Universidad X

Título de la Tesis

Por

Tu Nombre

Fecha: 8 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], que son los puntos más probables a seleccionar por el usuario, y 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.

Existen varios articulos publicados sobre el tema en los ultimos años, en (articulo legon2019)se propone un modelo probabilisto de autenticación gráfica que permite medir en la practica el nivel de autenticidad de el usuario en alto, medio y bajo , Hasta el momento en la bibliografia consultada se encuentran dos test efectivos(tesis lisset y joakin) para detectar contraseñas no aleatorias formadas por patrones agrupados o regulares e el escenario PassPoint, basados en (tesis de liset) en la distancia promedio de los perímetros de los triángulos de Delaunay y (joakin)en distancia media entre 5 puntos.En (sensor) se realiza un test de deteccion de los patrones suaves DIAG y LINE basado en el promedio angulos maximos de sus triangulos de delaunay, dados los resultados obtenidos se

demostró que el promedio de los angulos maximos de los triangulos de delaunay es un estadistico eficas para detectar contraseñas que sigan un patron DIAG o LINE

OBJETIVOOOOOOOO

En [2informe] se demostró que el promedio de los ángulos máximos de los triángulos de la traingulación de Delaunay de una contraseña es un estadígrafo eficiente para detectar contraseñas que sigan un patrón DIAG o LINE. El objetivo de este trabajo es hacer un test con las contraseñas que posean 3 triángulos en su triangulación de Delaunay y comparar estos resultados con los obtenidos en [2].

El resto del trabajo se encuentra formado con 3 secciones : La sección 2 posee una descripción de las triangulaciones de Delaunay y de los patrones DIAG y LINE . En sección 3 se muestra el test ,los experimentos y los resultados obtenidos. En la sección 4 tenemos una comparación del el test propuesto con el que se encuentra en[2]

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

A. Anexo A

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