Chaminade Thibault M2 ISC
Chapelle Luca

Rapport Info 910

Recommandations pratiques pour des mots de passe plus forts et plus utilisables

1. Introduction

Pour aider les utilisateurs à créer des mots de passe plus solides, les administrateurs système exigent souvent que les mots de passe dépassent une certaine longueur, contiennent au moins un nombre spécifique de classes de caractères ou n'apparaissent pas dans une liste de blocage (liste de mot commun ex : azerty etc ..).

Les utilisateurs sont également souvent incités à créer des mots de passe plus forts par des compteurs de mots de passe qui donnent un retour d'information sur la force des mots de passe et des suggestions sur la façon de les améliorer.
Les premières orientations sur la manière de déployer ces approches s'appuyaient principalement sur le bon sens et les avis des experts.
Au cours de la dernière décennie, une base scientifique a été mise en place pour déterminer quelles sont les exigences les plus efficaces pour encourager les utilisateurs à créer des mots de passe solides mais toujours mémorisables.

Par exemple, des recherches ont montré que l'augmentation de la longueur minimale peut augmenter la force des mots de passe, plus que le simple fait de se fier à des exigences de classe de caractères ; que les compteurs de mots de passe peuvent très efficacement inciter les utilisateurs à créer des mots de passe plus forts ; et que des listes de blocage soigneusement configurées peuvent aider à empêcher les utilisateurs de choisir des mots de passe faciles à deviner .
Ces premiers efforts ont permis de déterminer quelles exigences en matière de mots de passe étaient plus ou moins efficaces, mais n'ont pas permis de fournir des orientations définitives.

La manière dont les utilisateurs choisissent leurs mots de passe a changé au fil du temps, et que cela, combiné aux progrès réalisés dans l'estimation des mots de passe, implique que le fait d'exiger que les mots de passe aient plusieurs classes de caractères apporte, au mieux, un avantage mineur à la force des mots de passe.

Bien que certaines configurations de listes de blocage soient plus efficaces que d'autres pour éliminer les mots de passe faibles, les politiques qui exigent que les mots de passe aient au moins huit caractères et qui interdisent simultanément les mots de passe qui peuvent être devinés à 10^6 estimations sont plus performantes en termes d'encouragement de la force des mots de passe que les politiques de listes de blocage les plus performantes que nous avons examinées.

2. Contexte

a. Politiques de composition

Les politiques de composition des mots de passe visent à aider les utilisateurs à créer des mots de passe plus uniques et moins prévisibles. Les politiques de composition peuvent être utilisées au moment de la création du mot de passe pour imposer un nombre minimum de classes de caractères - lettres majuscules, minuscules, symboles et chiffres - et une longueur minimale.
Les premiers travaux sur les politiques de composition se sont concentrés sur les exigences en matière de classes de caractères pour augmenter la force des mots de passe .
En général, on a constaté que les politiques qui exigent davantage de classes de caractères produisent des mots de passe trop forts.
Des travaux ultérieurs ont étudié les politiques qui privilégient la longueur par rapport à la composition des classes de caractères.
Les chercheurs qui se sont penchés sur les exigences en matière de longueur ont découvert que la réduction du nombre de classes de caractères requises tout en augmentant la longueur minimale requise pourrait renforcer les mots de passe sans diminuer leur mémorisation ou les rendre plus difficiles à créer.

Bien que les chercheurs et, plus récemment, le NIST conseillent d'éviter les politiques de composition exigeant un nombre minimum de classes de caractères, ce type de politique est encore souvent utilisé dans la pratique.

b. Listes de blocage

Même si les exigences relatives aux mots de passe sont généralement efficaces pour améliorer la force, certains utilisateurs les rempliront de manière prévisible. Ainsi, les règles relatives à la classe de caractères et à la longueur minimale sont insuffisantes pour éviter les mots de passe très faibles .
Par exemple, les règles de 4 classes 8 et de 1 classe 16 permettent des mots de passe extrêmement prévisibles tels que "Mot de passe 1" et "passwordpassword".
Une solution courante consiste à combiner les exigences en matière de composition avec une vérification de la liste de blocage.
Par exemple, le NIST 800-63B recommande que les mots de passe ne figurent pas dans une liste de valeurs couramment utilisées, prévues ou compromises .

Les contrôles de liste de blocage correctement configurés peuvent rejeter les mots de passe prévisibles ou faciles à deviner.

L'exigence de liste de blocage utilise une liste de mots et un algorithme de correspondance qui vérifie si un mot de passe donné est empêché par cette liste de mots.

Les listes de mots peuvent contenir des séquences de caractères courantes, ainsi que des mots de passe ayant déjà fait l'objet d'une fuite.

Les algorithmes de correspondance vont de la correspondance exacte à des règles plus compliquées, par exemple en supprimant les symboles et les chiffres du mot de passe, en le rendant insensible à la casse et en vérifiant que la chaîne résultante ne correspond à aucune entrée de la liste de mots.

Les listes de blocage se distinguent par leurs listes de mots et leurs algorithmes de correspondance, par exemple si et comment les symboles ou les chiffres sont supprimés des mots de passe avant la correspondance.
Elles diffèrent également par l'interdiction, l'avertissement ou la réduction de la force du mot de passe si la vérification de la liste de blocage est positive.

En analysant de grandes séries de mots de passe ayant fait l'objet d'une fuite, Weir et al. ont constaté que des listes de blocage plus importantes renforçaient les mots de passe .
Kelley et al. ont testé trois listes de mots de passe de tailles différentes et ont également constaté que les listes de mots de passe plus importantes produisaient des mots de passe plus forts .

Les travaux antérieurs qui utilisent des analyses rétrospectives des politiques ont des limites, par exemple, la substitution des mots de passe autorisés par les politiques surestime rétroactivement l'impact des politiques de mots de passe sur la force et ne peuvent pas tenir compte des utilisateurs qui remplacent les mots de passe bloqués par des mots de passe encore plus faibles, mais non bloqués.

Les études rétrospectives ne peuvent pas non plus analyser de nombreux aspects des politiques de mots de passe liés à la facilité d'utilisation.
En outre, les listes de mots bloqués peuvent avoir un impact différent sur la force et la facilité d'utilisation des mots de passe en fonction des interactions entre la liste de mots, l'algorithme de correspondance et la politique de composition qu'elles augmentent.

C. Quantification de la force du mot de passe

La force des mots de passe produits dans le cadre d'une politique particulière de création de mots de passe peut être quantifiée à l'aide de chiffres approximatifs.
Les nombres d’estimations peuvent être calculés en énumérant les mots de passe prévus par un modèle d’estimations particulier, en probabilité décroissante, ou selon l'ordre dans lequel un outil de craquage de mots de passe communément configuré produirait des estimations.

Lorsque les attaques hors ligne sont applicables, ils font valoir que l'effort de l'utilisateur pour créer des mots de passe qui résistent à ces attaques est généralement gaspillé, à moins que les mots de passe ne puissent résister à des attaques qui font jusqu'à 10^14 suppositions.

3. Travaux effectués

a. Facteurs expérimentaux

Les facteurs expérimentaux comprennent trois types d'exigences qui peuvent être appliquées par une politique de création de mots de passe : la composition, la liste de blocage et les exigences de force minimale. Des analyses ont été effectuées sur des mots de passe sélectionnés au hasard pour aider à identifier les paramètres à explorer dans l'étude des utilisateurs pour chaque type de facteur expérimental. Il s'agissait d'appliquer rétroactivement une politique de mots de passe à un ensemble de mots de passe ayant fait l'objet d'une fuite et d'observer les proportions et les forces des mots de passe autorisés ou rejetés par cette politique. Les conclusions générales sont basées sur des données collectées à partir d'études expérimentales sur les utilisateurs, ce qui évite ces limites. En outre, les résultats de l'expérience 1 ont éclairé les paramètres explorés dans l'expérience 2.

b. Etude

Dans la première partie, les participants ont été invités à jouer un rôle, en imaginant qu'ils devaient créer un nouveau mot de passe parce que leur principal fournisseur de comptes de messagerie électronique avait été violé. Deux jours plus tard, ils ont reçu un courriel pour leur demander de participer à la deuxième partie, dans laquelle il leur était demandé de se souvenir de leur mot de passe. Il a été pris en compte que les données des participants qui ont rempli la partie 2 entre deux et cinq jours après la partie 1. Après chaque partie, les participants ont répondu à une enquête qui a permis de collecter des données démographiques et des données relatives à l'utilisation. La tâche de création de mots de passe de la première partie a utilisé un compteur de mots de passe développé lors de travaux antérieurs, qui comprenait un retour d'information en temps réel sur les exigences, une barre de renforcement des mots de passe et un retour d'information textuel sur l'amélioration du renforcement des mots de passe. Les participants ont reçu un retour d'information sur l'amélioration de la force des mots de passe seulement après que toutes les exigences en matière de composition, de force minimale et de liste de blocage aient été satisfaites. La configuration du compteur de mots de passe était basée sur les meilleures pratiques empiriquement démontrées par des travaux antérieurs.

Les participants à l'expérience 1 ont été recrutés en juillet et août 2019, Sur les 5099 participants qui ont commencé l'étude, 4317 ont terminé la partie 1 et 3463 ont également terminé Partie 2.

Les participants à l'expérience 2 ont été recrutés en octobre et novembre 2019. Sur les 4 817 participants qui ont commencé l'étude, 4005 ont terminé la partie 1 et 3014 également terminé la partie 2.

L'analyse comprend des données concernant 1 518 participants à l'expérience 1 et 1 362 participants à l'expérience 2.

C. Analyse

Ce compteur a fourni un retour d'information sous forme de texte sur la manière d'améliorer des mots de passe, une barre de force et un retour d'information sur les exigences en temps réel,dont chacune a été configurée selon les recommandations des études préalables. D'après les réponses à l'enquête, la majorité des participants ont trouvé le compteur informatif, utile et influent. Par exemple, la plupart des participants ont indiqué qu'ils avaient mis en œuvre les changements suggérés par les commentaires textuels et que c'était important pour eux que la barre de couleur donne une bonne note à leur mot de passe.

4. Résultats

Les résultats rapportés ici nous amènent à recommander des politiques de mots de passe qui comprennent à la fois des exigences de longueur et de résistance minimales.

Dans le cas où une organisation décide de ne pas exiger une force minimale, ils recommandent deux politiques comprenant des exigences de longueur minimale et de liste de blocage.

Ces politiques offrent une protection moindre que les politiques de force minimale contre les attaques hors ligne, mais fournissent une protection adéquate contre les attaques en ligne tout en restant utilisables pendant la création du mot de passe.

Les résultats de l'expérience 1 montrent que les listes de blocage peuvent ne pas améliorer sensiblement la force des mots de passe si la vérification de la liste de blocage utilise un algorithme de correspondance strict avec une liste de mots insuffisamment large.

Cependant, lorsqu'elles sont correctement configurées, les exigences de la liste de blocage peuvent être combinées avec d'autres exigences afin d'assurer une protection adéquate contre les attaques en ligne par estimation de mot de passe.

Les résultats de l'expérience 2 montrent que les politiques NN8 et NN10 peuvent être tout aussi utilisables que les politiques de liste de blocage que nous testons, tout en produisant des mots de passe plus résistants aux attaques hors ligne.

Ils ont comparé chaque condition de la liste de blocage à sa condition de base correspondante afin de quantifier l'impact des listes de blocage sur la facilité de deviner et d'utilisation. Ils ont constaté que les configurations de liste de blocage 1c8+Pwned-fs et 1c8+Xato-strip-cifs (1 caractère et 8 mot + une liste de mot) améliorent considérablement la force des mots de passe par rapport à leur condition de base sans nuire de manière substantielle à la facilité d'utilisation.

Les mots de passe créés dans le cadre des politiques 1c8+Xato-cifs ou 3c8+Xato-cifs n'étaient ni plus forts dans l'ensemble ni moins susceptibles d'être devinés lors d'attaques en ligne que les mots de passe créés dans le cadre des politiques de base qui ne contenaient que des exigences de composition.(donc 1 caractère équivaut à 3 caractère différent)

Si les politiques de listes de blocage qui utilisent la correspondance de chaînes complètes peuvent fournir une protection adéquate contre les attaques par estimation de mot de passe en ligne, nos résultats suggèrent que cela nécessite une liste de mots beaucoup plus large que la liste de mots Xato que nous avons testée.

Parmi les politiques avec listes de blocage qui ont amélioré la défense des mots de passe contre les attaques en ligne, deux politiques l'ont fait sans rendre les mots de passe

beaucoup plus difficiles ou longs à créer.

Cependant, les participants n'ont pas trouvé l'une ou l'autre politique sensiblement plus ennuyeuse ou difficile que la politique 1c8.

Ils ont constaté que la comparaison des chaînes complètes en tenant compte de la casse avec de très grandes listes de mots de passe divulgués conduit à des mots de passe aussi sûrs et utilisables que la comparaison floue avec de plus petites listes.

Parmi les configurations de listes de blocage utilisant la même liste de mots Xato, seules 1c8+Xato-ciss ont produit des mots de passe globalement plus résistants aux 10^14 attaques hors ligne que 1c8+Xatostrip-cifs.

Toutefois les graves problèmes de facilité de création de mots de passe associés à 1c8+Xato-ciss nous empêchent de le recommander à la place de 1c8+Xato-strip-cifs.

Les participants ont mis plus de temps à créer des mots de passe sous 1c8+Xato- ciss que sous 1c8+Xato-strip-cifs (liste de mots plus grande) et ont fait état de plus de désagréments et de difficultés.

Par rapport aux participants à 1c8+Xato-strip-cifs, les participants à 1c8+Xato-ciss étaient également plus nombreux à abandonner avant d'avoir terminé la première partie et à stocker ou écrire numériquement leur mot de passe après l'avoir créé .

Ces résultats amènent à conclure que si une liste de blocage correspondant à l'algorithm peut fournir une sécurité solide contre les attaques par estimation de mot de passe, elle peut également nuire gravement à la facilité de création de mots de passe si elle est utilisée avec une liste de mots aussi grande ou plus grande que la liste de mots Xato.

Ils ont constaté que si les politiques de force minimale peuvent être renforcées contre les attaques hors ligne en augmentant soit la longueur minimale requise, soit le nombre minimal de classes de caractères, l'augmentation de la longueur minimale permet d'atteindre cet objectif à un coût d'utilisation moindre, en termes de temps nécessaire aux utilisateurs pour créer un mot de passe conforme et de la difficulté ou de l'ennui qu'ils rencontrent dans cette tâche.

Dans l'ensemble, les résultats montrent que, pour les politiques imposant une exigence de force minimale particulière, des exigences de composition plus complexes peuvent conduire à des mots de passe plus résistants aux attaques par estimation de mot de passe, en particulier pour les scénarios d'attaques hors ligne. Bien que les résultats montrent que le fait d'exiger davantage de classes de caractères ou des mots de passe plus longs rend les mots de passe plus forts, l'augmentation de la longueur requise pourrait produire des avantages plus importants en matière de sécurité que l'augmentation des exigences relatives au nombre de classes de caractères, tout en ayant moins d'impact négatif sur la facilité de création des mots de passe.

5. Conclusion

Nous nous sommes intéressés donc à 3 méthodes imposées dans les politiques de mots de passe : les exigences de composition, les listes de blocage et les exigences de force minimale. À l'aide de deux études expérimentales à grande échelle sur les utilisateurs, la sécurité et la convivialité qui ont été examinées de chaque type d'exigences, et de leurs combinaisons, lorsqu'elles sont déployées dans un compteur de mots de passe moderne. Les résultats ont débouché sur des recommandations concrètes pour la configuration des listes d'exigences. Il est recommandé que les exigences de liste de blocage vérifient les mots de passe candidats par rapport à une liste d'environ 10^5 mots de passe ayant fait l'objet de fuites fréquentes en utilisant un algorithme de correspondance floue ou effectuent une vérification complète par rapport à une grande liste comprenant tous les mots de passe connus ayant fait l'objet de fuites. Les politiques de mots de passe intégrant des exigences de liste de blocage ne devraient pas imposer d'exigences de classe de caractères. Il a été également constaté que les politiques de force minimale peuvent améliorer les politiques de listes de blocage en augmentant la résistance aux attaques hors ligne.