Gestión de Claves Seguras

Osvaldo Callegari
Analista de Sistemas
ocalle@ar.inter.net

En sistemas informáticos, mantener una buena política de seguridad de creación, mantenimiento y recambio de claves es un punto crítico para resguardar la seguridad y privacidad.

Si se utiliza una clave de 8 caracteres de longitud, con los 96 caracteres posibles, puede tardarse 2.288 años en descifrarla (analizando 100.000 palabras por segundo).

Sin embargo, nuestras claves pueden caer en manos de personas non-sanctas, mediante un antiguo método denominado "Fuerza Bruta" donde el atacante simplemente prueba distintas combinaciones de palabras hasta dar con la clave del usuario.

Introducción

Un viejo "*chiste*" dice: ¿Cuál es el eslabón más débil de la cadena de seguridad en sistemas informáticos?.

El usuario final.

Si usted se sintió afectado, por favor pregúntese si la clave para acceder a su sistema tiene algo que lo relacione con usted mismo. Muchas *passwords* de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia. En esta caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "*diccionarios*" que prueban millones de posibles claves, en tiempos muy breves, hasta encontrar la password correcta.

Los *diccionarios* son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Este archivo es utilizado para descubrir dicha password en pruebas de fuerza bruta. Actualmente es posible encontrar diccionarios de gran tamaño orientados, incluso, a un área específica de acuerdo al tipo de organización que se este atacando.

Normas de Elección de Claves

Se deben tener en cuenta los siguientes consejos:

1. No utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado).
2. No usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I., fecha de nacimiento, patente del automóvil, etc.).
3. Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.
4. Deben ser largas, de 8 caracteres o más.
5. Tener contraseñas diferentes en máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.
6. Deben ser fáciles de recordar para no verse obligado a escribirlas. Algunos ejemplos son:

- Combinar palabras cortas con algún número o carácter de puntuación: *soy2_yo3*
- Usar un acrónimo de alguna frase fácil de recordar: ¨A río Revuelto Ganancia de Pescadores¨ *ArRGdP*
- Añadir un número al acrónimo para mayor seguridad: *A9r7R5G3d1P*
- Mejor incluso si la frase no es conocida: ¨Hasta Ahora no he Olvidado mi Contraseña¨ *aHoello*
- Elegir una palabra sin sentido, aunque pronunciable: *taChunda72, AtajulH, Wen2Mar*
- Realizar reemplazos de letras por signos o números: ¨En Seguridad Más Vale Prevenir que Curar¨ *35M\/Pq*

Normas para Proteger una Clave

La protección de la contraseña recae tanto sobre el administrador del sistema como sobre el usuario. Al comprometer una cuenta se puede estar comprometiendo todo el sistema.

La siguiente frase difundida resume algunas de las reglas básicas de uso de la contraseña: "*Un password debe ser como un cepillo de dientes. Úsalo cada día; cámbialo regularmente y NO lo compartas con tus amigos*".

Algunos consejos a seguir:

1. No permitir ninguna cuenta sin contraseña. Si se es administrador del sistema, repasar este hecho periódicamente.
2. No mantener las contraseñas por defecto del sistema.
3. Nunca compartir con nadie la contraseña. Si se hace, cambiarla inmediatamente.
4. No escribir la contraseña en ningún sitio. Si se escribe, no debe identificarse como tal y no debe identificarse al propietario en el mismo lugar.
5. No teclear la contraseña si hay alguien mirando. Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña.
6. No enviar la contraseña por correo electrónico ni mencionarla en una conversación. Si se debe mencionar no hacerlo explícitamente diciendo: "*mi clave es...*".
7. No mantener una contraseña indefinidamente. Cambiarla regularmente. Disponer de una lista de contraseñas que puedan usarse cíclicamente.

Muchos sistemas incorporan ya algunas medidas de gestión y protección de las contraseñas. Entre ellas podemos citar las siguientes:

1. **Número de intentos limitado.** Tras

Continúa en página 188

Cantidad de Caracteres	26 Letras Minúsculas	36 Letras y Dígitos	52 Mayúsculas y minúsculas	96 Todos los Caracteres
6	51 minutos	6 horas	2,3 días	3 meses
7	22,3 horas	9 días	4 meses	24 años
8	24 días	10,5 meses	17 años	2.288 años
9	21 meses	32,6 años	890 años	219.601 años
10	45 años	1.160 años	45.840 años	21.081.705 años

un número de intentos fallidos, pueden tomarse distintas medidas:
- Obligar a reescribir el nombre de usuario (lo más común).
- Bloquear el acceso durante un tiempo.
- Enviar un mensaje al administrador y/o mantener un registro especial.

2. **Longitud mínima.** Las contraseñas deben tener un número mínimo de caracteres (se recomienda 7 u 8 como mínimo).
3. **Restricciones de formato.** Las contraseñas deben combinar un mínimo de letras y números, no pueden contener el nombre del usuario ni ser un blanco.
4. **Envejecimiento y expiración de contraseñas.** Cada cierto tiempo se fuerza a cambiar la contraseña. Se obliga a no repetir ciertas cantidad de las anterior. Se mantiene un periodo forzoso entre cambios, para evitar que se vuelva a cambiar inmediatamente y se repita la anterior.
5. **Ataque preventivo.** Muchos administradores utilizan crackeadores para intentar atacar las contraseñas de su propio sistema en busca de debilidades.

Contraseñas de un solo uso

Las contraseñas de un solo uso *(One-Time Passwords)* son uno de los mecanismos de autentificación más seguros, debido a que su descubrimiento tan solo permite acceder al sistema una vez. Además, en muchas ocasiones se suelen utilizar dispositivos hardware para su generación, lo que las hace mucho más difíciles de descubrir.

Ejemplos de este tipo de contraseñas serían las basadas en funciones unidireccionales *(sencillas de evaluar en un sentido pero imposible o muy costoso de evaluar en sentido contrario)* y en listas de contraseñas.

Se distinguen tres tipos de contraseñas de un solo uso:

1. Las que requieren algún dispositivo hardware para su generación, tales como calculadoras especiales o tarjetas inteligentes (Token Cards).
2. Las que requieren algún tipo de software de cifrado especial.
3. Las que se basan en una lista de contraseñas sobre papel.

La tarjeta genera periódicamente valores mediante a una función secreta y unidireccional, basada en el tiempo y en el número de identificación de la misma.

El usuario combina el número generado por la tarjeta con su palabra de paso para obtener el password de entrada , lo que le protege en caso de robo o perdida.

Tiempos de búsqueda de una clave

Como puede verse en la tabla, arriba, si se utiliza una clave de 8 caracteres de longitud, con los 96 caracteres posibles, puede tardarse 2.288 años en descifrarla (analizando 100.000 palabras por segundo). Esto se obtiene a partir de las 96^8 (7.213.895.789.838.340) claves posibles de generar con esos caracteres.

Partiendo de la premisa en que no se disponen de esa cantidad de años para analizarlas por fuerza bruta, se deberá comenzar a probar con las claves más posibles, comúnmente llamadas Claves Débiles.

Según demuestra el análisis de *+NetBuL* *1 realizado sobre 2.134 cuentas y probando 227.000 palabras por segundo:

- Con un diccionario 2.030 palabras *(el original de John de Ripper 1.04)*, se obtuvieron 36 cuentas en solo 19 segundos *(1,77%)*.
- Con un diccionario de 250.000 palabras, se obtuvieron 64 cuentas en 36:18 minutos *(3,15%)*.

Otro estudio *2 muestra el resultado obtenido al aplicar un ataque, mediante un diccionario de 62.727 palabras, a 13.794 cuentas:

- En un año se obtuvieron 3.340 contraseñas *(24,22%)*.
- En la primera semana se descubrieron 3.000 claves *(21,74%)*.
- En los primeros 15 minutos se descubrieron 368 palabras claves *(2,66%)*.

Según los grandes números vistos, sería válido afirmar que: es imposible encontrar *¡36 cuentas en 19 segundos!* También debe observarse, en el segundo estudio, que el porcentaje de hallazgos casi no varía entre un año y una semana.

Tal vez, ¿esto sucedió porque existían claves nulas; que corresponden al nombre del usuario; a secuencias alfabéticas tipo "*abcd*"; a secuencias numéricas tipo "*1234*"; a secuencias observadas en el teclado tipo "*qwer*"; a palabras que existen en un diccionario del lenguaje del usuario?. Sí, estas claves (las más débiles) son las primeras en ser analizadas y los tiempos obtenidos confirman la hipótesis. ☒

*1 +NetBul. Tabla de Tiempos del John the Ripper 1.4. SET N°15-0x07. Junio de 1998.

*2 KLEIN, Daniel V. Foiling the Cracker: A Survey of, and Improvement to, Password Security.

Fuente: www.segu-info.com.ar