Proteja su Información

Yanina Galaburda

Departamento de Ingeniería de Sistemas
Universidad Católica Boliviana San Pablo
Cochabamba - Bolivia
e-mail: galaburd@ucbcba.edu.bo

Introducción

El número de delitos informáticos crece constantemente y crecen también los límites de fraudes cometidos mediante el uso de computadora. Según las estadísticas, en los Estados Unidos las pérdidas económicas provocadas por delitos informáticos aumenta anualmente un 35 %. La cifra alcanzada en el año 2000 es de aproximadamente 3.500 millones de dólares.

Cuando ocurre el robo de un banco, el promedio de sus pérdidas se calcula en 19.000 dólares, pero mediante la utilización de algunas técnicas de delito informático, el promedio de pérdidas asciende a 560 mil dólares. Sin embargo para un delincuente informático la probabilidad de ser atrapado es muchísimo menor que para un asaltante de banco, y aun si éste fuese atrapado existiría muy poca probabilidad de que termine en la cárcel. Se descubre solamente el 1 % de todos los delitos informáticos cometidos en el mundo y la probabilidad de que el delincuente termine en la cárcel es menor de 10 %.

La principal causa de las pérdidas relacionadas con el uso de computadoras es la falta de conocimiento de los aspectos de seguridad y la casi total ausencia de cultura de seguridad. Solamente los conocimientos que tenga el usuario final acerca de los métodos de protección pueden proporcionar un adecuado nivel de seguridad.

Probablemente usted piense que la Seguridad Informática es un área que no le concierne, ya porque siente que su computador es seguro, ya porque no considera que la información contenida en su disco duro sea de gran importancia o interés para alguien además de Ud. mismo.

Una computadora que no participa en una red es tan segura como el sitio en donde esté funcionando. En estos casos pueden pasarse por alto las medidas de seguridad sin mayores riesgos. Diferente es el caso de las computadoras conectadas a redes públicas como la red Internet, en el cual es aconsejable tomar algunas precauciones, a fin de evitar que personas malintencionadas intenten ingresar sin permiso a su computador.

Las contraseñas

La contraseña es una secuencia de números y letras que, dispuesta junto a un *login* determinado, permite acceder a un sistema. Las contraseñas son la forma básica de la seguridad y la más importante. Aunque son un componente vital de un sistema de seguridad, pueden ser adivinadas o violadas con relativa facilidad.

Según las estadísticas, un gran número de delitos informáticos se comete utilizando la técnica de romper barreras de contraseñas a fin de obtener acceso al sistema y a la información almacenada.

Romper barreras de contraseñas

Password Cracking es el proceso de adivinar o violar las contraseñas para conseguir entrar sin autorización a un sistema o a una cuenta. Este proceso es mucho más fácil de lo que piensa la mayoría de usuarios. La manera más simple de romper una contraseña es utilizar un programa de diccionario para averiguar la palabra usada como contraseña. Estos programas comparan listas de palabras o combinaciones de caracteres hasta encontrar una coincidencia.

Otra forma sencilla de romper una contraseña es utilizar un poco de lógica, recopilando algo de información sobre el propietario de la contraseña. Un gran porcentaje de las personas utilizan como contraseña combinaciones muy sencillas y fáciles de adivinar. Estas combinaciones pueden variar desde su propio nombre o el nombre de sus hijos, hasta las fechas de nacimiento o la dirección de su casa. Un pequeño estudio realizado con más de 1.000 usuarios ha demostrado que el 44 % de las personas usa como contraseña el nombre de alguien querido y otro 22 % elige el nombre de un amor platónico.

También se puede obtener una contraseña mediante ingeniería social. Se entiende por ingeniería social el método por el cual los datos necesarios para efectuar alguna maniobra de acceso ilegal son obtenidos directamente de las víctimas o de sus allegados. Cuando se hace necesario conocer algo que por otras vías no es posible, se recurre a este medio que, en esencia, consiste en comunicarse con la víctima, convencerla de empezar un diálogo y obtener la información requerida, como, por ejemplo, el *password* u otros datos útiles para lograr un acceso al sistema, sin que la víctima se dé cuenta de lo que realmente sucede. Una técnica más elaborada de averiguar una contraseña es a través de los *sniffers*, que son programas que "absorben" datos de la red. Todo lo que pasa a través de la red lo toman y lo almacenan para su análisis posterior. De esta forma se puede obtener información sobre claves de acceso o, incluso, los mensajes de correo electrónico en el que se envían estas claves.

Los *hackers* pueden intentar conseguir su archivo de contraseñas. Este archivo guarda el login (nombre de identificación) de cada usuario en el sistema, así como su contraseña encriptada. Para ello, usarán los fallos de seguridad de las aplicaciones que corren en la máquina, como servidores de páginas Web, puertos de red mal configurados o utilizarán la técnica llamada puertas traseras.

Algo de probabilidades

Según el National Computer Security Center de EEUU, la probabilidad que tiene una contraseña de ser adivinada, se puede expresar mediante la siguiente ecuación:

$$P = (L \times R)/S \qquad (1)$$

donde:

P : Probabilidad de que una contraseña sea adivinada

L : Tiempo de vida de la contraseña

R : Tasa de generación de contraseñas

S : Número de contraseñas únicas, y

$$S = A^m \qquad (2)$$

donde

A : Total de caracteres posibles

m : Longitud de la contraseña

Por ejemplo:

Un usuario tiene una contraseña de 6 caracteres en un sistema de autentificación que permite el uso de sólo 62 caracteres (A...Z; a...z; 0...9) y por políticas del administrador deben cambiarse las contraseñas cada 90 días (90 días = 7776000 segundos). Si consideramos que una computadora puede verificar 3.500 contraseñas por segundo, entonces la probabilidad de que la

confidencialidad del usuario sea violada es de:

$$P = (7776000 \times 3500)/626 = 0,48$$

Malas contraseñas

Se consideran malas, aquellas contraseñas que son fáciles de adivinar porque:

- Incluyen únicamente letras o únicamente números.
- Incluyen una mezcla de letras y números pero sólo letras en mayúsculas o sólo en minúsculas.
- Incluyen palabras contenidas en cualquier diccionario de cualquier idioma.
- Incluyen referencias a datos personales del usuario, como son: iniciales de los nombres , números de identificación o licencia de conducir, fechas de nacimiento, referencias acerca de domicilios, nombres o datos relacionados con la empresa en donde trabaja o donde ha trabajado el usuario, etc.
- Incluyen nombres o referencias de marcas registradas.
- Incluyen nombres de personajes y series de ciencia-ficción.

Ejemplos de malas contraseñas serían: `Pablo2002`, `ximena1970`, `Rhlinux61`, `1218America`.

Otras causas que ponen en peligro nuestros sistemas son contraseñas que han sido escritas en medios físicos (por ejemplo, en papel) o han sido proporcionadas a otras personas.

¿Cómo elegir una buena contraseña?

Ahora que se ha explicado la importancia de las contraseñas y su vulnerabilidad, podemos discutir la manera de crear contraseñas buenas y fuertes.

1. **Tome en cuenta las características principales de una contraseña.** Una contraseña fuerte y efectiva requiere de un determinado grado de complejidad. Hay tres factores a tener en cuenta para desarrollar esta complejidad: longitud, anchura y profundidad.

   a. *Longitud* es el número de caracteres que forman una contraseña, eso significa que cuanto más larga es la contraseña, más difícil es de romperla. En sí, mientras más larga, mejor. Generalmente se recomienda que las contraseñas tengan entre seis y nueve caracteres. Son aceptables contraseñas más largas, siempre que el sistema lo permita y el usuario no tenga dificultad en recordarlas, en cambio deberían evitarse contraseñas más cortas de seis caracteres.

   b. *Anchura* es el número de diferentes caracteres que pueden aparecer en una contraseña. No se limite al alfabeto, hay también números y caracteres especiales como "%" y en la mayoría de los sistemas se distinguen las mayúsculas de las minúsculas.

   c. *Profundidad.* Se refiere a la elección de una contraseña con un significado difícil de adivinar. Es aconsejable no pensar más en palabras y empezar a pensar en frases. El propósito de una frase mnemónica es permitir la creación de contraseñas complicadas sin la necesidad de tener que anotarlas. Un ejemplo puede ser utilizar las primeras letras de una conocida frase como "`LeEiAlo&`" = *"Lo esencial Es invisible A los ojos"*. Lo más efectivo es elegir una frase que tenga un significado personal (para recordarla fácilmente), tomar las iniciales de cada una de las palabras en esa frase y convertir algunas de las letras

en otros caracteres (por ejemplo el "4" por la "H").

2. **No use palabras del diccionario, nombres propios o palabras extranjeras**. Como ya se ha mencionado, las herramientas para romper contraseñas son muy efectivas al procesar grandes cantidades de letras y combinaciones de números. Por lo tanto, debemos evitar utilizar palabras del diccionario seguidas de números o palabras convencionales escritas al revés como "ojabart". Lo que para las personas puede ser difícil de adivinar puede ser muy sencillo para estos incansables programas de fuerza bruta.
3. **No use información personal**. Una de las cosas frustrantes de las contraseñas es que deben de ser fáciles de recordar por los usuarios. Naturalmente, esto lleva a muchos usuarios a incluir información personal en sus contraseñas. Es alarmante la facilidad con la que los *hackers* obtienen información personal sobre próximos blancos de sus ataques. Por tanto intente que su contraseña no sea ni su teléfono, ni su fecha de nacimiento, ni la patente del auto, etc.
4. **No comparta la contraseña.** Mientras más personas conozcan una contraseña, más posibilidades hay de que ésta se "expanda". Trate siempre de memorizarlas, sin escribirlas en ningún sitio (como papel, pared o monitor). Las historias sobre *hackers* que consiguen contraseñas mirando por encima del hombro o rebuscando siempre las papeleras no son leyendas urbanas, son reales, así que evite hacerlo siempre que sea posible.
5. **Evite usar las opciones "Guardar contraseña"**, tanto en el momento de la conexión telefónica como cuando el Explorer le solicite una contraseña para ingresar a una página de acceso restringido. Estas contraseñas se guardan en el disco duro de su máquina y son fácilmente descifrables para alguien con los conocimientos (o el software) necesarios.
6. **Cambie su contraseña con frecuencia.** Puede darse el caso de que alguien se haya apoderado por medios ilícitos de su contraseña y esté utilizándola tanto para conectarse a Internet en forma gratuita utilizando su cuenta, como para leer su correo o para acceder a páginas de acceso restringido donde Ud. posee acceso, todo esto sin que Ud. lo haya notado siquiera. Por esto es saludable cambiar la contraseña tanto de conexión como del correo por lo menos una vez al mes, sin repetir nunca contraseñas anteriores. Una buena forma de detectar si alguien utiliza su cuenta para conectarse a Internet de manera fraudulenta, es revisar periódicamente su tiempo en línea (incluso si posee una tarifa plana) en busca de conexiones en horarios sospechosos.
7. **No utilice la misma contraseña en diferentes cuentas.** Debe evitar utilizar la misma contraseña (por buena que sea) en diferentes cuentas, esto crea un único punto de fallo lo que significa que si un intruso accede a una sola de sus cuentas ya tiene acceso a todas las demás.

Consecuencias del mal uso de contraseñas

Entre las consecuencias más importantes que puede traer esto podemos mencionar:

- El robo de información: podemos estar expuestos a que otras personas consigan nuestros archivos de contraseñas para acceder a la información confidencial.
- La pérdida de integridad de información: las personas que ingresen a nuestro sistema pueden manipular nuestra

información o, más aún, eliminarla, ya sea por su conveniencia o por pura diversión.

- Suplantación: una persona puede hacerse pasar por uno de nosotros.
- Podemos también perder algunos servicios que son importantes para la empresa.

De lo anterior, debe quedar claro que la contraseña elegida es de vital importancia debido que una contraseña mal escogida puede ser objeto de una intromisión.

Referencias

[1] www.550m.com.

[2] www.bezpeca.com.

[3] www.es.geocities.com.

[4] www.pc.idg.net.

[5] www.zonavirus.com.