Ciencias Matemáticas, Vol. 33, No. 1, Pag. 75-81, 2019

Patrones en el orden de los clics y su influencia en la debilidad de las claves en la Técnica de Autenticación Gráfica Passpoints
Clic Order patters and their influence on the weakness of the passwords in the Passpoints Graphic Authentication Technique

Osviel Rodriguez Valdés[1]*, Carlos M. Legón[2], Raisa Socorro Llanes[3]

Resumen Para garantizar la seguridad y privacidad de acceso a los sistemas digitales, tradicionalmente se han utilizado las contraseñas alfanuméricas. Los usuarios casi siempre ignoran las recomendaciones para conformar contraseñas seguras, las que emplean son sencillas y fáciles de predecir. Como alternativa, las contraseñas gráficas requieren que el usuario recuerde una imagen o partes de ella en vez de grupos de caracteres alfanuméricos. Estas poseen espacios de claves considerables y ayudan a que el usuario recuerde mejor su secreto. En este artículo se resumen los principales tipos y estrategias de ataques de diccionario a contraseñas gráficas y se profundiza en la influencia de los patrones de clics lineales en la seguridad de las claves. Existe evidencia que demuestra que su existencia es independiente de las imágenes de fondo usadas en el proceso de registro-autenticación. Además, estos patrones tienen un gran impacto en la fortaleza de las claves ya que los usuarios tienden a seguir patrones de flujo por la forma en la que naturalmente perciben las imágenes.

Abstract To guarantee the security and privacy of access to digital systems, traditional alphanumeric passwords have been used. Users almost always ignore recommendations for safe passwords, these are simple and easy to predict. As an alternative, graphic passwords require the user to remember an image or parts of it instead of groups of alphanumeric characters. These have considerable password spaces and help the user remember their secret. In this article, we summarize the types and strategies of dictionary attacks against graphic passwords and it delves into the influence of linear click patterns on password security. There is solid evidence that it's existence is independent of the background images used in the registration-authentication process. In addition, these patterns have a great impact on the strength of the keys since users tend to follow flow patterns by the way they naturally perceive the images.

Graphical password, Authentication, Patrones de Clics Lineales, Ataque de semillas humanas, Contraseñas débiles, Espacio de clave.
Graphical password, Authentication, Linear Click patterns, Human-seeded attack, Weak passwords, Password space.

[1] *Departamento de Programación y Sistemas Digitales, Universidad de las Ciencias Informáticas, La Habana, Cuba, osviel@uci.cu*
[2] *Instituto de Criptogtafía, Universidad de la Habana, La Habana, Cuba*
[2] *Universidad Tecnológica de la Habana José A. Echeverría, La Habana, Cuba*
***Autor para Correspondencia**

Introduction

Las Contraseñas Gráficas (CG) ganan terreno sobre las tradicionales Contraseñas Alfanuméricas (CA) dado que se basan en la bien documentada evidencia de que las humanos poseen mayor habilidad para recordar imágenes que palabras parte de ella en vez de una palabra compuesta de caractéres alfanuméricos. Las CA son siempre inseguras [Itti and Koch, 2001, Valdés et al., 2018]. Como alternativa, las CG requieren que el usuario recuerde una imagen o [Vorster and van Heerden, 2015]. El gran problema de estas radica en que para poder recordarlas con facilidad los usuarios escogen las que son sencillas y con significado personal; estas en consecuencia son fáciles de atacar [Thorpe and van Oorschot, 2007].

Dentro de las Técnicas de Autenticación Gráficas (TAG) ha recibido especial atención el PassPoints [Bhong and Shahade, 2013, Wiedenbeck et al., 2005]. El PassPoints requiere que el usua-

rio seleccione un conjunto de puntos (cinco en total) sobre una imagen [Blonder, 1996]. Este es simple y efectivo, además soporta modificaciones que puedan personalizar sus implementaciones para cada escenario en particular. Las desventajas principales del PassPoints radican en la calidad de las imágenes que se utilizan en el proceso de autenticación [1], la existencia de patrones por la forma en la que el usuario establece su contraseña (*Clic-order patterns*) y en el uso de mecanismos de discretización que introducen vulnerabilidades propias de su funcionamiento [Valdés et al., 2018].

Ataques de diccionario efectivos se han materializado para la Técnica de Autenticación Gráfica PassPoints. Estos buscan explotar dos características en la selección de la contraseña: los puntos más probables conocidos como HotSpots y los Patrones de Clics también conocidos como Patrones de Clics Lineales (PCL). Los HotSpots son los puntos de una imagen más probables a seleccionar por el usuario. Estos se pueden pronosticar utilizando Técnicas de Procesamiento de Imágenes (TPI) para detectar bordes, esquinas, centroides y cambios de intensidad. Los patrones lineales de clics (PLC) son las relaciones en cuanto al orden, el sentido, espaciado y la ubicación de los puntos en las CG [Comaniciu and Meer, 2002]. Ambas características constituyen debilidades de las contraeñas gráficas que contribuyen a que sean predecibles [Zhu et al., 2013].

En este artículo se profundiza en la forma de selección de los puntos que hace el usuario a partir de los modelos de atención y leyes de percepción, para relacionarlos entre si. Estas formas de selección de contraseñas impactan en la seguridad puesto que son fácilmente explotadas por ataques que buscan PLC en la ubicación y orden de los puntos (Click-order pattern) en la Técnica de Autenticación Gráfica Passpoints.

Métodos

1. Modelos visuales de atención

Los Modelos Visuales de Atención (MVA) estudian la forma en la que las personas observan una imagen. Se estima que un grupo significativo de usuarios escoge los puntos siguiendo estos patrones [Salehi-Abari et al., 2008]. De esta manera se pueden construir diccionarios con los grupos de puntos más probables a seleccionar por el usuario.

Los modelos computacionales de atenciçón *Botton-up*, se definen normalmente por características de las imágenes digitales tales como: la intensidad, el color y la orientación [Itti et al., 1998] [12]. Por otra parte los modelos computacionales *Top-down*, pueden ser definidos por entrenamiento. La dificultad de estos últimos se basa en que la tarea *Top-down* debe ser predefinida (ej. encontrar personas en una imagen) en un grupo de imágenes que se etiquetan con áreas que contienen a los sujetos [Salehi-Abari et al., 2008].

Nos enfocaremos en la propuesta de Itti [Itti et al., 1998, Itti and Koch, 2001] ya que existe evidencia empírica de que este captura la forma en la que las personas observan una imagen desde lo profundo hacia arriba (*Botton-up*) [Ouerhani et al., 2004]. La idea principal de esta propuesta es que algunas áreas de una imagen, son "salientes" o de alguna manera resaltan por lo que difieren del resto en su entorno. De esta manera dada un imagen el modelo devuelve las localizaciones y el orden en que el ser humano de forma inconsciente y automática la observa. El proceso se compone de dos etapas. En la primera etapa se crea un mapa de "salientes" basado en las caracterísiticas visuales. En la segunda etapa se usa una red neural "winner-take-all" con el objetivo de replicar la forma en la que el usuario observaría la imagen. Thorpe et al. en [Thorpe and van Oorschot, 2007] desarrolla un ataque automático de diccionario que se basaba solo en variaciones de la primera etapa donde utilizaba detección de esquinas para encontrar puntos referenciables; luego en [Salehi-Abari et al., 2008] se describe como sería la segunda etapa del proceso.

La idea principal (primera etapa) de este método sirve de soporte para las técnicas de análisis y procesamiento de imágenes. Estas se basan en la detección de esquinas y centroides así como la aplicación de herramientas y algoritmos de inteligencia artificial para detectar objetos en las imágenes.

2. Leyes de Gestalt

Es razonable pensar que los usuarios escogerán puntos en forma de curvas que luzcan naturales a la forma en que se observa las imágenes y que de esta manera puedan recordarlas fácilmente. Mientras que algunas personas encuentran más sencillo recordar pequeños pedazos de información, otro grupo significativo prefiere sin embargo escoger puntos que poseen relación parcial o total entre sí [van Oorschot and Thorpe, 2011, Van Oorschot et al., 2010] cumpliendo con las denominadas leyes de Gestalt.

En Alemán Gestalt significa "forma", los principios de esta teoría fueron propuestos por Max Wertheimer en 1912; pero el concepto surgió inicialmente en el 1890 en un artículo titulado "Las cualidades de Gestalt"[King and Wertheimer, 2005]. Max introdujo cinco leyes de organización de la percepción:

- **Ley de la proximidad o cercanía:** Nuestra percepción tiende a agrupar los objetos cercanos. En el anexo 1 figura 1(a) observamos 3 columnas dada la separación entre los círculos.
- **Ley de la similitud:** nuestra visión tiende a agrupar los objetos similares en forma. En el anexo 1 figura 1(b) vemos cuatro filas dada la similitud de colores.
- **Ley de continuidad:** Los objetos que se encuentran siguiendo una dirección continua son visualmente agrupados. En el anexo 1 figura 1(c) vemos dos lineas que se cortan en ves de 4 que se unen en el medio.
- **Ley de cierre:** Nuestra visión tiende a percibir un todo manteniendo el balance y la armonía de la estructura. En el anexo 1 figura 1(d) vemos una "S".

[1] Las imagenes pueden contener puntos o áreas más atractivas para que el usuario las seleccione como su clave (HotSpots)

- **Ley del destino común:** Nuestra visión tiende a agrupar los objetos que se mueven en la misma dirección.

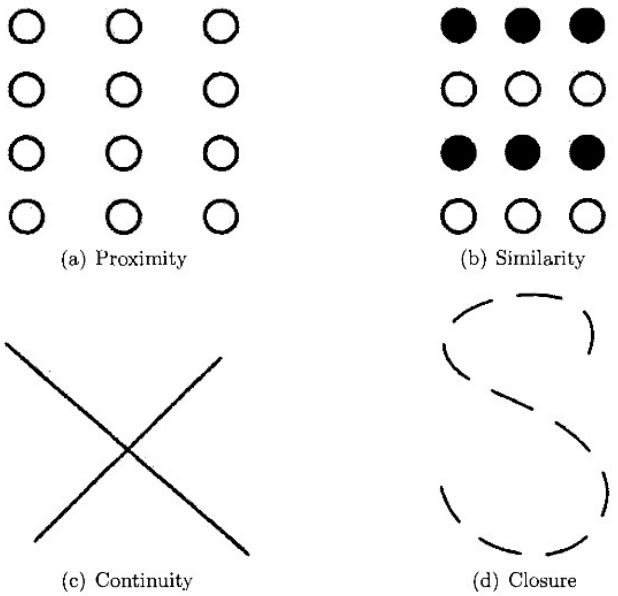

Figura 1. Leyes de Gestalt de la percepción visual.

3. Métodos para construir diccionarios de contraseñas gráficas

Los ataques de diccionario consisten en intentar inferir el valor de una contraseña probando todas las palabras del diccionario. Se diferencian de los ataques de fuerza bruta puesto que limitan la búsqueda a las combinaciones más probables. Los ataques de este tipo pueden llegar a ser muy efectivos; en un pequeño estudio de casos en [Klein, 1990] el 25 % de 14000 contraseñas fueron atacadas con solo 3 millones de entradas en un diccionario de 21,5 bits. Siguiendo el método anterior en [Van Orschot and Thorpe, 2005] un diccionario de 21,5 bits puede ser agotado en 0,22 segundos por un procesador Pentium 4 a 3,2 GHz. Para las CG estos en grán medida dependen de la composición particular de las imágenes, siendo para algunas muy alta la efectividad con que se logran obtener las contraseñas y para otros casos muy bajo.

En las investigaciones de [**?**, van Oorschot and Thorpe, 2011, Chiasson et al., 2009, Salehi-Abari et al., 2008] que fueron hechas sobre el PassPoints mezclan Técnicas de procesamiento de imágenes (TPI) con probabilidades, heurística, inteligencia artificial y patrones de selección en contraseñas gráficas para construir diccionarios. A partir de estas, se pueden identificar entonces tres métodos básicos para la construcción de diccionarios de contraseñas gráficas: Primero, técnicas de procesamiento digital de imágenes para detectar HotSpots (ej. bordes, centroides, esquinas y objetos a partir de heurística, probabilidades, inteligencia artificial y redes neuronales), segundo, detección de patrones en la forma y orden de selección de los puntos sobre la imagen a partir de las leyes de forma y percepción de los usuarios y tercero, combinación de las técnicas anteriores.

4. Estrategias de ataques basados en TPI

Las TPI, aprovechando las capacidades de las computadoras modernas, permiten analizar miles de datos simultáneamente y cruzarles para encontrar coincidencias. Este procedimientos utiliza a profundidad información recopilada del comportamiento de los usuarios y herramientas digitales para encontrar: salientes, bordes, esquinas, centroides, rostros humanos o partes de ellos, objetos, zonas de colores intensos, etc. A continuación se describen algunos de los métodos de ataques más exitosos.

4.1 Ataques de Semillas humanas (Human Seeded Attack)

En este tipo de ataques se utiliza la información recopilada de un grupo de usuarios para predecir las claves que otro grupo puede escoger sobre una imágen [van Oorschot and Thorpe, 2011]. Utiliza como hipótesis la idea de que los puntos seleccionados por un grupo arbitrario de personas va a tener un alto grado de coincidencia con los que seleccione otro grupo distinto de personas. De esta manera se pretende que las claves almacenadas de un grupo de usuarios pueda ser utilizada para estimar el comportamiento de otro grupo y de esta forma construir un diccionario de ataque. En [Thorpe and van Oorschot, 2007] aseguran que pueden pronosticar correctamente el 36 % de las claves dentro de 2^{31} conjeturas (o 12 % dentro de 2^{16} conjeturas) en el primer intento y el 20 % dentro de 2^{33} conjeturas en un segundo intento. Este método en esencia depende de la composición de las imágenes; se resalta en la investigación que para algunas imágenes con composición aleatoria es más difícil efectuar un ataque exitoso dado que se necesitarían mayores muestras iniciales. Como parte de este estudio se analizó además el efecto de los PLC (Se profundizará en ellos en la sección siguiente) como forma de capturar la relación entre los clics que conforman una clave. En [van Oorschot and Thorpe, 2011] se determinó que en efecto estos patrones reducen el tamaño del diccionario pués muchos usuarios utilizan estas predisposiciones como reglas nemotécnicas para recordar sus claves. Por lo que la técnica original se vuelve más precisa cuando se cruzan los datos con los diccionarios de PLC.

4.2 Ataques automáticos puros (Purely Automated Attacks)

En [Thorpe and van Oorschot, 2007] también se investigó un ataque automático puro utilizando TPI. Este ataque creaba el diccionario modelando las decisiones de un usuario utilizando un grupo de métodos y herramientas de procesamiento de imágenes. La idea es que este métodos ayude a predecir los puntos críticos por medios automáticos, lo que lleva a búsquedas más eficientes para ataques exhaustivos. Como premisa, para que un punto fuera candidato a escogerse por el usuario este debía poderse identificar con presición y a la

vez ser distinguible de su entorno. Para lograr estas premisas se implementa una variación del MVA de Itti, Button-up y se combina con el método de detección de esquinas de Harris detallado en [Harris and Stephens, 1988]. La detección de esquinas escoge áreas de una imagen que tienen variación de intensidad en dirección horizontal y vertical.

Como resultado se obtiene una lista de puntos candidatos con la cuál se puede efectuar un ataque de diccionario. Con este método se lograron obtener el 30 % y 29 % de las claves para algunas imágenes bien definidas, pero en otros casos los resultados están por debajo del 2 %. Esto implica que para algunas imágenes este tipo de ataques no es efectivo. También los autores determinan que el método funciona mejor en imágenes que el MVA devuelve resultados más exactos y decisiones más definidas. En este método no se tuvo en cuenta estrategias nemotécnicas pero los autores reconocen que podría ser mejorado utilizando los PLC.

5. Ataques basados en detección de patrones

Los patrones son lineas rectas, curvas suaves, arcos o formas geométricas simples formadas por la selección del usuario en una CG. Las personas prefieren recordar menores piezas de información visual [Luck and Vogel, 1997] y tienden a agrupar información para ayudar a la memorabilidad [Cowan., 2000]. Los ataques de este tipo toman ventaja de las debilidades en la fase de creación de la contraseña para crear el diccionario [Gao et al., 2013]. Las dependencias entre los puntos que el usuario seleccione pueden reducir drásticamente el espacio de claves [van Oorschot and Thorpe, 2011, Vorster, 2014]. Por lo que combinados con otras estrategias son efectivos puesto que no dependen de la composición específica de la imagen en cuestión.

5.1 Patrones identificados en la forma y orden en que el usuario escoge los puntos

En la TAG Passpoints existen comportamientos de los usuarios muy interesantes descritos en [Chiasson et al., 2009] que fundamentan la idea de que el usuario distribuye los puntos en composiciones independientes de las imágenes de fondo.

- **Distribución de los puntos:** Por ejemplo en el Passpoints, los usuarios tienden a seleccionar el primer punto comenzando por la parte izquierda superior de la imagen y seleccionar los demás hasta la esquina inferior derecha de la misma. Por lo que existe una clara progresión de izquierda a derecha y de arriba hacia abajo. Incluso es posible determinar qué áreas de una imagen son más propensas a contener puntos basándose solamente en el orden numérico en que se seleccionaron sin ningún conocimiento sobre la imagen en cuestión.

- **Longitud de los segmentos:** Se demostró que existía una forma de relacionar las distancias entre los puntos y esta era constante en muchos casos e independiente del orden en que cada punto se selecionó.

- **Ángulos y pendientes:** Muchos de los usuarios de Passpoints tienden a crear lineas rectas con sus puntos (Los ángulos más comunes formados entre dos segmentos de recta están cercanos a 0 grados). La distribución de las pendientes por el eje x muestra que los usuarios favorecen las lineas horizontales seguidas por segmentos verticales hacia abajo (pendientes de 270 grados).

- **Formas:** En la investigación identificaron 5 figuras que se pueden formar en el caso del Passpoints con 5 puntos sin importar la orientación de la forma (En el anexo 1 figura 2 se muestran algunos ejemplos gráficos de estas formas). Además en el anexo 1 figura 3 se pueden apreciar el porciento de contraseñas que contiene cada una de estas formas.

  - **Forma de Linea:** La suma de los valores absolutos de los 3 ángulos es menor a 15 grados. El 26 % de las claves de un estudio realizado en [Vorster et al., 2016] cumplieron con este patrón.
  - **Forma de W:** El ángulo 1 y el 3 tienen el mismo signo (van en la misma dirección), el ángulo 2 en dirección opuesta.
  - **Forma de Z:** Dos de los ángulos tienen signos opuestos y el tercer ángulo tiene menos de 15 grados (forma una linea recta).
  - **Forma de V:** Dos de los ángulos tiene menos de 15 grados y el tercero tiene más de 15 grados.
  - **Forma de C:** Los tres ángulos tienen el mismo signo (van en la misma dirección) y la suma del valor absoluto de los 3 es mayor de 180 grados.
  - **Otros:** Todo lo que no coincida con los patrones anteriores tiene forma desconocida.

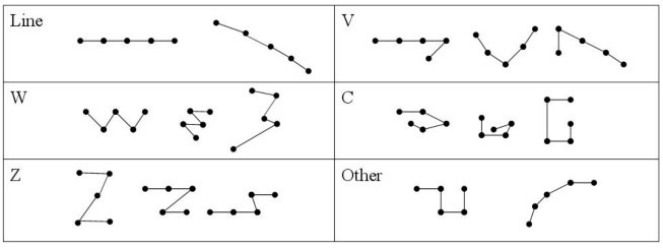

Figura 2. Ejemplos de PLC para cada categoría de acuerdo a la forma.

También en [van Oorschot and Thorpe, 2011, Van Oorschot et al., 2010, Vorster, 2014] se consideran algunos PLC que tienen puntos de encuentro con el estudio previo. Estos se relacionan a continuación:

- **HOR:** Puntos en linea horizontal (de izquierda a derecha o derecha a izquierda).

- **VER:** Puntos en linea vertical (de arriba a abajo o abajo a arriba).
- **DIAG:** Puntos en dirección horizontal y vertical, incluye las lineas rectas.
- **LOD (*Localized Omni-Direction*):** Cada 2 puntos consecutivos de los 5 que conforman la clave, están a distancias constantes.
- **CWCCW:** Puntos en sentido horario (a favor de las manecillas del reloj) o anti-horario (en contra de las manecillas del reloj). se puede definir como secuencias de al menos 3 puntos consecutivos que van en la misma dirección (horario o anti-horario) y la suma de sus ángulos no es mayor de 360 grados.

Cada una de las aproximaciones anteriores tienen en cuenta un error asociado ($t \geq 0$) que relajaría la forma de interpretación del patrón, puesto que es muy difícil que el usuario seleccione por ejemplo 5 puntos en linea perfectamente recta. Como se puede apreciar HOR, VER y DIAG están incluidos en las interpretaciones de 'Forma de linea' que se hicieron en la investigación de Chiasson et al., CWCCW puede verse como una aproximación de las 'Forma de C' y LOD como la interpretación de mantener una cierta distancia relativa entre la longitud de los segmentos imaginarios entre puntos.

5.2 Resultados en la aplicación de PLC en ataques de diccionario

En [Van Oorschot et al., 2010], se recuperaron con la aplicación de DIAG con $t = 9$ y $2^{33,02}$ entradas del diccionario en la imagen de la piscina y los carros respectivamente (Anexo 1 figura 4) el $21,1\,\%$ y el $27,5\,\%$ de las contraseñas. Sin embargo para la aplicación de DIAG con $t = 19$ y $t = 28$ con $2^{35,26}$ entradas del diccionario en la imagen de la piscina y los carros respectivamante el $48{,}2\,\%$ y $54{,}2\,\%$ de las contraseñas.

También con la aplicación de patrones LINE con $t = 9$ y $2^{20,88}$ entradas de diccionario en la imagen de la piscina y los carros respectivamente el $3{,}5\,\%$ y el $22\,\%$ de las contraseñas. Para el mismo patrón pero con $t = 19$ y $t = 28$ con ^{29,02} entradas de diccionario en la imagen de la piscina y los carros respectivamente el $23{,}7\,\%$ y el $52{,}3\,\%$ de las contraseñas.

Los resultados de la aplicación de los diccionarios LINE y DIAG se optimizaron en [Van Oorschot et al., 2010] hasta 7 y 10 veces respectivamente utilizando la variantes de estos algoritmos con $t = 19$ y $t = 18$ cruzados con información con los MVA y TPI.

Para el caso de LOD, los resultados de los diccionarios generados con distancias de $20, 40, 60, 80$ y 100 píxeles para la imagen de la piscina es comparable al de DIAG con $t = 19$ y $t = 28$. LOD con 100 píxeles, en este caso con un diccionario de 2^{35} entradas obtuvo el $47,4\,\%$ de las contraseñas.

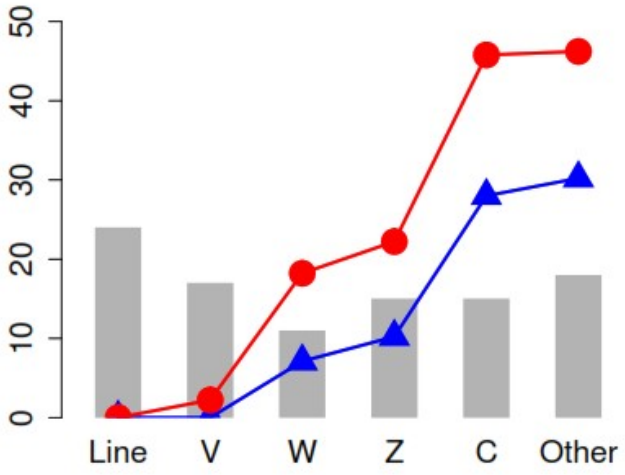

Figura 3. Porciento de las contraseñas de [Chiasson et al., 2009] que contienen cada uno de los cinco patrones de formas

6. Resultados y Discusión

Existen imágenes que en su composición son más propensas a poseer patrones en el orden en que el usuario selecciona sus puntos. Las imágenes que tienen significado, flujo o movimiento pueden ser una influencia mayor para que el usuario siga estas lineas inducidas y escoja su secreto cumpliendo estos patrones.

En la figura 4 se puede apreciar un claro ejemplo donde se utilizan 2 imágenes (un aparcamiento de carros y piscina con personas). Las zonas rojas equivalen a datos (clusters) capturados por TPI en [van Oorschot and Thorpe, 2011] para detectar HotSpots. De forma superpuesta, ejemplos de PLC; se puede apreciar que de igual manera las concentraciones de HotSpots responden a PLC luego de aplicarle las leyes de percepción de Gestalt, los MVA y los PLC propuestos por Chiasson et al. Es evidente que la imagen con carros es más propensa a inducir PLC por la disposición de los objetos que la de la piscina, pero ambas los contienen.

Aunque los PLC se pueden hallar solo analizando las formas y disposiciones de los puntos que conforman la contraseña, la selección de estos responde en gran medida a objetos y caminos conectados sobre la imagen. Por lo que en un gran por ciento de los casos no sería necesario aplicar TPI exhaustivas y costosas computacionalmente para realizar un ataque efectivo de diccionario. En cualquier caso se recomienda desarrollar y emplear técnicas que eduquen al usuario para disuadirlo de emplear en la creación de sus contraseñas estos patrones clásicos.

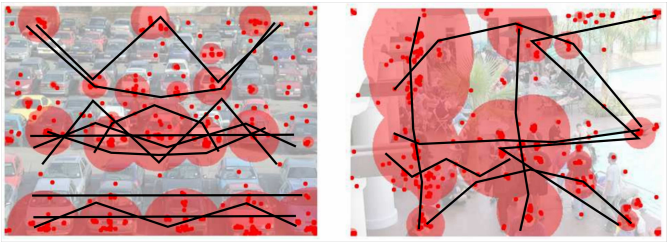

Figura 4. Presencia de PLC en las mayores concentraciones de HotSpots detectadas en [van Oorschot and Thorpe, 2011].

Conclusiones

A partir de los elementos antes planteados se puede concluir que:

- Los usuarios de la TAG Passpoints escogen claves sencillas debido a que luego las tendrán que usar en entornos prácticos.
- El usuario prefiere áreas específicas de la imagen que resalten por poseer "salientes", picos, esquinas u objetos de colores llamativos y este comportamiento es dependiente de la imágen y de su contenido.
- Las estrategias donde se utlizan TPI son dependientes de la imágen que el usuario utilizó en el proceso de registro.
- El usuario escoge en un por ciento significativo de las veces de forma inconsciente la secuencia de puntos de tal forma que estos tienen relación entre sí de manera parcial o total (sobre todo en entornos prácticos), acorde a la forma en que percibe un escenario para garantizar poder recordarlo. Esta apreciación es independiente de la imágen y de su contenido y se basa en las leyes de Gestalt y MVA.
- Los Patrones de clics aparecen en muchas de las imágenes de las investigaciones mencionadas ya sea de forma individual o combinados con otras técnicas. Esto puede ser aprovechado por los atacantes puesto que estas características no dependen de las imágenes utilizadas de fondo.
- Muchos de los usuarios de Passpoints prefieren las lineas rectas donde los puntos estén esparcidos por la imagen comenzando de izquierda a derecha y ya sea completamente horizontal o en pendiente de arriba a abajo.
- Para el Passpoints los ataques que buscan PLC poseen ventajas ya que estos pueden estar inducidos por objetos y caminos concretos de las imágenes de fondo.
- Los patrones DIAG, VER y HOR producen mejores resultados cuando el margen de error para identificar el patrón es mayor $t = 19$ y $t = 28$.
- Evidencias obtenidas de estudios analizados demuestran que los ataques de diccionarios utilizando los PCL de forma individual o con la informacón cruzada de TPI, son ataques efectivos para la TAG Passpoints.
- La calidad de las imágenes en cuanto a su composición es un factor determinante en la efectividad de la TAG Passpoints puesto que no todas son vulnerables en igual medida a los ataques de diccionario.
- Una de las alternativas para aumentar la seguridad del sistema Passpoints puede ser educar al usuario informándole que su clave es débil mostrándole visualmente que contiene alguno de los PLC clásicos.

Referencias

[Bhong and Shahade, 2013] Bhong, V. and Shahade, V. (2013). Authentication using graphical passwords: effects of tolerance and image choice. *International Journal for Engineering Applications and Technology*, 5:239–245.

[Blonder, 1996] Blonder, G. E. (1996). Graphical password. US Patent 5,559,961.

[Chiasson et al., 2009] Chiasson, S., Forget, A., Biddle, R., and van Oorschot, P. C. (2009). User interface design affects security: Patterns in click-based graphical passwords. *International Journal of Information Security*, 8(6):387.

[Comaniciu and Meer, 2002] Comaniciu, D. and Meer, P. (2002). Mean shift: A robust approach toward feature space analysis. *IEEE Transactions on pattern analysis and machine intelligence*, 24(5):603–619.

[Cowan., 2000] Cowan., N. (2000). The magical number 4 in short-term memory: A reconsideration of mental storage capacity. *Behavioral and Brain Sciences, 24:87185,* .

[Gao et al., 2013] Gao, H., Jia, W., Ye, F., and Ma, L. (2013). A survey on the use of graphical passwords in security. *JSW*, 8(7):1678–1698.

[Harris and Stephens, 1988] Harris, C. and Stephens, M. (1988). A combined corner and edge detector. Citeseer.

[Itti and Koch, 2001] Itti, L. and Koch, C. (2001). Computational modelling of visual attention. *Nature reviews neuroscience*, 2(3):194.

[Itti et al., 1998] Itti, L., Koch, C., and Niebur, E. (1998). A model of saliency-based visual attention for rapid scene analysis. *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE*, 20(11):1255.

[King and Wertheimer, 2005] King, D. B. and Wertheimer, M. (2005). *Max Wertheimer and gestalt theory*. Transaction Publishers.

[Klein, 1990] Klein, D. (1990). Foiling the cracker: A survey of, and improvements to, password security. In *In Proceedings of the 2nd USENIX Security Workshop.*, pages 5–14.

[Luck and Vogel, 1997] Luck, S. J. and Vogel, E. K. (1997). The capacity of visual working memory for features and conjunctions. *Nature*, 390(6657):279.

[Ouerhani et al., 2004] Ouerhani, N., Von Wartburg, R., Hugli, H., and Müri, R. (2004). Empirical validation of the saliency-based model of visual attention. *ELCVIA: electronic letters on computer vision and image analysis*, 3(1):13–24.

[Salehi-Abari et al., 2008] Salehi-Abari, A., Thorpe, J., and van Oorschot, P. C. (2008). On purely automated attacks and click-based graphical passwords. In *Computer Security Applications Conference, 2008. ACSAC 2008. Annual*, pages 111–120. IEEE.

[Thorpe and van Oorschot, 2007] Thorpe, J. and van Oorschot, P. C. (2007). Human-seeded attacks and exploiting hot-spots in graphical passwords. In *USENIX Security Symposium*, volume 8, pages 1–8.

[Valdés et al., 2018] Valdés, O. R., Legón, C. M., and Llanes, R. S. (2018). Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica. *Revista Cubana de Ciencias Informáticas*, 12:13–27.

[Van Oorschot et al., 2010] Van Oorschot, P. C., Salehi-Abari, A., and Thorpe, J. (2010). Purely automated attacks on passpoints-style graphical passwords. *IEEE Transactions on Information Forensics and Security*, 5(3):393–405.

[van Oorschot and Thorpe, 2011] van Oorschot, P. C. and Thorpe, J. (2011). Exploiting predictability in click-based graphical passwords. *Journal of Computer Security*, 19(4):669–702.

[Van Orschot and Thorpe, 2005] Van Orschot, P. and Thorpe, J. (2005). *On the Security of Graphical Password Schemes.*

[Vorster and van Heerden, 2015] Vorster, J. and van Heerden, R. (2015). Graphical passwords: A qualitative study of password patterns. In *The Proceedings of the 10th International Conference on Cyber Warfare and Security (ICCWS 2015), L. Armistead, Ed. Academic Conferences Limited*, pages 375–383.

[Vorster, 2014] Vorster, J. S. (2014). *A Framework for the Implementation of Graphical Passwords*. PhD thesis, Master thesis, University of Liverpool, 12 2014.

[Vorster et al., 2016] Vorster, J. S., Van Heerden, R. P., and Irwin, B. (2016). The pattern-richness of graphical passwords. In *Information Security for South Africa (ISSA), 2016*, pages 69–76. IEEE.

[Wiedenbeck et al., 2005] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon., N. (2005). Passpoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, Vol. 63(1-2):102–127.

[Zhu et al., 2013] Zhu, B. B., Wei, D., Yang, M., and Yan, J. (2013). Security implications of password discretization for click-based graphical passwords. In *Proceedings of the 22nd international conference on World Wide Web*, pages 1581–1591. ACM.