Criptografía y psicología de la contraseña: generando una contraseña fuerte para diferentes servicios

Password's cryptography and psychology: generating a strong password for different services

Milagros Alessandra Infante Montero[1]
Universidad Continental

INTRODUCCIÓN

La aparición de la informática y el uso de comunicaciones digitales han ocasionado muchos problemas de seguridad contra los que se ha aprendido a lidiar con distintas técnicas e incluso buenas prácticas o políticas que se deben seguir. En el pasado existía un cifrado clásico con el que se cambiaban algunas letras de frases a cifrar por otras letras, números o combinaciones; al no ser suficientes, los criptógrafos investigaron y debido a los avances en la matemática y la tecnología se ha logrado obtener algoritmos mucho más seguros.

Aunque no lo parezca, la criptografía no es solo una cuestión de informáticos; por el contrario, suele formar cada vez más parte de nuestra vida cotidiana, ya que a diario usamos claves para producir la salida funcional de algoritmos criptográficos, que en palabras simples significa que usamos claves para verificar si estamos o no autorizados para acceder a algún servicio o sistema. Pero aun cuando este tema parezca tan sencillo, existe toda una psicología detrás, como también criterios que deben tomarse en cuenta para proteger nuestra información y más detalles que muchas veces pasamos por alto y que de reparar en ello nos permitiría tener menos casos de robo y/o infiltración de información.

Criptografía: el principio de Kerckhoffs

Que nuestra información se mantenga protegida debería ser para todos un derecho plenamente garantizado; sin embargo, existen personas que movidas por intereses de por medio buscan la manera de obtener estos datos y hacen que este derecho sea vulnerado. Un punto importante a tomar en cuenta para evitar esta situación es lo que establece el principio de Kerckhoffs, que "solo el mantener la clave en secreto proporciona seguridad", o como sostiene el gran impulsor del desarrollo teórico de la criptografía después de la Segunda Guerra Mundial, Claude Shannon, que si el enemigo conoce el sistema, debemos estar prevenidos para todo tipo de ataque y no llegar a ser sorprendidos, por el contrario, adelantarnos a lo que pueda pasar y de esta manera lograr que nuestros mecanismos sean mejores y mantengan nuestra información a salvo.


Milagros Infante

milagros@milale.net

1 Estudiante de la Escuela de Ingeniería de Sistemas e Informática de la Universidad Continental, miembro del staff de "Hackers & Developers Magazine" y del equipo de traducción al español de GNOME.

Recibido: 10-05-13 Aprobado: 28-05-13

Mantener las claves en secreto es uno de los problemas más difíciles; esta pequeña pieza, no obstante, puede proteger todo un enorme sistema y por esto se considera como uno de los eslabones más débiles para un supuesto atacante, ya que si la obtiene, accede inmediatamente a todos los datos cifrados y se trae abajo todo lo que protegía. Precisamente por este motivo cada vez se toman más medidas y precauciones para proteger grandes sistemas, quizás ya no solo una o dos claves, sino otros conceptos como la verificación en dos o tres pasos, la biometría y más.

Un ejemplo claro de la relevancia que le dan a este tema, es la Agencia de Seguridad Nacional de los Estados Unidos (2), quienes crearon el CIS (estrategia de interoperabilidad criptográfica) que ha sido desarrollada para encontrar los caminos en los que se comparte información de manera más rápida usando protocolos y algoritmos; para que de esta manera, se pueda tener un control más exacto en lo que se refiere al servicio de inteligencia de este país y de las políticas nacionales que se deben tener en cuenta. Por ejemplo, en la figura N° 1 se puede observar un criptosistema que nos muestra como puede cifrarse una frase.

Este es un texto cifrado:
XQLYHUVLGDG FRQWLQHQWDO

Este criptosistema tiene como clave sumar 3 letras al texto normal, por lo que resuelto, la frase descifrada es:
UNIVERSIDAD CONTINENTAL

Figura N° 1: Ejemplo del principio de Kerckhoffs

El secreto perfecto

La longitud de la clave es el tamaño medido en bits, ya que la criptografía moderna maneja medidas binarias; este aspecto es determinante ya que mientras más pequeña sea, la susceptibilidad de un cifrador será mayor frente a un ataque de búsqueda exhaustivo. Una clave debería ser tan grande como para que un ataque de fuerza bruta sea imposible, este ataque se refiere a obtener una clave probando todas las combinaciones posibles hasta encontrar la correcta, la longitud debería ocasionar que este ataque lleve demasiado tiempo al ejecutarlo y finalmente no obtener el dato que buscaba, esto es considerado el secreto perfecto; para explicar esto con un ejemplo sencillo, una clave de longitud de n bits tiene 2^n claves posibles, por eso es que mientras más extensa sea más alto será el grado de dificultad de poder obtenerla.

Según Schneier (6) raramente los usuarios hacen uso de conjuntos de caracteres largos para formar una contraseña, el estudio que él realizó, reveló a través de un esquema de phishing que en el año 2006 de 34 000 contraseñas, solo el 8,3 % usaba letras mayúsculas, números y símbolos.

Psicología de las contraseñas

Existe una interesante intersección entre criptografía y psicología, lo que da como resultado la psicología de la contraseña, que estudia qué es lo que hace a las claves fáciles de recordar o adivinar, para que una contraseña funcione exitosamente es importante que el usuario la memorice. La psicología detrás de escoger una clave es un balance único entre memorización, seguridad y conveniencia; las contraseñas pueden ser reflejo de la personalidad, aquellos que sean más orientados a la seguridad pueden elegirlas más complicadas, los que se sienten muy seguros con su vida cotidiana pueden nunca cambiarla. La memorización está relacionada con el uso de la nemotecnia pero para algunas personas esto se vuelve un tema complicado, la solución a ello es tener ciertas políticas que permitan mantener las contraseñas seguras.

Si una persona tiene por números preferidos algún primo, esto puede ser un mal indicio para que alguien sin mucho esfuerzo pueda descubrirlo, ya que como dice Kirk (1), los números primos solo son divisibles por uno y por el mismo número, motivo por el cual al identificar que estos números formen parte del conjunto de caracteres de la contraseña puede ocasionar que se adivine la contraseña privada y se descifren los

mensajes.

Políticas de seguridad

Existen muchos factores en la seguridad que debemos tener en cuenta al hablar de contraseñas, una política es un conjunto de reglas para mejorar la seguridad haciendo que los usuarios empleen claves seguras; una de las políticas es acerca de la longitud y formación, se recomienda usar letras mayúsculas y minúsculas, incluir letras, números y caracteres especiales, se debe evitar el uso de palabras que se encuentren en el diccionario o información personal, se debe evitar el uso de números de teléfono u otros números comunes; otra política es respecto a la duración de la contraseña, se recomienda que se proponga un determinado tiempo para cambiarla, puede ser de 90 o 120 días, así se podrían prevenir muchos ataques que requieren de tiempo para obtener esta pieza de información; la siguiente política nos habla sobre la gestión de las claves, se recomienda nunca usar la misma contraseña para más de una cuenta, nunca proporcionarla a nadie, nunca escribirla en un papel y dejarla a lado de la computadora, ser cuidadoso de desconectarse del servicio del que estábamos haciendo uso al finalizar; entre muchas más.

Phishing

Actualmente existen muchas formas de atentar contra la seguridad de la información, uno de los delitos más conocidos es el Phishing, este está dentro de las estafas cibernéticas, ya que es cometido mediante el uso de ingeniería social, al querer adquirir información de forma fraudulenta, el phisher (el estafador) se hace pasar por una persona de confianza de alguna empresa y por correo electrónico o por llamadas telefónicas intenta obtener los datos que desea. Es importante entender como funciona la ingeniería social, esta es la práctica de obtener información confidencial manipulando a los usuarios, el principio que la sustenta es que en todo sistema el eslabón débil es el usuario, los daños causados varían entre la pérdida del acceso al correo electrónico y pérdidas económicas sustanciales.

Por ejemplo, las técnicas con las cuales debemos tener más cuidado es cuando llega un mail al correo electrónico en el cual dan una ruta manipulada para que parezca la original de algún servicio que usemos, quizás es un mail del banco al que está afiliado, pero en realidad es un enlace que nos estará dirigiendo a solicitarnos el usuario y la contraseña de nuestra cuenta y según muchos estudios las personas suelen ser muy confiadas de indicar sus datos sin pensar que esto se trata de una estafa; otro caso puede ser al recibir una llamada telefónica de parte de alguna persona de confianza de la empresa u organización en la que trabaja quien en realidad es un estafador que averiguó cierta información y ahora quiere utilizar eso para obtener los datos que desea.

Crackeo de cuentas y robo de información

Hay una importante diferencia que recalcar entre hacker y cracker, las personas suelen usar el término hacker de mala manera ya que definen con esto a un ladrón informático; sin embargo, un hacker es alguien apasionado por la informática que llega a entrar a un sistema sin autorización pero no con un fin malvado sino con el objetivo de depurar y arreglar errores, ya que disfruta de un conocimiento profundo de su funcionamiento interno. Y al contrario, un cracker es quien accede a determinado sistema, pero con propósitos malvados de robo, fraude y otros. Muchas personas no se dan el tiempo de buscar cómo crear una contraseña segura, es más, el problema radica en que pueden usar la misma clave para todas sus cuentas, pero deben pensar que si un cracker llega a obtener esa información tiene acceso a todo, esto es sumamente peligroso ya que puede hacerse pasar por uno, enviar mails desprestigiando su centro laboral u ocasionándole conflictos de otra índole, pero por otro lado, es cierto que el motivo principal es que si colocan una clave distinta para cada servicio es muy probable

que las puedan olvidar. Afortunadamente, como indica el mismo blog oficial de Gmail (5), sus datos recientes indican que el 15 % de los mensajes que no son spam vienen de dominios protegidos por DMARC, lo que significa que los usuarios de Gmail no tienen de que preocuparse ya que están a salvo de posibles ataques.

¿Cómo crear contraseñas fuertes para cada servicio?

La fortaleza de las contraseñas (4) es una medida de la efectividad de este conjunto de caracteres al resistir que sean adivinadas o atacadas por fuerza bruta; en su forma usual, la fortaleza estima cuantos intentos ha realizado un atacante con resultados fallidos. La fortaleza de una contraseña es una función de longitud, complejidad e imprevisibilidad.

Para darle solución a esto existen muchas maneras que podemos empezar a aplicar para poner a salvo y asegurar nuestra información. Un método eficaz para crear una contraseña segura es elegir una frase (de una canción, del trabajo, etc), luego tomar la primera letra de cada palabra

La frase:
Universidad Continental - Exigencia para grandes cambios.

Resultaría en:
Ucepgc

Y podríamos cambiarles ciertos caracteres y obtener lo siguiente:
uC3pgC

Figura N° 2: Ejemplo para crear contraseñas seguras usando de base una frase

y finalmente cambiar alguna de ellas por números o caracteres especiales, de esta manera la contraseña es larga y será mucho más complicada de ser adivinada como lo podemos ver en la figura N° 2.

Si su contraseña predeterminada es:
uC-3pgC

Se puede crear una contraseña para gmail:
uC-3pgCGmaiL

O una contraseña para twitter:
uC-3pgCTwitteR

Figura N° 3: Ejemplo para crear contraseñas distintas para cada servicio

La figura N° 3 nos muestra otro buen método, ya teniendo una base se puede crear contraseñas distintas para cada servicio que usemos, por ejemplo, según las letras obtenidas anteriormente añadirle algo que nos indique de que servicio se trata.

CONCLUSIONES

Las personas muchas veces se quejan del robo de su información, de la pérdida de sus cuentas, sin darse cuenta que ellos mismos son quienes ocasionan este tipo de situaciones y malas experiencias. Por más que uno piense que la información que tiene en determinado servicio no es muy importante y que no hay problema si llegan a acceder a ella es mejor protegerla de todas maneras o si no vas a usar esa cuenta eliminarla, es importante contar con una contraseña segura y distinta para cada servicio y de una u otra forma seguir todas las indicaciones redactadas líneas arriba, aplicar nuestras propias políticas de seguridad y cumplirlas ya que la mejor defensa contra la ingeniería social es educar y entrenar a los usuarios y sobretodo que ninguno sienta que nunca va ser víctima de un cracker porque si podría pasar.

Algo que ocurre con mucha frecuencia en nuestros días, es que muchos navegadores ofrecen la opción de "Recordar contraseña" (4) y muchas veces acceden a ella, sin pensar en las consecuencias que esto puede tener, ya que los niveles de seguridad de las distintas páginas webs no ofrecen la misma privacidad, es el caso de los clientes de correo que almacenan esta pieza de información en un archivo en la computadora, al que cualquier desconocido podría tener acceso; por esto es que se recomienda evitar esta opción si no se confía plenamente en determinado servicio o equipo. Lucena (7), un reconocido investigador en criptografía, cita que la

criptografía depende en gran medida de la Teoría de Algoritmos, ya que por un lado hemos de asegurar que el usuario legítimo, que posee la clave, puede cifrar y descifrar la información de forma rápida y cómoda, mientras que por otro hemos de garantizar que un atacante no dispondrá de ningún algoritmo eficiente capaz de comprometer el sistema. Está en nuestras manos evitar malos ratos e inconvenientes protegiendo nuestra información, siguiendo las simples maneras mencionadas a lo largo del artículo, definitivamente es un asunto al que debemos empezar a darle la importancia que merece y con la finalidad de tener tranquilidad.

REFERENCIAS BIBLIOGRÁFICAS

1. Kirk J. Researcher: RSA 1024-bit Encryption not Enough [Internet]. PCWorld; 2007 [citado 08/05/2013]. [aproximadamente 01 pantalla]. Disponible en: http://www.pcworld.com/article/132184/article.html
2. National Security Agency. [Internet]. Estados Unidos: Gobierno de Estados Unidos; 2009 [fecha de actualización 11/03/2013; citado 08/05/2013]. Cryptography / Cryptographic Interoperability [aproximadamente 03 pantallas]. Disponible en: http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml
3. Citizendium. [Internet]. The Citizens' Compendium; [fecha de actualización 01/06/2010; citado 09/05/2013]. Kerckhoffs' Principle [01 pantalla]. Disponible en: http://en.citizendium.org/wiki/Kerckhoffs%27_Principle
4. McDowell M. Security Tip (ST04-002) [Internet] US-CERT; 2009 [citado: 06/02/2013]. [aproximadamente 01 pantalla]. Disponible en: http://www.us-cert.gov/ncas/tips/st04-002
5. Dawes A. Landing another blow against email phishing. 29/01/2012 [citado 11/05/2013] en: Seguridad en línea de Google, Blog. [Internet]. Estados Unidos: Gmail Blog [01 pantalla]. Disponible en: http://gmailblog.blogspot.com/2012/01/landing-another-blow-against-email.html
6. Schneier B. MySpace Passwords Aren't So Dumb [Internet]. Wired; 2006 [citado 14/12/2006] [aproximadamente 01 pantalla]. Disponible en: http://www.wired.com/politics/security/commentary/securitymatters/2006/12/72300?currentPage=2
7. Lucena M. Criptografía y Seguridad en Computadores. 4ta ed. España. p 57-60.