Universidad de la Habana

Facultad de Matemática y Computación

Test para la detección de patrones DIAG y LINE en las contraseñas gráficas de PassPoint, basada en la cantidad de triángulos de Delaunay

Autor: Ovidio Navarro Pazos

Tutor(es): MrS.Lisset Suárez Plasencia
MrS.Joaquín A. Herrera Macías

La Habana, Cuba
11 de diciembre de 2024

Índice general

Introducción

En la actualidad, una gran mayoría de los usuarios tiende a ignorar las recomendaciones de seguridad al momento de crear contraseñas alfanuméricas. Es común observar el uso de contraseñas cortas y cargadas de información personal, lo cual facilita su memorización, pero también aumenta significativamente su vulnerabilidad frente a ataques de fuerza bruta o de diccionario [[1,4,5,6]].

Para abordar estas debilidades, se han desarrollado nuevas alternativas, entre las cuales destacan las contraseñas gráficas. Este enfoque se basa en la capacidad humana de recordar patrones visuales en una imagen con mayor facilidad que largas cadenas de caracteres alfanuméricos. En este tipo de contraseñas, el usuario debe recordar una imagen o partes específicas de ella mediante la selección de determinados puntos, imágenes que dadas sus características posean un amplio espacio para la construcción de sus contraseñas y de este modo ser más resistentes a los ataques de diccionarios, obteniendo un espacio de búsqueda mucho más amplio y resistente a los ataques comunes.

En este trabajo, específicamente, vamos a trabajar sobre el PassPoint[1], una técnica de autenticación gráfica que en su fase de registro consiste en seleccionar cinco puntos de una imagen elegida por el usuario. Durante la autenticación, el usuario debe hacer clic en una determinada vecindad y en el mismo orden de los puntos registrados. Entre las debilidades de esta técnica se encuentran los Hotspots[6](puntos más probables a seleccionar por el usuario), además diversos patrones predefinidos que los usuarios tienden a seguir durante el registro para facilitar la memorización. Estos patrones incluyen formas específicas como Z, W, C, V, patrones agrupados o regulares, y patrones LOD, DIAG o LINE (formas de línea o diagonales).

La tendencia de los usuarios a crear patrones entre los puntos seleccionados, ya sea de manera independiente o en combinación con Hotspots, constituye una debilidad importante. Esto hace que las contraseñas generadas sean menos aleatorias y más susceptibles a ataques basados en diccionarios específicos. Por ello, resulta fundamental desarrollar pruebas que detecten la existencia de estos patrones en las contraseñas antes de su uso, ya que contribuirían significativamente a mejorar la seguridad de la técnica PassPoint.

A lo largo de los últimos años, se han realizado pocas investigaciones enfocadas en este tema. Entre los métodos más comunes para evaluar la Aleatoriedad Espacial Completa se encuentran: el test de la función K-Ripley, el test de la función G, que analiza la distancia al vecino más cercano, y el test de la función F, que se centra en la distancia de espacio vacío. Sin embargo, en [9-10 sensor] se demuestra que, en el contexto de PassPoint, dos de estos métodos son ineficaces para detectar contraseñas gráficas compuestas por patrones agrupados. Por otro lado, en [15, 16] se evidencia que los tres tests no logran identificar ni el agrupamiento ni la regularidad en las contraseñas de este escenario. Hasta ahora, en la bibliografía revisada, se han encontrado dos tests efectivos (tesis de Liset y Joakin) para identificar contraseñas no aleatorias que presentan patrones agrupados o regulares en el contexto de PassPoint. Estos métodos se basan, en el caso de (Liset), en la distancia

promedio de los perímetros de los triángulos de Delaunay, y, en el caso de (Joakin), en la distancia media entre cinco puntos.

Teniendo en consideración que las propiedades de una triangulación de Delaunay brindan la capacidad de obtener información acerca de la interrelación entre puntos, se ha empleado como una herramienta en la mitad de la década de 1980 para identificar configuraciones de puntos. En el estudio realizado por Chiu [22], se emplearon varias de estas propiedades para reconocer la agrupación y la regularidad entre los puntos. Específicamente, la característica del“ ángulo máximo de un triángulo de Delaunay”, según la literatura revisada, nunca había sido utilizada previamente para identificar otro tipo de configuraciones además de las agrupadas o regulares. No obstante, dado que los patrones DIAG y LINE se distinguen por presentar un ángulo cercano a 0° entre dos segmentos consecutivos, en [sensor] se propuso y demostró que la media de los ángulos máximos de los triángulos de Delaunay generados a partir de los puntos de las contraseñas gráficas de PassPoint es un estadígrafo eficaz para detectar la presencia de patrones DAIG y LINE, incluso con un número limitado de puntos. En [15] se entendía como el ángulo formado entre dos segmentos consecutivos ,el menor de los dos ángulos que forman la intersección de la prolongación de los segmentos de una contraseña.Nos referiremos al mayor de estos dos ángulos como el ángulo adyacente entre dos segmentos .

Según los resultados obtenidos en (sensor) se sugiere investigar la eficacia de un test de detección de los patrones DIAG y LINE utilizando como estadígrafo el promedio de los ángulos máximos de los triángulos de Delaunay pero realizando análisis independientes según la cantidad de triángulos en su triangulación (3,4,5) y realizar un análisis comparativo respecto a los resultados obtenidos en (sensor).

Problema de investigación:

Detectión contraseñas que sigan los patrones suaves DIAG y LINE en PassPoint, basada en la cantidad de triángulos de Delaunay.

Objetivo de estudio:

Comprobar si el estadígrafo “promedio de los ángulos máximos de las triangulaciones de Delaunay ”, es más eficaz si se trabaja individualmente sobre las distintas cantidades de triángulos existentes en las triangulaciones.

Campo de acción:

Detección de contraseñas gráficas no aleatorias en el escenario PassPoint utilizando las triangulaciones de Delaunay.

Hipótesis:

Es posible que utilizar el estadígrafo “promedio de los ángulos máximos de las triangulaciones de Delaunay”de manera individual sobre las distintas cantidades de triángulos existentes en las triangulaciones es mas eficaz que trabajarlo de manera general.

Idea de la solución:

Para cada cantidad de triángulos en las triangulaciones de Delaunay para 5 puntos:

- Encontrar como distribuyen las contraseñas aleatorias
- Realizar un análisis estadístico obteniendo los errores tipo I y II
- Realizar una comparación con los resultados obtenidos en (SENSOR).

Objetivos

Objetivos generales:Detectar[1] la no aleatoriedad en las contraseñas gráficas que siguen patrones DIAG o LINE en PassPoint para cada número de triángulos en una triangulación de Delaunay

Objetivos específicos:

- Crear un criterio de desición basados en el promedio de los ángulos máximos de los triángulos de Delaunay para cada posible cantidad de triángulos en su triangulación.
- Para cada cantidad de triángulos, obtener estimaciones teóricas del número esperado de fallos en la detección de contraseñas gráficas débiles.

1. Marco Teórico

Incluye el marco teórico, revisiones de la literatura y conceptos clave relacionados con tu trabajo.

1.1. Conceptos Fundamentales

En esta sección se definen los conceptos clave que son relevantes para este trabajo.

1.1.1. Definición del Término A

El término A se refiere a...

1.1.2. Definición del Término B

El término B, por otro lado, se entiende como...

1.2. Teorías Relacionadas

Esta sección presenta las teorías principales que fundamentan el estudio.

2. Metodología

Describe la metodología utilizada en tu investigación, incluyendo los métodos, herramientas y procedimientos.

3. Resultados

Presenta los resultados obtenidos durante tu investigación.

4. Discusión

Analiza los resultados y compara con otros estudios o referencias relevantes.

5. Conclusiones y Recomendaciones

Resume los hallazgos principales y ofrece recomendaciones futuras.

Bibliografía

[1] Autor A, et al. Título del artículo. Revista, año.

Bibliografía

A. Anexo A

Incluye aquí cualquier información adicional como encuestas, gráficos, o tablas complementarias.