TABLAS RAINBOW (ARCOIRIS)

AUTOR: RICARDO CASTILLO

NOVIEMBRE: 2020

San Marcos

Introducción

Los programas para descifrar contraseñas funcionan de manera similar al proceso de inicio de sesión. El programa de descifrado comienza tomando contraseñas de texto sin formato, ejecutándolas a través de un algoritmo hash, como MD5, y luego compara la salida hash con los hash en el archivo de contraseña robado. Si encuentra una coincidencia, el programa ha descifrado la contraseña. Como dijimos antes, este proceso puede llevar mucho tiempo. Es precisamente esta función las que realizan las tablas rainbow (en español: arcoris).

A continuación, se presentan aspectos relevantes relacionados con esta herramienta como definición y funcionalidad.

Contenido

¿Qué son las Tablas Arcoiris?

Las tablas arcoiris son básicamente grandes conjuntos de tablas precalculadas llenas de valores hash que coinciden previamente con las posibles contraseñas de texto sin formato. Las tablas del arcoiris esencialmente permiten a los piratas informáticos invertir la función de hash para determinar cuál podría ser la contraseña de texto sin formato. Es posible que dos contraseñas diferentes den como resultado el mismo hash, por lo que no es importante averiguar cuál era la contraseña original, siempre que tenga el mismo hash. Es posible que la contraseña de texto sin formato ni siquiera sea la misma contraseña que creó el usuario pero siempre que coincida con el hash, no importa cuál sea la contraseña original.

¿Para qué se utilizan las tablas arco iris?

Hoy las contraseñas ya no se guardan sin cifrar, al menos eso es lo que se espera. Cuando los usuarios de una plataforma fijan una clave de acceso para su cuenta, esta secuencia de caracteres no aparece en texto plano en una base de datos en algún servidor, puesto que no sería seguro: si encontrara la forma de entrar en ella, un hacker lo tendría muy fácil para acceder a todas las cuentas de un determinado usuario.

Para el eCommerce, la banca en línea o los servicios gubernamentales online esto tendría consecuencias fatales. En lugar de ello, los servicios online utilizan diversos mecanismos criptográficos para cifrar las contraseñas de sus usuarios de modo que en las bases de datos solo aparezca un valor hash (valor resumen) de la clave.

Incluso conociendo la función criptográfica que lo ha originado, desde este valor hash no es posible deducir la contraseña, porque no es posible reconstruir el procedimiento a la inversa. Esto lleva a los ciberdelincuentes a recurrir a los ataques de fuerza bruta, en los cuales un programa informático intenta “adivinar” la secuencia correcta de caracteres que constituye la contraseña durante tanto tiempo como haga falta.

Este método puede combinarse con los llamados “diccionarios” de contraseñas. En estos archivos, que circulan libremente en Internet, pueden encontrarse numerosas contraseñas que bien son muy populares o ya fueron interceptadas en el pasado. Los hackers prueban primero todas las contraseñas del diccionario, lo que les permite ahorrar tiempo, aunque, en función de la complejidad de las contraseñas (longitud y tipo

de caracteres), este proceso puede resultar más largo y consumir más recursos de lo esperado.

También disponibles en la Red y también un recurso para descifrar claves secretas, las tablas rainbow van un paso más allá de los diccionarios. Estos archivos, que pueden llegar a tener un tamaño de varios cientos de gigabytes, contienen un listado de claves junto con sus valores hash, pero de forma incompleta: para reducir su tamaño y así su necesidad de espacio en memoria, se crean cadenas de valores a partir de las cuales pueden reconstruirse fácilmente los demás valores. Con estas tablas los valores hash encontrados en un banco de datos pueden ordenarse con sus claves en texto plano.

Funcionamiento de las Tablas Arcoiris

Para poder entender cómo funcionan las tablas arco iris conviene echar un vistazo a la mecánica de los algoritmos de cifrado, pues esto permite comprender más fácilmente las ventajas de estas listas de búsqueda y el llamado compromiso tiempo-espacio.

Tecnología de cifrado

Desde que se comenzaron a aplicar funciones hash criptográficas en el cifrado, los algoritmos no han dejado de evolucionar y los estándares que hace diez años se consideraban inexpugnables hoy son vistos como graves vulneraciones de la seguridad. Todos, no obstante, tienen algo en común, y es que el contenido que debe cifrarse se somete a diversos algoritmos hasta que finalmente se genera un valor hash. Este valor resumen es normalmente una cifra hexadecimal con una longitud fija, que no depende de la del contenido inicial. Al final del proceso siempre resulta, por ejemplo, un valor hash de 128 bits.

Tres son los aspectos decisivos en el cifrado:

1. La misma entrada genera siempre el mismo valor hash: solo así este valor puede funcionar como suma de verificación (del inglés “checksum”). ¿Es la clave introducida idéntica a la que hay en la base de datos? El sistema solo autoriza el acceso cuando ambos valores hash coinciden.

2. Un valor hash debería ser siempre único: dos entradas diferentes no deberían

generar el mismo valor resumen, pues solo siendo únicos pueden garantizar que se ingresa la clave correcta. Como el número de valores hash posibles está limitado, pero el de posibles entradas no, es imposible descartar este tipo de coincidencias, llamadas colisiones en este contexto. Las funciones hash modernas y los valores hash con una longitud suficiente intentan mantener este riesgo a raya.

3. Los valores resumen no son reversibles, es decir, que a partir del valor resumen no es posible deducir el contenido original (la clave). Por ello tampoco es posible descifrar valores resumen, como se sostiene a veces de forma algo imprecisa. Solo pueden reconstruirse.

4. Las funciones hash deben ser muy complejas, pero no en exceso: si un algoritmo trabaja demasiado rápido, facilita el trabajo a los atacantes y ya no puede garantizar la seguridad. Pero la transformación tampoco debe ser excesivamente compleja porque en definitiva ha de llevarse a la práctica.

Funciones de reducción

Los valores hash contenidos en las tablas rainbow no se crean con ocasión de un ataque, sino con anterioridad, de modo que los hackers puedan hacerse con ellas y utilizarlas para encontrar claves de acceso. Pero como estos archivos son muy grandes, se aplica una función de reducción que permite ahorrar memoria. Esta función convierte al valor hash en un texto plano –no devuelve al valor original del valor hash, esto es, a la contraseña original, pues esto no es posible, sino que genera un texto completamente nuevo.

A partir de este texto se crea otro valor resumen nuevo, un proceso que en una tabla arco iris no sucede una sola vez, sino muchas, de forma que se genera una cadena. En la tabla definitiva, no obstante, solo aparecen la primera clave y el último valor resumen de la cadena. Con esta información y utilizando las mismas funciones de reducción es posible averiguar todos los demás valores. El valor hash que se quiere romper se reduce y se resume una y otra vez siguiendo las mismas reglas, comprobando cada resultado con los valores que figuran en la tabla para encontrar su clave correspondiente.

El desafío a la hora de crear una tabla reside en el hecho que la palabra inicial que representa el comienzo de una cadena no puede figurar como texto plano en otra cadena precedente.

Con este método puede reducirse en gran medida el tamaño de estas tablas, aun

teniendo todavía un volumen de varios cientos de gigabytes.

Compromiso espacio-tiempo

Se habla de una situación de compromiso espacio-tiempo o tiempo-memoria cuando la memoria se reduce a costa de una ejecución más lenta o a la inversa, el tiempo de ejecución se reduce incrementando el uso de la memoria. Un ataque de fuerza bruta necesita muy poco espacio, porque los cálculos criptográficos comienzan siempre de cero en cada ataque. En cambio, una tabla que contiene miles de millones de contraseñas junto con sus valores hash ocupa mucha memoria, aunque puede descifrar muy rápido. Las rainbow tables representan un acuerdo intermedio, pues, aunque también lleva a cabo cálculos en tiempo real, lo hace a pequeña escala, de modo que, en comparación con las tablas completas, reduce claramente las necesidades de memoria.

Mecánica de las tablas arco iris

La situación inicial es esta: dado un valor hash, se pretende conocer la clave de acceso que lo originó. En un primer paso, se busca este valor en la lista. Si se encuentra al comienzo o al final de una cadena, entonces es fácil encontrar la contraseña, porque solo habrá que reconstruir los pasos que recorrió la cadena hasta obtener el resultado que se busca. ¿Qué ocurre entonces cuando el valor resumen no se encuentra en la tabla?

En este caso, se comienza reduciendo el valor con la misma función con la cual se creó la cadena. El resultado se somete a su vez a la función resumen, proceso que se denomina hashear y que se repite tantas veces como sean necesarias hasta que se encuentre al valor resumen en algún punto final. Con todo, esto no significa que se haya encontrado la clave, aunque sí se ha encontrado la cadena en la cual se esconde el valor hash. Entonces se comienza en el punto inicial de la cadena y se lleva a cabo de nuevo esta alternancia de reducción y hashing hasta que se logra encontrar el valor hash que se busca y con él a la clave en texto plano.

Conclusiones y recomendaciones

En conclusión, las Tablas Arcoiris son un poderoso instrumento con el que es posible crackear contraseñas. A esta tarea se dedica con empeño un buen número de personas a ambos lados de la legalidad, unos por el beneficio que aspiran a obtener con ellas, los otros porque su trabajo como expertos consiste en comprobar periódicamente la efectividad de los estándares de seguridad vigentes y las tablas arco iris.
Una recomendación es mantenerse alejados de las aplicaciones web que restringen la longitud de su contraseña a una pequeña cantidad de caracteres. Esta es una clara señal de las rutinas de autenticación de contraseña de la vieja escuela vulnerables. La longitud y la complejidad de la contraseña extendida pueden ayudar un poco, pero no es una forma garantizada de protección. Cuanto más larga sea su contraseña, más grandes tendrán que ser las Rainbow Tables para descifrarla, pero un hacker con muchos recursos aún puede lograr esto.

Finalmente, la mejor manera de defenderse de las tablas arcoiris está destinado a desarrolladores de aplicaciones y administradores de sistemas. Están en primera línea cuando se trata de proteger a los a los usuarios contra este tipo de ataque.

Referencias bibliográficas

IONOS España (2019) Rainbow tables: qué son y cómo funcionan las tablas arco iris. Recuperado de: https://www.ionos.es/digitalguide/servidores/seguridad/rainbow-tables/

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica