Engineer

Mot de passe

✳ Chaîne secrète permettant de s'authentifier

Ce que c'est

Un mot de passe est une chaîne de caractères qu'une personne garde en mémoire ou dans un gestionnaire de mots de passe, et présente pour montrer qu'un compte lui appartient. Les définitions du glossaire du NIST s'accordent sur l'essentiel : des lettres, des chiffres et d'autres symboles « servant à authentifier une identité ou à vérifier une autorisation d'accès », et, dans certains documents, à dériver des clés cryptographiques. Les recommandations actuelles sur l'identité numérique, SP 800-63-4, le classent comme facteur « quelque chose que vous savez » et précisent que leur première édition employait le nom de secret mémorisé. Une phrase de passe, composée d'une suite de mots, et un code PIN, composé uniquement de chiffres décimaux, sont tous deux des mots de passe au sens large.

Une même chaîne peut remplir deux rôles qui se ressemblent. Un mot de passe de connexion est envoyé à un vérificateur, qui conserve de quoi le reconnaître et ne devrait jamais conserver le mot de passe lui-même. Un mot de passe servant à déverrouiller quelque chose localement reste sur l'appareil. SP 800-63B appelle ce type un secret d'activation, avec pour exemple habituel le code PIN de déverrouillage d'un authentificateur multifacteur : il sert sur l'appareil à accéder au secret que détient l'authentificateur.

La difficulté tient au fait qu'un mot de passe est un secret partagé. L'utilisateur le connaît, le service doit le reconnaître, et quiconque l'apprend peut s'en servir exactement comme l'utilisateur. Rien dans la chaîne ne la lie au site qui l'a demandée : SP 800-63B affirme donc clairement que les mots de passe ne résistent pas à l'hameçonnage. L'essentiel du travail technique autour des mots de passe vise à limiter les conséquences de la divulgation de ce secret partagé.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce qu'un mot de passe ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Des comptes, mots de passe et droits attribués selon les besoins exacts de chaque poste, puis retirés le jour du départ.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 1 000 règles RBAC pour sécuriser Linux — 1,000 règles d'accès écrites pour combler une faille de sécurité

1 000 règles RBAC pour sécuriser Linux Contactez-nous →

Pourquoi c'est important

Un mot de passe est souvent la seule protection d'un compte. Deux types d'essais de mots de passe entrent en jeu, chacun freiné par des moyens différents.

La recherche en ligne consiste à essayer des mots de passe sur le vrai formulaire de connexion, où le service impose le rythme. SP 800-63B limite à 100 les échecs consécutifs avec un même authentificateur sur un même compte et impose de comparer les nouveaux mots de passe à une liste de blocage contenant des valeurs courantes, prévisibles ou compromises, pour ne jamais accepter celles qu'un attaquant essaierait en premier.

La recherche hors ligne commence lorsqu'une copie des données de mots de passe stockées a quitté les locaux. Il n'y a plus ni formulaire ni limite. Les recommandations notent que les attaquants peuvent calculer plusieurs milliards de condensats par seconde hors ligne, et que des mots de passe destinés à y résister doivent être « plus complexes de plusieurs ordres de grandeur » que ceux confrontés au seul formulaire de connexion. Le stockage décide donc de l'issue. SP 800-63B impose de saler et de hacher les mots de passe avec un procédé de hachage de mots de passe qui prend le mot de passe, un sel et un facteur de coût pour rendre chaque essai coûteux. Le sel doit comporter au moins 32 bits et être choisi pour que les valeurs de sel entrent rarement en collision, ce qui évite que deux comptes ayant le même mot de passe partagent un condensat stocké. Le facteur de coût devrait être aussi élevé que le vérificateur peut le supporter et augmenter au fil du temps. Les recommandations conseillent aussi d'enregistrer le procédé et le coût ayant produit chaque condensat, afin de pouvoir passer plus tard à un procédé plus robuste.

La RFC 9106 décrit Argon2, une fonction délibérément coûteuse en mémoire, conçue pour cet usage, et recommande sa variante Argon2id : un passage sur 2 Gio de mémoire par défaut pour tous les environnements, ou trois passages sur 64 Mio lorsque la mémoire manque. La RFC indique que le premier réglage maximise le coût pour un attaquant utilisant du matériel dédié à la force brute, propriété décisive dès qu'un fichier de condensats a fuité. La fiche pratique OWASP sur le stockage des mots de passe donne des minimums opérationnels plus bas et des solutions de repli pour les systèmes ne pouvant pas utiliser Argon2id, puis énonce la règle commune à tous. Les hachages rapides tels que SHA-256 ne conviennent pas, car ils permettent beaucoup d'essais rapides. Les mots de passe sont hachés plutôt que chiffrés, car le chiffrement est réversible et permet de retrouver l'original.

À quoi cela ressemble en pratique

Avant la mise en place d'un système de gestion des mots de passe pour toute une entreprise, chacun stockait et partageait les identifiants à sa façon. Au quotidien, cela ressemble rarement à une compromission spectaculaire, mais plutôt à un mot de passe dans une conversation, à un compte partagé dont personne ne renouvelle le mot de passe, et à une lente accumulation de petites expositions. Le système a donné à l'organisation une méthode cohérente pour stocker et partager les identifiants, sans que son usage soit laissé au choix de chacun : un gestionnaire de mots de passe utilisé par la moitié de l'équipe n'aide guère si le risque se trouve dans l'autre moitié. Une fois les identifiants réunis dans un espace de stockage centralisé et géré, le contrôle des accès est devenu plus simple et plus cohérent. SP 800-63B va dans le même sens du côté du service : les vérificateurs doivent autoriser les gestionnaires de mots de passe et le remplissage automatique, devraient autoriser le collage, et les recommandations citent le gestionnaire de mots de passe comme moyen de conserver un mot de passe distinct pour chaque service.

Lors du provisionnement d'un second serveur à partir du code, l'histoire de la première machine a fourni l'argument. Elle avait été créée à la main, puis son pare-feu ajouté après coup, ce qui laisse une fenêtre durant laquelle un nouvel hôte ayant une politique de mots de passe par défaut est accessible depuis Internet. La correction tient à l'ordre des opérations : la nouvelle machine naît derrière son pare-feu, car le play du pare-feu s'exécute avant celui du serveur.

Lors d'une connexion auprès d'un grand fournisseur de messagerie, l'application disait à l'utilisateur que son mot de passe était incorrect. Il ne l'était pas. Ce fournisseur exige un mot de passe propre à l'application pour les clients tiers : un

même compte avait donc deux types de mot de passe, et un message qui n'en connaissait qu'un envoyait l'utilisateur ressaisir quelque chose qui ne pouvait jamais fonctionner. Le message réécrit nomme le fournisseur, indique qu'il exige un mot de passe d'application et dit où le créer ; un test vérifie le nom du fournisseur et le type de mot de passe requis.

Où les problèmes surviennent

Un mot de passe pour plusieurs comptes. Quand le même mot de passe protège plusieurs services, une fuite chez le plus faible ouvre les autres. SP 800-63B appelle cela le bourrage de mots de passe : un mot de passe récupéré sur un site est essayé sur les comptes de la même personne sur d'autres sites. Les utilisateurs se défendent avec un mot de passe distinct par service, ce qui implique en pratique un gestionnaire de mots de passe ; les services, en vérifiant les nouveaux mots de passe selon les valeurs issues de fuites antérieures.

Des règles qui affaiblissent les mots de passe. Les exigences de composition paraissent strictes et produisent des résultats prévisibles. L'exemple des recommandations est une personne qui aurait choisi « password », mais qui choisit « Password1 » lorsqu'on exige une majuscule et un chiffre, et « Password1! » lorsqu'on exige aussi un symbole. Elles interdisent les règles de composition, les changements programmés, les indices lisibles avant connexion et les questions de sécurité telles que le nom du premier animal de compagnie, tout en imposant un changement dès qu'il existe une preuve de compromission.

Un hachage rapide, ou le même sel pour chaque ligne. Une table de mots de passe hachés avec une fonction généraliste, ou tous salés avec la même valeur, donne à un attaquant hors ligne des essais peu coûteux à vérifier contre tous les comptes en même temps. Les systèmes qui héritent d'anciens condensats peuvent hacher à nouveau chaque mot de passe avec le nouveau procédé lors de la connexion suivante de l'utilisateur, comme le décrit la fiche pratique OWASP. La référence au procédé stockée avec le condensat indique quelles lignes utilisent encore l'ancien.

Le mot de passe est tronqué, ou le collage est impossible. SP 800-63B impose de vérifier le mot de passe soumis dans son intégralité, jamais une partie tronquée, et souhaite que le collage soit autorisé pour que les gestionnaires fonctionnent là où le remplissage automatique ne fonctionne pas. Certaines fonctions de hachage ont leur propre limite : la fiche pratique OWASP indique

que bcrypt accepte au maximum 72 octets d'entrée dans la plupart des implémentations et demande aux services qui l'utilisent de faire respecter ce maximum.

Le mot de passe se retrouve là où il ne devait pas être. Un mot de passe collé dans une conversation, écrit dans un ticket ou imprimé dans un journal constitue une copie hors de tout contrôle du véritable stockage. Le changer est la seule façon de neutraliser cette copie : un espace de stockage centralisé et géré compte donc davantage que toute règle portant sur l'apparence du mot de passe.

Pour aller plus loin

- Mot de passe, dans le glossaire CSRC du NIST — définitions de FIPS 140-2, SP 800-63-4 et d'autres documents, avec la phrase de passe comme cas particulier.
- NIST SP 800-63B-4 — règles actuelles de choix, de vérification et de stockage des mots de passe, avec leurs justifications en annexe A.
- RFC 9106 — Argon2 et les deux réglages Argon2id recommandés pour le hachage des mots de passe.
- Fiche pratique OWASP sur le stockage des mots de passe — paramètres opérationnels d'Argon2id, scrypt, bcrypt et PBKDF2, et mise à niveau des anciens condensats.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce qu'un mot de passe ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/password/