Tecnológico de Monterrey

Reflexión Actividad 5.2

Jorge Humberto Guillen Berrueta, A01639681

9/6/22

Programación de estructuras de datos y algoritmos fundamentales

Las tablas hash son estructuras de datos que se usan para almacenar datos para luego buscarlos con operaciones de búsqueda. Una tabla hash guarda dos datos: la clave y el valor. La clave es única para cada elemento de la tabla y es el dato que se usa para buscar un determinado valor. Por ejemplo, una palabra es una clave mientras que su significado es su valor dentro de un diccionario. Dentro del contexto de la ciberseguridad, el hash se implementa principalmente en algoritmos de cifrado. Las entradas no tienen sentido para los hackers sin una clave de descifrado. Los hash tienen tres propiedades claves que agregan características de seguridad a las funciones típicas de ciberseguridad, lo que dificulta la detección de un mensaje o información sobre el mensajero y el destinatario.

1. Están libres de colisiones: no se deben asignar dos hashes de entrada al mismo hash de salida
2. Pueden ocultarse: es difícil adivinar el valor de entrada a partir de su salida
3. Deben de funcionar bien con rompecabezas.

Algunas implementaciones prácticas de hashes en la ciberseguridad pueden ser comprobar la integridad de archivos usando una “cadena de confianza” que revisa que el mensaje no sea manipulado. También se pueden verificar contraseñas, de hecho la gran mayoría de

páginas web guardan las contraseñas de sus usuarios como hashes en lugar de archivos de texto normales.

Cuando dos claves generan un hash idéntico, se crea una colisión. Una buena función hash no debe producir el mismo valor hash a partir de entradas diferentes. Aun así las colisiones no son raras de ver. Al haber más colisiones en la tabla hash, el resumen así como la lista completa de direcciones accesadas cambia y no es 100% precisa ya que habría valores repetidos.