Engineer

Contraseña

✳ Cadena secreta que acredita quién inicia sesión

Qué es

Una contraseña es una cadena de caracteres que una persona guarda en la memoria o en un gestor de contraseñas y presenta para demostrar que una cuenta le pertenece. Las definiciones del glosario del NIST coinciden en lo esencial: letras, números y otros símbolos «utilizados para autenticar una identidad o verificar una autorización de acceso» y, en algunos documentos, también para derivar claves criptográficas. La guía actual de identidad digital, SP 800-63-4, la llama el factor «algo que sabe» y señala que su primera edición usaba el nombre secreto memorizado. Una frase de contraseña, formada por una secuencia de palabras, y un PIN, formado solo por cifras decimales, también son contraseñas en sentido amplio.

Una misma cadena puede cumplir dos funciones que se parecen. Una contraseña para iniciar sesión se envía a un verificador, que conserva lo suficiente para reconocerla y nunca debería guardar la propia contraseña. Una contraseña para desbloquear algo local permanece en el dispositivo. SP 800-63B llama a esta última secreto de activación y pone como ejemplo habitual el PIN de desbloqueo de un autenticador multifactor: se utiliza en el dispositivo para acceder al secreto que contiene el autenticador.

La dificultad es que una contraseña es un secreto compartido. La persona lo conoce, el servicio debe reconocerlo y cualquiera que lo averigüe puede utilizarlo exactamente igual que ella. Nada en la cadena la vincula al sitio que la pidió; por eso SP 800-63B declara con claridad que las contraseñas no son resistentes al phishing. La mayor parte de la ingeniería que las rodea consiste en limitar el coste de ese conocimiento compartido cuando se filtra.

Utilice el concepto en una decisión

Aplique «¿Qué es una contraseña?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Cuentas, contraseñas y permisos organizados para que cada persona tenga exactamente el acceso que necesita y lo pierda el mismo día que deja la empresa.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 1.000 reglas RBAC para servidores Linux — 1,000 reglas de acceso escritas para cerrar una brecha de seguridad

1.000 reglas RBAC para servidores Linux Póngase en contacto →

Por qué importa

A menudo, una contraseña es lo único que protege una cuenta. Importan dos formas de adivinarlas, y cada una se frena de manera distinta.

Adivinar contraseñas en línea significa probarlas en el formulario real de inicio de sesión; ahí el servicio marca el ritmo. SP 800-63B limita a 100 los intentos fallidos consecutivos con un autenticador en una cuenta y exige cotejar las contraseñas nuevas con una lista de valores bloqueados que incluya contraseñas comunes, previsibles y filtradas, para no aceptar las opciones que un atacante probaría primero.

Los intentos sin conexión empiezan cuando una copia de los datos de contraseñas almacenados sale de la organización. No hay formulario ni límite. La guía señala que, sin conexión, los atacantes pueden calcular muchos miles de millones de hashes por segundo, y que las contraseñas destinadas a resistirlos deben ser «varios órdenes de magnitud más complejas» que las que solo se enfrentan a un formulario de inicio de sesión. Por eso el almacenamiento decide el resultado. SP 800-63B exige aplicar sal y una función de hash específica para contraseñas, que recibe la contraseña, una sal y un factor de coste, y está diseñada para encarecer cada intento. La sal debe tener al menos 32 bits y elegirse de modo que sus valores rara vez coincidan, para que dos cuentas con la misma contraseña no compartan un hash almacenado. El factor de coste debería ser tan alto como pueda asumir el verificador y aumentarse con el tiempo. La guía también recomienda registrar el método y el coste con los que se produjo cada hash, para poder pasar a uno más robusto más adelante.

RFC 9106 describe Argon2, una función que exige mucha memoria y fue creada para esta tarea, y recomienda su variante Argon2id: una pasada sobre 2 GiB de memoria como opción predeterminada para todos los entornos, o tres pasadas

sobre 64 MiB cuando la memoria escasea. El RFC afirma que el primer ajuste maximiza el coste del atacante en hardware dedicado a fuerza bruta, que es lo que importa cuando se ha filtrado un archivo de hashes. La hoja de referencia de OWASP sobre almacenamiento de contraseñas ofrece mínimos operativos más bajos y alternativas para los sistemas que no pueden usar Argon2id, y establece la regla que los sustenta. Los hashes rápidos como SHA-256 no son adecuados, porque permiten probar muchas contraseñas con rapidez; las contraseñas se almacenan mediante hash, no mediante cifrado, porque el cifrado es reversible y permite recuperar el original.

Cómo se aplica en la práctica

Antes de implantar un sistema de gestión de contraseñas para toda una organización, cada persona almacenaba y compartía credenciales como prefería. En el día a día, esto rara vez parece una intrusión espectacular; suele ser una contraseña en un chat, unas credenciales de acceso compartidas que nadie renueva y una lenta acumulación de pequeñas exposiciones. El sistema dio a la organización una forma uniforme de almacenar y compartir credenciales, y su uso no era opcional para cada persona: un gestor que solo usa la mitad del equipo apenas ayuda si el riesgo está en la mitad que no lo usa. Con las credenciales en un solo lugar gestionado, el control de acceso se volvió más sencillo y uniforme. SP 800-63B apunta en la misma dirección desde el lado del servicio: los verificadores deben permitir los gestores de contraseñas y el autocompletado, deberían permitir pegar, y la guía recomienda un gestor para mantener una contraseña distinta en cada servicio.

Cuando se aprovisionó un segundo servidor desde código, el historial del primero aportó el argumento. Se había creado a mano y su cortafuegos se añadió después, lo que deja un intervalo en el que un host recién creado, con la política predeterminada de contraseñas, es accesible desde internet. La solución es el orden: la máquina nueva nace detrás de su cortafuegos, porque el play del cortafuegos se ejecuta antes que el del servidor.

En un inicio de sesión con un gran proveedor de correo, la aplicación decía que la contraseña de la persona era incorrecta. No lo era. El proveedor exige una contraseña específica de aplicación para los clientes de terceros, de modo que una cuenta tenía dos tipos de contraseña, y un mensaje que solo conocía uno pedía volver a escribir algo que nunca podría funcionar. El mensaje reescrito identifica al proveedor, indica que exige una contraseña específica de aplicación y explica dónde crearla; una prueba comprueba el nombre del proveedor y el tipo de credencial.

Dónde surgen los problemas

Una contraseña para muchas cuentas. Si la misma contraseña protege varios servicios, una filtración en el más débil abre los demás. SP 800-63B lo llama password stuffing: una contraseña obtenida de un sitio se utiliza contra las cuentas de esa misma persona en otros. Las personas se defienden con una contraseña distinta por servicio, lo que en la práctica exige un gestor, y los servicios cotejan las contraseñas nuevas con valores de filtraciones anteriores.

Reglas que debilitan las contraseñas. Las exigencias de composición parecen estrictas y producen resultados previsibles. El ejemplo de la propia guía es alguien que habría elegido «password», pero escoge «Password1» si se le exige una mayúscula y una cifra, y «Password1!» cuando también se pide un símbolo. La guía prohíbe las reglas de composición, los cambios programados, las pistas visibles antes de iniciar sesión y las preguntas de seguridad como el nombre de la primera mascota; aun así, exige cambiar la contraseña en cuanto haya indicios de que se ha visto comprometida.

Un hash rápido o la misma sal para todas las filas. Una tabla de contraseñas con hashes calculados mediante una función de propósito general, o con el mismo valor de sal en todas las filas, permite a un atacante sin conexión hacer intentos de bajo coste que puede cotejar con todas las cuentas a la vez. Los sistemas con hashes antiguos pueden recalcular el hash de cada contraseña con el método nuevo en el siguiente inicio de sesión, como describe la hoja de referencia de OWASP; la referencia al método almacenada muestra qué filas siguen usando el antiguo.

La contraseña se recorta o no se puede pegar. SP 800-63B exige verificar toda la contraseña enviada, nunca una parte truncada, y pide permitir pegar para que los gestores funcionen donde no lo haga el autocompletado. Algunas funciones de hash tienen su propio límite: la hoja de referencia de OWASP señala que bcrypt admite como máximo 72 bytes de entrada en la mayoría de las implementaciones e indica a los servicios que lo usen que hagan cumplir ese máximo.

La contraseña acaba donde nunca debió estar. Una contraseña pegada en un chat, escrita en un ticket o impresa en un log es una copia fuera de todos los controles del almacén real. Cambiarla es la única forma de invalidar esa copia; por eso un solo lugar gestionado importa más que cualquier regla sobre el aspecto de la contraseña.

Lecturas adicionales

- Contraseña en el glosario NIST CSRC — definiciones de FIPS 140-2, SP 800-63-4 y otros documentos, con la frase de contraseña como caso particular.
- NIST SP 800-63B-4 — las reglas actuales para elegir, comprobar y almacenar contraseñas, con sus motivos en el apéndice A.
- RFC 9106 — Argon2 y las dos configuraciones recomendadas de Argon2id para calcular hashes de contraseñas.
- Hoja de referencia de OWASP sobre almacenamiento de contraseñas — parámetros operativos para Argon2id, scrypt, bcrypt y PBKDF2, y cómo actualizar hashes antiguos.

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es una contraseña?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

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

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

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

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/password/