Instituto Tecnológico de Estudios Superiores Monterrey

CAMPUS QUERÉTARO

Análisis y diseño de algoritmos avanzados

Ramona Fuentes Valdéz

TC2038 Grupo 601

Actividad integradora 1
Transmisiones de datos comprometidas

PRESENTAN

José Armando Rosas Balderas	A01704132
Diego Perdomo Salcedo	A01709150
Ramona Nájera Fuentes	A01423596

Fecha:
01/10/2023

Problemática

Hoy en día las transmisiones de datos de un lugar a otro son cosa de lo más común, como por ejemplo, cuando recibimos y mandamos mensajes, al estar jugando un videojuego en línea o incluso en una llamada telefónica. Sin embargo, los datos contenidos en estas transmisiones pueden contener información maliciosa que puede dañar nuestros equipos o comprometernos de diferentes maneras.

En este proyecto, dados ciertos códigos maliciosos que conocemos, nuestra labor es inspeccionar algunas transmisiones y descubrir si tienen código malicioso.

Propuesta de solución

Parte 1: Detección de código malicioso

Dadas las transmisiones y los segmentos de código malicioso a identificar, se realizó una búsqueda de patrones para encontrar todas las coincidencias por archivo.

El algoritmo implementado fue KMP porque reducía la búsqueda a una complejidad lineal (O(N)), pero se mantenía simple porque se trata de un acercamiento similar a la fuerza bruta.

La optimización se encuentra en que usa la información de comparaciones anteriores para determinar desde dónde retomar la búsqueda del patrón una vez que se encontró una coincidencia o fracasó la búsqueda anterior.

Parte 2: Detección de código espejado

Bajo la suposición de que el código malicioso siempre tiene código espejado, se identificó el palíndromo más grande por cada transmisión que se presentó.

El algoritmo de Manacher para búsqueda del palíndromo más grande es el más óptimo ya que tiene una complejidad algorítmica lineal (O (N)) y es una mucho mejor alternativa a la fuerza bruta, cuya complejidad es de O(N^2). Este algoritmo logra ser eficiente dada una característica especial de los palíndromos, y esta es que se pueden ahorrar iteraciones cuando se buscan palíndromos dentro de palíndromos.

Parte 3: Similitudes entre transmisiones

En esta última fase se pretendía encontrar similitudes entre archivos de transmisión, desplegando la subcadena común más larga entre pares de archivos.

Aquí, optamos por usar la programación dinámica para construir una solución simple que nos permitiera realizar la comparación entre archivos una sola vez y resultó en una complejidad cuadrática ($O(N^2)$).

El algoritmo implementado consiste en construir una matriz donde cada carácter de una cadena se compara con cada carácter de la otra y en caso de coincidir, se almacena la suma de las coincidencias anteriores más uno.

De esta manera, al terminar la comparación, el recuadro con el número más grande contiene la longitud de la subcadena común más larga y la posición de la matriz donde se encuentra indica la posición de la coincidencia en las cadenas originales.

Conclusiones finales

En la solución de este proyecto buscamos algoritmos diferentes a la fuerza bruta, ya que cuando se trata de buscar código malicioso, ya sea en el ámbito personal, o en una empresa, la detección y eliminación de este debe ser lo más rápido posible para evitar algún desastre. Una vez comprendimos la aproximación de cada uno de los algoritmos, la programación no fue muy difícil.

Finalmente, como equipo comprendimos la importancia de buscar algoritmos eficientes y sobre la inseguridad que existe en el mundo de la informática. Los algoritmos de detección y prevención ante código malicioso son muy importantes y es de mucha importancia su implementación y rapidez.