Tablas rainbow y su uso

Pablo Menéndez Suárez
UO252406@uniovi.es

Resumen
Este trabajo trata de ayudar al lector a comprender lo que son la Tablas Rainbow, así como su funcionamiento en general, detallando el proceso de creación por el que pasan y el algoritmo que siguen a la hora de realizar un ataque. Para que el lector comprenda mejor su funcionamiento, el funcionamiento de dichas tablas será ejemplificado.

1. Introducción

A la hora de diseñar una aplicación que requiera de autentificación siempre se plantea un problema cuando se necesita almacenar las contraseñas de los usuarios en una base de datos. Éstas pueden ser almacenadas de varias formas, bien sea en texto plano (nada recomendable), cifradas con un algoritmo bidireccional o cifradas mediante un algoritmo unidireccional dando como resultado un "Hash". Ésta última es la más usada en sistemas seguros y también la más recomendable., ya que invertir el proceso de cifrado es muy difícil y la única manera de obtener las contraseñas es mediante la fuerza bruta. En este trabajo vamos a ver como apoyándonos en las tablas rainbow, podemos realizar fuerza bruta de una forma mucho más rápida y eficiente.

2. Tablas Rainbow

2.1 Definición

Las Tablas Rainbow, son un tipo de tablas pregeneradas utilizadas para la obtención de contraseñas por medio de fuerza bruta que nos permiten ahorrar tiempo de ejecución sacrificando espacio en disco y memoria. Este tipo de tablas almacenan una relación de pares de palabras en texto plano donde, por un lado está la palabra inicial y por otro lado la palabra final. El vínculo formado entre estas dos palabras viene dado por el uso de ambas en la función de resumen y reducción que representa la Tabla Rainbow. Existen diferentes tipos de Tablas Rainbow para cada algoritmo de cifrado, generalmente ocupan muchos gigas o incluso teras. Antes de pasar a hablar del funcionamiento de estas tablas y para comprender bien lo que acabamos de leer, debemos tener claros algunos conceptos.

2.2 Función Hash o de resumen

Una función hash o de resumen es una función que aplica una fórmula matemática a una entrada, normalmente un texto plano, dando como resultado una salida alfanumérica de longitud fija, conocida como hash, que solo puede ser obtenida a través de esa misma entrada.

2.3 Función de reducción

Una función de reducción es una función que transforma un hash en una cadena de texto plano. Es muy importante no interpretar mal este concepto. La función de reducción no es el proceso contrario a una función

hash, es decir, aplicar una función de reducción sobre un hash no te va a devolver su cadena original, si no que te va a devolver otra cadena cualquiera, ya que precisamente el objetivo de las funciones hash es que no se pueda realizar una función inversa.

2.4 Funcionamiento

2.4.1 Creación de Tablas Rainbow

Anteriormente hemos dicho que las Tablas Rainbow almacenan pares de palabras en forma de palabra inicial y palabra final. Pues bien, para la creación de dichas tablas se parte de una palabra inicial, que es un texto plano, y se le realiza una función de resumen obteniendo así su hash. Al hash que se obtiene se le aplica una función de reducción, dando lugar a otra palabra en texto plano a la cual se le volverá a aplicar una función de reducción y así sucesivamente. Este proceso finaliza cuando se ha realizado unas 40.000 veces y lo único que se almacena es la palabra inicial y la final. De esta manera rápidamente nos podemos dar cuenta del enorme ahorro de memoria que se produce, ya que pasa de almacenar 40.000 palabras a únicamente la de entrada y salida. Una vez obtenido el primer par de palabras este proceso se realizará con otra entrada distinta y así sucesivamente tantas veces como se desee. Una vez obtenidos todos los pares de palabras, se ordenan en orden alfabético de acuerdo al valor final, permitiendo así realizar búsquedas binarias que optimicen el trabajo. Cabe destacar que la tabla solo se genera una única vez y una vez generada ya se puede utilizar para la ruptura de múltiples hash.

2.4.2 Algoritmo de las Tablas Rainbow

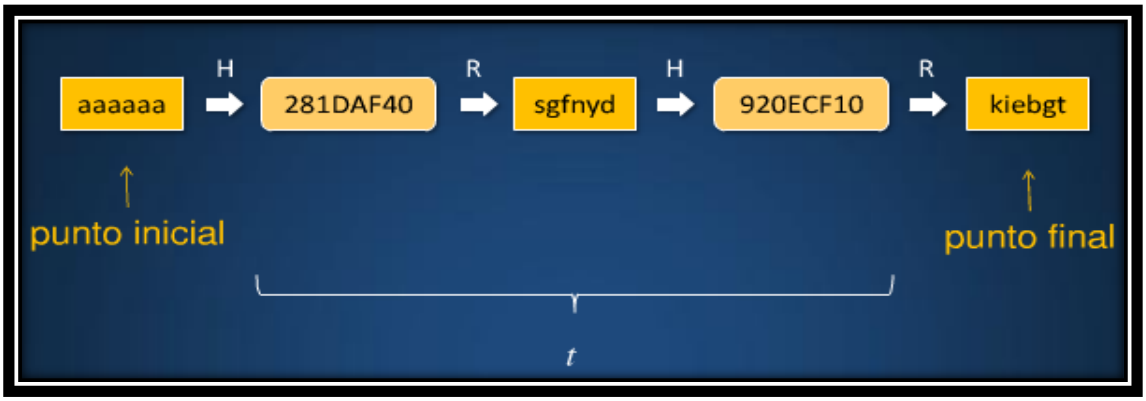
Ahora que ya sabemos como se crea una Tabla Rainbow, vamos a ver cómo sería el proceso para la obtención de una clave partiendo de un hash con una de estas tablas. El algoritmo que habría que seguir sería el siguiente:

1º Se realiza una función de reducción sobre el hash que tenemos.
2º Se comprueba si la palabra obtenida se encuentra entre las palabras finales de la tabla. En caso afirmativo saltamos al cuarto paso.
3º En caso de que la palabra obtenida no se encuentre entre los valores finales de la tabla se le aplica la función de resumen y volvemos al primer paso.
4º Si la palabra obtenida está entre las finales obtenemos la palabra inicial correspondiente a esta.
5º Le aplicamos la función de resumen.
6º Si el hash obtenido es igual al original hemos obtenido la palabra deseada, por lo que podemos pasar directamente al octavo paso.
7º En caso de que el hash obtenido no sea igual al original debemos aplicarle una función de reducción y volver al quinto paso.
8º Devolvemos la palabra encontrada antes de haberle aplicado la función de resumen.

2.5 Ejemplo del funcionamiento de una Tabla Rainbow

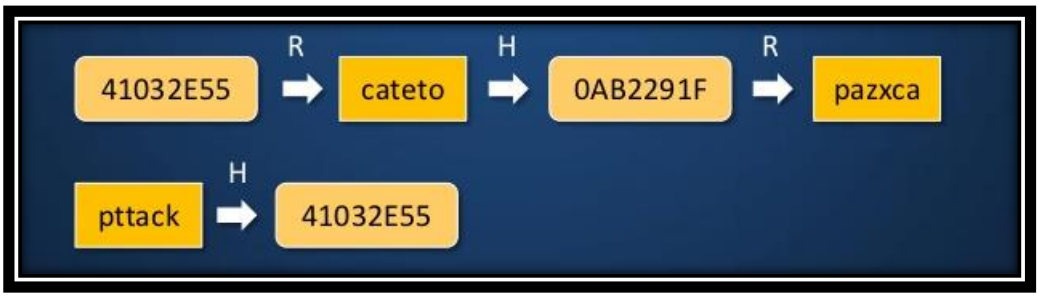
Es posible que hayas llegado a este punto del documento sin tener del todo claro el funcionamiento de estas tablas, de modo que, para hacerlo más comprensible, vamos a ilustrar el funcionamiento de éstas mediante un ejemplo.

Antes de empezar con el ejemplo, vamos a realizar un breve resumen de como sería la creación de estas tablas ayudándonos de imágenes, con el fin de entender mejor lo visto anteriormente y lo que viene después. Recordando lo visto anteriormente, para la creación de estas tablas partimos de una palabra a la que le vamos a aplicar una función hash. Una vez obtenemos el hash resultante, le aplicamos a éste una función de reducción obteniendo así otra palabra distinta a la inicial y así sucesivamente. Podemos hacernos una idea del proceso en la siguiente imagen:



En la imagen podemos observar como partiendo de una palabra inicial, en este caso “aaaaaa” obtenemos una palabra final “kiebgt”. Entre estas dos palabras se encuentra todo el proceso descrito anteriormente. La flecha con una “H” encima representa que se está aplicando una función hash, mientras que la flecha con una “R” representa que se aplica una función de reducción. Obviamente el proceso para llegar de la palabra inicial a la final se encuentra altamente simplificado en esta imagen, ya que sería un proceso mucho más largo. Una vez obtenidos el primer par de valores se pasaría a obtener el segundo par y así sucesivamente dando lugar a una Tabla Rainbow con un aspecto similar (aunque muy simplificado) al de la siguiente imagen:

Ahora ya podemos empezar con el ejemplo. Supongamos que hemos conseguido acceder a la base de datos donde se almacenan las contraseñas de los usuarios de una aplicación y queremos saber la contraseña de un usuario en concreto, en este caso del usuario "Pepe". Para nuestra desgracia, las contraseñas se encuentran almacenadas en forma de hash, por lo que no podemos saber cuales son las verdaderas claves de los usuarios. Sin embargo, tenemos una Tabla Rainbow exactamente igual a la vista anteriormente a nuestra disposición, así que vamos a intentar obtener la clave del usuario "Pepe" a través de ella.
Primero cogemos el hash que se corresponde al usuario "Pepe". En este caso supongamos que es "41032E55". Le aplicamos una función de reducción y la palabra obtenida es "cateto". Comprobamos si la palabra se encuentra entre las finales de la tabla y nos damos cuenta de que no es así, por lo que le aplicamos una función hash obteniendo "0AB2291F". Al hash obtenido le volvemos a aplicar una función de reducción y la palabra resultante es "pazxca". Comprobamos si esta palabra se encuentra entre las finales y así es. Ahora cogemos la clave inicial correspondiente a la final que acabamos de obtener, en este caso es "pttack" y le aplicamos una función hash dando lugar al hash "41032E55" que, si nos fijamos, es el mismo hash que el inicial, por lo que podemos concluir que la clave del usuario "Pepe" es "pttack".
Este proceso se puede ver más claro en la siguiente imagen:



3. Conclusión

Las Tablas Rainbow son una muy buena elección a la hora de realizar ataques de fuerza bruta ya que por lo que hemos podido ver nos permite realizar el trabajo de una manera más rápida y eficiente. Sin embargo, el sacrificio de memoria realizado para su almacenamiento es un factor que hay que tener en cuenta.

4. Referencias

- http://www.flu-project.com/2011/09/rainbow-tables-tablas-arco-iris_5.html
- https://security.stackexchange.com/questions/379/what-are-rainbow-tables-and-how-are-they-used
- https://en.wikipedia.org/wiki/Rainbow_table
- http://kestas.kuliukas.com/RainbowTables/
- https://www.genbetadev.com/seguridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales
- Apuntes de clase