorisés et N la longueur du mot de passe. Donc, augmenter le nombre de symboles possibles fait grandir la base, tandis qu'augmenter la taille fait grandir l'exposant.

Or, mathématiquement, une augmentation de la base provoque une croissance géométrique (courbe bleue ci-après), tandis qu'une augmentation de l'exposant provoque une croissance exponentielle (courbe rouge) :



Déduction : à terme, si vous avez le choix entre augmenter la longueur du mot de passe ou le nombre de caractères autorisés, privilégiez toujours la longueur.

5.3.2 Le principe

Le principe de base est de prendre plusieurs mots au hasard, disons quatre pour les exemples suivants, puis les concaténer.

Par exemple : LutinPortableCameoGencive

Facilement mémorisable !

Facilement craquable ? Pas si sûr…

5.3.3 Robustesse théorique

Nous n'utilisons que des minuscules/majuscules, l'attaquant doit donc tester dans le pire des cas 5225 combinaisons. Comparons ce résultat à celui des mots de passe forts :

	Mot de passe fort	Passe-phrase
Combinaisons	90^{10}	52^{25}
Possibilités	34 867 844 010 000 000 000 (35 trillions)	7 944 811 378 381 907 919 170 379 739 856 654 861 074 432(8 septillions)
Entropie	65 bits	142 bits
Temps avant craquage	1 milliard d'années	200 quintillions d'années (10^{32})

L'avantage est évident*****.

Note : ******* *Arguons que la taille ne sera pas systématiquement de 25 caractères, cela dépend des mots choisis. Néanmoins à partir de 12 caractères (difficile de faire moins avec 4 mots), la performance reste supérieure à celle des mots de passe forts.*

Quittons maintenant le pays de la théorie, avec ses chats morts/vivants et concentrons-nous sur la réalité.

5.3.4 Qui dit succès, dit adaptation des hackers

Si les passe-phrases se démocratisent jusqu'à remplacer/égaler les mots de passe, les attaquants s'adapteront.

Les passe-phrases sont robustes du point de vue de l'attaque itérative, mais il existe d'autres attaques. En remarquant que les passe-phrases sont basées sur des mots existants, le hacker peut utiliser une attaque par dictionnaire.

Avec la méthode itérative, la passe-phrase PatteMeteoGilbertFaisan nécessite de tester **toutes les combinaisons des 52 symboles possibles pour les 25 caractères qui la composent**. Soit un ordre de grandeur de 5225. Mais si l'on change de paradigme en considérant que chaque mot utilisé est en fait un « caractère » et que pour chacun de ces caractères il existe un nombre fini de symboles possibles (les mots du dictionnaire), alors nous avons désormais à tester **toutes les combinaisons des 15000* symboles possibles (les mots du dictionnaire) pour les 4 caractères qui la composent**. Soit un ordre de grandeur de 150004.

*Note : ***** Concernant le nombre de mots dans le dictionnaire, le français usuel comprend environ 30 000 mots (dont 2/3 d'origine savante ou étrangère et 1/3 d'origine populaire). Bien que variable entre les langues, un noyau de 5000 mots permet généralement de couvrir les usages courants **[11]**. On peut estimer qu'avec un dictionnaire de 15000 mots, un attaquant possède de quoi craquer 90% des passe-phrases.*

Comme il a été dit précédemment, il faut toujours privilégier la longueur, or nous venons de la réduire de 25 caractères à seulement 4 (au prix d'une augmentation considérable des symboles possibles). Comparons :

	Attaque basique	Attaque par dictionnaire
Combinaisons	50^{25}	15000^{4}
Possibilités	7 944 811 378 381 907 919 170 379 739 856 654 861 074 432 (8 septillions)	50 625 000 000 000 000 (50 billiards)
Entropie	142 bits	55 bits
Temps avant craquage	200 quintillions d'années (10^{32})	1,6 million d'années (10^{6})

L'augmentation, drastique, du nombre de symboles possibles ne suffit clairement pas à compenser la perte de longueur, tout aussi drastique.

Telle quelle, cette méthode n'est pas suffisante de par sa faible résistance aux attaques par dictionnaire.

5.3.5 Mais nous pouvons être moins gentils

Pour dépasser les 65 bits d'entropie, l'attaquant doit être forcé d'utiliser un dictionnaire d'au moins 80 000 mots. Donc l'utilisateur doit puiser dans des sources plus variées en y ajoutant :

- la possibilité de mettre ou non une majuscule aux mots utilisés : multiplication par 2 du nombre de mots possibles. En ajoutant les déformations basiques de mot : maisoN, m4ison, etc., nous multiplions par 10 (minimum) ;

- les noms propres : Nintendo, OneDirection, etc. D'une personne à l'autre, les noms propres connus et utilisés varient considérablement (suivant les centres d'intérêt). Un dictionnaire les regroupant tous serait colossal.

- les différents jargons : argot, verlan, insultes, etc. que peu de dictionnaires en ligne contiennent ;

- les mots étrangers.

Le dictionnaire explose littéralement.

SarkoJambonGroovySkywalker est une passe-phrase facilement mémorisable. Pour la craquer, il faut un dictionnaire contenant les mots :

- français ;

- anglais ;

- issus de la culture cinématographique populaire (Skywalker) ;

- issus des personnalités françaises (Sarko).

Soit un nombre de mots compris entre plusieurs dizaines et centaines de milliers*****. En introduisant des déformations mineures, la passe-phrase conserve sa facilité de mémorisation :

Sarko!J4mboNgr00vySkywalker

Mais l'attaquant doit ajouter des déformations pour chaque entrée de son dictionnaire, ce qui fait croître démesurément le nombre de possibilités. L'entropie dépasse aisément les 100 bits.

*Note : ***** Cette estimation se base sur le pire des cas. C'est-à-dire celui où l'attaquant savait qu'il lui faudrait ces familles de mots. En pratique, l'attaquant est plus souvent obligé de miser sur un dictionnaire trop gros, en espérant qu'il contiendra, entre autres, les bonnes familles de mots.*

5.3.6 Conseils

L'objectif de la passe-phrase est d'être simplement mémorisable pour ne pas avoir à être notée sur un support physique.

Si l'attaquant utilise une méthode de craquage classique (itération par caractère), il n'a de toute façon aucune chance de succès. S'il utilise une attaque par dictionnaire alors la meilleure recommandation est : SORTEZ DU DICTIONNAIRE !

La protection suprême, pour une passe-phrase, est qu'il n'y ait aucune liste de mots au monde qui possède les 4 mots qui la composent*****.

*Note: ***** Ainsi, Jantealu, québlo, Kant et bicchiere n'existent très probablement pas ensemble au sein d'une seule liste de mots.*

La personnalisation de la passe-phrase est gage de difficulté pour l'attaquant, mais elle doit être savamment dosée. Utiliser exclusivement 4 mots ayant un rapport intime à l'utilisateur rendrait la passe-phrase vulnérable à l'ingénierie sociale*****.

*Note : * JackyTunningPSGBiere pourrait être percée en dressant le profil de la personne. L'attaquant déterminera une* short list *des mots qu'il a été susceptible d'utiliser (pour notre ami Jacky, l'attaquant listerait les mots constituant les champs lexicaux du football, des voitures et de la boisson).*

Voici les règles qui peuvent être respectées pour garantir la qualité et la force d'une passe-phrase :

1 - aucun lien entre les 4 mots (PouletFritePuréeJambon n'est pas une bonne passe-phrase) ;

2 - ne pas être générée automatiquement (un générateur se base sur une liste de mots, rendant la passe-phrase vulnérable à une attaque par dictionnaire) ;

3 - pas de lien psycho-social **trop** évident : code postal, prénoms des enfants, etc. (de manière générale, toute information pouvant être glanée facilement) ;

4 - ne contient pas 4 mots présents au sein d'un même dictionnaire (mélangez mots étrangers, noms propres, nombres, noms communs, etc.) ;

5 - pas de lien évident avec le service à sécuriser (MaPassePhraseFacebook ne doit pas être utilisée comme passe-phrase Facebook) ;

6- n'est inscrite nulle part.

5.3.7 Les limites

Les passe-phrases sont donc une alternative sérieuse aux faiblesses intrinsèques des mots de passe classiques. Il est aisé d'obtenir des entropies élevées (même compte tenu des biais statistiques exploités par les hackers) tout en conservant une facilité de mémorisation.

En revanche, les « astuces » permettant de complexifier la passe-phrase et de gagner en entropie, reposent sur l'élargissement du dictionnaire. Donc une croissance par le nombre de symboles (croissance géométrique et non pas exponentielle).

Il est impossible, par cette méthode, de faire croître régulièrement l'entropie des passe-phrases de manière significative.

Pour cela il faudrait augmenter l'exposant, donc le nombre de mots que l'on concatène. Ce qui deviendrait rapidement problématique vis-à-vis de la mémoire humaine.

La recommandation officielle de sécurité est de 80 bits d'entropie **[14]**. La marge est confortable compte tenu de la croissance des puissances de calcul. Néanmoins la faculté des passe-phrases d'être facilement mémorisables, s'affranchissant d'être inscrites, ne saurait être maintenue à l'infini.

Cette alternative est très intéressante aujourd'hui sans pour autant être le Graal de l'authentification.

Une autre limitation beaucoup plus « pratique » est qu'il n'est pas toujours possible d'utiliser des passe-phrases. Beaucoup de sites limitent la taille des mots de passe à 16 caractères, forcent l'usage des chiffres, etc.

5.4 La biométrie

L'utilisation de la biométrie pour l'authentification existe dans beaucoup de secteurs sensibles, mais elle est de moins en moins utilisée seule.

5.4.1 Avantages

- pas de problématique de mémoire, on « est » le mot de passe ;

- non trivial à falsifier ;

- non trivial à dérober.

5.4.2 Inconvénients

- utilisation à distance limitée : nécessite des lecteurs biométriques sur les ordinateurs. Les données circulent alors via un canal non sécurisé : Internet (possibilité accrue de vol/substitution de l'empreinte envoyée) ;

- possibilités croissantes de falsification ;

- coût important ;

- problématiques éthiques de respect de la vie privée ;

- le « vol » du « mot de passe » a des conséquences rapidement dramatiques (notamment pour l'empreinte rétinienne).

5.5 Les cartes à puce

Après cet examen de l'état de l'art des mots de passe, il est beaucoup moins facile de se rire de l'ANSSI qui recommande massivement d'utiliser des cartes à puce pour l'authentification (règle 13 du guide d'hygiène informatique : http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf).

5.5.1 Avantages

Généralement perçue comme surdimensionnée par rapport aux besoins, la carte à puce offre pourtant des avantages non négligeables, au vu des inconvénients/faiblesses des autres méthodes :

- coût raisonnable ;

- difficile à dérober : l'accès à la carte à puce n'implique pas la compromission automatique du secret, il faut connaître le PIN (bloqué si trop d'essais échoués) ;

- technologie maîtrisée et mature ;

- attaques par canaux auxiliaires difficiles : accéder au secret depuis les circuits requiert du matériel très coûteux. Le PIN est facilement mémorisable, le risque qu'il soit noté est réduit ;

- évolutivité : le code PIN déverrouille une clé cryptographique dont le dimensionnement peut être augmenté avec l'état de l'art (transparent pour l'utilisateur).

5.5.2 Inconvénients

- plus coûteuse qu'un mot de passe ;

- utilisation à distance limitée ;

- utilisation répandue de code PIN « pathétiques » : 0000, 1234, etc. ;

- dégradable : si la carte à puce est endommagée, l'accès est indisponible le temps de son remplacement.

5.6 L'authentification multi-critères

Ce type d'authentification s'est démocratisé notamment grâce aux banques. Le principe est de demander à l'utilisateur au moins 2 vecteurs d'authentification. Exemple : son mot de passe + un code reçu par SMS.

La robustesse repose sur le fait que les deux facteurs, fragiles individuellement, utilisent deux canaux différents. Dans l'exemple donné, le mot de passe utilise le canal Internet et le code SMS le canal GSM. Un attaquant doit alors dérober le mot de passe de l'utilisateur et être en même temps être capable de lire les données de son mobile.

La biométrie, les cartes à puces, les « *tokens* », les SMS, les mots de passe, etc. peuvent être combinés au choix afin de forcer l'attaquant à devoir « être partout ».

Google propose notamment son application Authenticator pour smartphone (open source jusqu'en v2.21, des forks existent) qui démocratise la double authentification via un système OTP (mot de passe à usage unique). Elle s'interface avec la plupart des services populaires (Amazon, Dropbox, Facebook, Gmail, etc.).

Des solutions plus orientées « professionnels » existent également : citons RSA Secure ID.

Cette méthode a l'inconvénient d'être plus lourde en infrastructure et plus lente à l'usage.

Une autre faiblesse découle de la croissance de la convergence numérique. Les mots de passe sont de plus en plus sauvegardés sur les smartphones. Dans une authentification mot de passe/SMS, les deux facteurs sont localisés sur le même terminal.

Ce système n'en demeure pas moins très sérieux et il est à juste titre largement privilégié pour les opérations sensibles. Forcer l'attaquant à devoir réussir au moins deux attaques, nécessitant des compétences différentes, est une très bonne protection (tant que le gain en jeu n'est pas trop élevé).

Aucune solution ne respecte l'ensemble des critères de sécurité (robustesse, évolutivité, applicabilité) et chacune connaît des utilisateurs qui l'emploient mal (code PIN 0000, passe-phrase : JaimeLePain). Il existe donc un seuil incompressible de sésames vulnérables aux hackers.

La recommandation la plus pragmatique est donc de respecter les bonnes pratiques (quelle que soit la solution choisie) afin de se situer au-dessus de ce seuil.

En guise de conclusion, citons le fabuleux Randall Munroe :

Ce que s'imaginent les experts en crypto : « L'ordinateur est chiffré, hummm, construisons un supercalculateur à 1 million de dollars pour le craquer. Oh non ! C'est du RSA 4096, notre plan diabolique est déjoué »

Ce qui arrive en vrai : « L'ordinateur est chiffré, droguons-le et tapons-lui dessus avec cette clé à molette à 5$, il nous donnera le mot de passe ».

Références & liens

[1] https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html#!s!xkcd

[2] http://www.explainxkcd.com/wiki/index.php/936:_Password_Strength

[3] http://security.stackexchange.com/questions/6095/xkcd-936-short-complex-password-or-long-dictionary-passphrase

[4] http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

[5] http://blog.zorinaq.com/?e=42

[6] http://www.zdnet.com/article/cheap-gpus-are-rendering-strong-passwords-useless/

[7] http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html

[8] http://research.microsoft.com/pubs/74164/www2007.pdf

[9] https://www.grc.com/haystack.htm

[10] http://fr.slideshare.net/sth4ck/sthack-2014-mano-0xsata-zwahlen-paware-a-diy-hardware-password-safe

[11] http://www.guichetdusavoir.org/viewtopic.php?t=9699

[12] http://xkcd.com/936/

[13] https://subrabbit.wordpress.com/2011/08/26/how-much-entropy-in-that-password/

[14] http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

https://xato.net/passwords/analyzing-the-xkcd-comic/#.VO-ATrvg3f4

https://www.grc.com/sn/sn-313.htm#!s!math%20is%20wrong

http://www.reddit.com/r/YouShouldKnow/comments/232uch/ysk_how_to_properly_choose_a_secure_password_the/cgt6ohq

http://www.reddit.com/r/technology/comments/1yxgqo/bruce_schneier_on_choosing_a_secure_password/cfp2z9k

http://en.wikipedia.org/wiki/Talk:Passphrase

http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time

http://www.fidian.com/programming/passwordsecurity

http://world.std.com/~reinhold/diceware.html

http://world.std.com/~reinhold/dicewarefaq.html#calculatingentropy

http://xkcd.com/792/

http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

http://robinmessage.com/2014/03/why-bruce-schneier-is-wrong-about-passwords/