Revista Cubana de Ciencias Informáticas
Vol. 12, No. Especial UCIENCIA, Septiembre 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 13-27
http://rcci.uci.cu

Tipo de artículo: Artículo original
Temática: Ciberseguridad
Recibido: 28/05/2018 | Aceptado: 13/09/2018

Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica

Security and usability of graphic authentication schemes and techniques

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

[1]Universidad de las Ciencias Informáticas (UCI). Facultad de Ciencias y Tecnologías Computacionales
[2]Universidad de la Habana (UH). Facultad de Matemática y Computación. Instituto de Criptografía
[3]Universidad Tecnológica de la Habana (CUJAE). Facultad de Informática

*Autor para correspondencia: osviel@uci.cu

Resumen
La autenticación es un área clave en la seguridad de la información. En la modernidad los usuarios necesitan acceder a muchos servicios digitales imprescindibles para su vida cotidiana. Las contraseñas basadas en caracteres alfanuméricos han sido las más comunes en todo tipo de sistemas por su fácil implementación. Estas a partir de la forma en la que los usuarios las escogen, poseen desventajas que introducen vulnerabilidades en los sistemas que protegen. Las Técnicas de Autenticación Gráfica se han convertido en alternativas a la tradicional introducción de caracteres alfanuméricos; existen variadas y han sido preferidas por características de las imágenes que ayudan al recuerdo de la contraseña. En este artículo se resumen las principales técnicas de autenticación gráficas, se definen las tendencias modernas y se hacen recomendaciones a partir de los criterios de seguridad y usabilidad.

Palabras claves: Autenticación, Seguridad, Contraseñas Gráficas, Usabilidad, Técnicas de Autenticación Gráfica

Abstract
The authentication is a key area in the field of Information Security. In modern times users need to use many digital services. The passwords based on alphanumerical caracters have been the most common and easy to implement. These introduce many issues in the systems they protect because the way users select them. The Graphic authentication techniques have become in alternatives to traditional alphanumerical ones; they are in a great variety and have been prefered for some caracteristics of images to improve password remembering. In this paper is presented a survey of main authentication techniques in order to define the modern trends and also give recomendation starting from the approaches of usability and security.

Keywords: *Authentication, Security, Graphical Password, Usability, Graphical Authentication Technique*

Revista Cubana de Ciencias Informáticas
Vol. 12, No. Especial UCIENCIA, Septiembre 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 13-27
http://rcci.uci.cu

Introducción

El desarrollo de las tecnologías de la informática y las comunicaciones ha propiciado nuevos entornos de desarrollo social y profesional. El volumen de datos sensibles que se maneja en los Sistemas de Gestión de Información (SGI) sigue siendo el objetivo de los atacantes que buscan hurtar o dañar a los usuarios y las empresas. Los mecanismos para garantizar que los sistemas y la información que estos controlan solo sean utilizados por las personas autorizadas son variadas y poseen diversas características que determinan su elección para cada entorno específico.

La autenticación es un paso dentro del proceso de Identificación-Autenticación en el que se determina si un usuario o entidad puede tener acceso a un sistema o recurso[1]. Esta es una de las áreas claves en las investigaciones sobre seguridad y diseño de Sistemas de Control de Seguridad de la Información en los últimos años. Un ciudadano promedio utiliza las tecnologías para acceder a todo tipo de servicios en la vida moderna (correo, cuentas bancarias, redes sociales, dispositivos móviles, servicios de comunicaciones, etc.). Estos servicios deben proveer seguridad y confiabilidad, siendo necesario algún tipo de información que identifique de forma única al usuario. Los métodos de autenticación se clasifican en cinco tipos: los basados en un token (Algo que el usuario posee), los basados en información biométrica (Algo que el usuario es y lo identifica unívocamente), los basados en conocimiento (Algo que el usuario conoce), la ubicación (Direcciones IP) y los sistemas híbridos.

En los esquemas de autenticación basados en token de seguridad el usuario porta un objeto que le identifica ante un sistema informático y en el cuál reside una llave de criptografía. Se utilizan combinados con contraseñas o pines para proveer seguridad a los servicios de cobro y pago en los bancos y oficinas comerciales [Suo (2006)]. La forma más común en la que se presentan es como tarjetas inteligentes o magnéticas, pero pueden verse en muchas otras como dispositivos digitales y memorias USB. En este tipo de esquema el usuario debe evitar la pérdida o robo de su Token y este es también proclive al deterioro por tiempo de uso.

Los esquemas de autenticación basados en información biométrica son alternativas a las Contraseñas Alfanuméricas (CA)[Rejman-Greene (2001)]. Para su implementación es necesario en todos los casos la utilización de elementos de hardware especializado. Puede ser en concepción difícil de falsificar pero relativamente fácil de robar [Patrick et˜al. (2003)]. El rendimiento de estos también puede verse comprometido por circunstancias como la salud del usuario, estrés y otros factores que pueden hacer el proceso de identificación extenso e incómodo.

En los esquemas de autenticación basados en conocimiento se ha utilizado tradicionalmente las Contraseñas Alfanuméricas (CA). Las CA son una combinación de caractéres utilizando el código ASCII para generar una

[1]Primero el usuario presenta sus credenciales al sistema (Identificación) y luego a partir de la veracidad de estas se le garantiza acceso a los recursos o no en función de sus permisos (Autenticación).

Revista Cubana de Ciencias Informáticas
Vol. 12, No. Especial UCIENCIA, Septiembre 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 13-27
http://rcci.uci.cu

clave secreta de dimensión variable [Patrick et˜al. (2003)]. Son fáciles de implementar y muy comunes en todos los tipos de sistemas. Surgieron en 1960 como solución a los problemas de seguridad asociados al surgimiento del primer sistema operativo multi-usuario. Una CA fuerte debe ser aleatoria y larga; como consecuencia difícil de recordar [Radhika and Biswas (2014)]. Esto se conoce en la literatura como "el problema de la password"[Walkup (2016)]. Por la naturaleza de los procesos nemotécnicos cuando los usuarios tienen que establecer o recordar muchas contraseñas usualmente utilizan en sistemas distintos, claves parecidas o con frases sencillas de recordar [Daf et˜al. (2017); Gao et˜al. (2013)].

En [Wiedenbeck et˜al. (2005)] se demuestra que una práctica común es la de escribir en papel todas las claves para no olvidarlas o utilizar la misma clave para todos los sistemas. En otros casos los usuarios crean sus propios procedimientos para generar claves distintas, adicionando un número o una letra al final de cada palabra o nombre. Todos estos requerimientos y conductas van en detrimento de la seguridad y la información que estos sistemas manejan. Según [Bhong and Shahade (2013)] los usuarios casi siempre ignoran las recomendaciones para la confección de claves seguras, estas tienden a ser cortas y poco aleatorias. Existen muchas técnicas y herramientas que aprovechan estas vulnerabilidades y de una manera relativamente fácil permiten obtener la contraseña [Sobrado and Birget (2002b); Daf et˜al. (2017)]. Lamentablemente estas pueden ser fácilmente pronosticadas o atacadas.

Los Sistemas de Autenticación Gráficas (SAG) se encuentran dentro de Los Sistemas Basados en Conocimiento. Estos son usados en la autenticación de usuarios en un sistema o la generación de llaves para el uso en algoritmos criptográficos [Sunil et˜al. (2014)]. Las Contraseñas Gráficas (CG) pueden estar formadas por la combinación de fotos, imágenes o iconografías. Dadas las características de las imágenes, estas producen un espacio de claves mucho mayor. Además son resistentes a los ataques clásicos a CA que los usuarios olvidan fácilmente cuando son complejas y para poder recordarlas utilizan frases que son relativamente fáciles de predecir [Gao et˜al. (2013)]. La eficiencia de los SAG se basa en la gran capacidad de los seres humanos de recordar patrones en imágenes en vez de memorizar conjuntos de caracteres de grandes longitudes y complejidad. Aún son muchas las investigaciones que trabajan en mejorar estos sistemas gráficos, en general estos poseen probadas ventajas sobre los tradicionales de introducción de texto y conservan espacios de claves considerables. Todas estas ventajas los hacen deseables y prácticos para muchos entornos donde las CA se olvidan por ser demasiado complejas y largas o son atacadas por los clásicos Ataques de Diccionario, Fuerza Bruta o Spaywares[2].

En este artículo se presentan y discuten los principales esquemas y técnicas existentes de Autenticación Gráfica (AG). Se definen dentro de este tipo de esquemas las tendencias y principales vulnerabilidades mediante una comparación basada en sus características. A partir de esta comparación se hacen recomendaciones de cuál emplear a criterio de los autores.

[2]Aplicaciones que capturan todo lo que introduce el usuario por teclado sin que este sea consciente de ello.

Revista Cubana de Ciencias Informáticas
Vol. 12, No. Especial UCIENCIA, Septiembre 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 13-27
http://rcci.uci.cu

Materiales y métodos

1 Contraseñas gráficas

Las CG aprovechan el hecho de que los sentidos humanos están preparados para procesar y almacenar gran cantidad de información gráfica. Fueron ideadas originalmente por Blonder Blonder (1996) encontrándose registrada la patente a su nombre desde 1996. Cuando para una persona puede ser difícil recordar 50 caracteres alfanuméricos, en contraste fácil recordar rostros humanos, lugares que ha visitado y cosas que ha visto. La información gráfica contenida en las imágenes representa millones de bits y puede proveer espacios de claves considerables para ser usados como técnica fiable de autenticación [Sobrado and Birget (2002b)]. En los estudios psicológicos de [Kirkpatrick (1894); Shepard (1967)] demuestran que esta habilidad para reconocer patrones visuales hace que esta en particular tenga ventajas sobre las CA [Sunil et˜al. (2014)] y sea a su vez resistente a los ataques clásicos a los que estas son vulnerables.

Las CG engloban también un grupo de técnicas. Para aclarar la diferencia entre estas, las literaturas hasta 2017 muestran que pueden ser divididas en cuatro categorías: Técnicas basadas en el reconocimiento (*Recognition based techniq*), Técnicas basadas en el recuerdo de patrones en imágenes (*Recall based technique*), Técnicas basadas en el recuerdo de puntos claves en imágenes (*Cued-recall based technique*) y las Técnicas híbridas (*Hibrid techniques*) [Lashkari et˜al. (2010); Nikhil and Arati (2015); Gao et˜al. (2013); Bulganmaa and Junxing (2017)].

1.1 Técnicas basadas en el reconocimiento

Este tipo de técnica se basa en el principio del reconocimiento de patrones de imágenes siendo una de las más sencillas para la memoria humana. Se le presenta al usuario un grupo de imágenes en orden aleatorio y de composición también aleatoria. El usuario debe seleccionar las que considere para formar su clave; luego para autenticarse debe recordar y repetir su selección dentro de un grupo mayor de imágenes aleatorias. Algunos de los más relevantes son:

El método de Dhamija y Perring [Dhamija and Perrig (2000)] con las propuestas de mejora de Akula and Devisetty's [Akula and Devisetty (2004)] para optimizar el almacenamiento utilizando SHA-1 y Takada [Takada and Koike (2003)] para permitir al usuario seleccionar las imágenes de su preferencia.

El método de [Jansen (2004)] se diferencia del anterior en dos aspectos. Primero el usuario para autenticarse debe seleccionar las imágenes en un orden correcto y estas se limitan a 30. Segundo, se asigna a cada imagen un identificador y la secuencia ordenada constituye una contraseña numérica. Otros métodos semejantes son Story [Davis et˜al. (2004)] y Deja Vú [Dhamija and Perrig (2000)].

Revista Cubana de Ciencias Informáticas
Vol. 12, No. Especial UCIENCIA, Septiembre 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 13-27
http://rcci.uci.cu

Sobrado and Birget (2002a) propone dos método resistentes a los ataques de tipo Shoulder Surfing[3], ambos utilizan mil objetos de forma icónica. En el primero el usuario selecciona como clave tres de ellos. Para autenticarse debe seleccionar los objetos contenidos en el triángulo que forman estos tres. En el segundo (Movable Frame Scheme) [Sobrado and Birget (2002a)] se debían reconocer tres objetos donde uno de ellos se encontraba en un marco que se debía alinear a los demás formando una linea recta. El uso de mil objetos provoca que el despliegue sea atestado y la identificación difícil; pero usar un grupo de objetos pequeño reduce el espacio de claves.

[Man and Mathews (2003)] propone un algoritmo también resistente a los ataques de tipo Shoulder-Surfing basado en la selección de objetos en forma icónica. Cada objeto posee posee un código único. El usuario debe introducir la secuencia de códigos correspondiente a los objetos y a sus posiciones, que conforman su clave. Al no utilizarse el ratón, incluso si es grabado en video el procedimiento es difícil de imitar. Su desventaja radica en que el usuario debe recordar los códigos relativos a cada objeto. Hong más adelante mejora la memorabilidad permitiendo a los usuarios escoger los códigos para cada objeto.

La Real User Corporation Autores (a) propuso un método basado en la identificación de rostros humanos. El usuario selecciona de una base de datos cinco rostros que conforman su clave secreta. Para autenticarse debe reconocer (cinco veces) uno de ellos entre nueve aleatorios. El proceso es mas largo que el de introducción de texto y los usuarios tienden a seleccionar rostros de razas similares.

1.2 Técnicas basadas en la memorización de patrones

También conocidos como Pure Recall Based Techniques. En este tipo de sistemas los usuarios escriben su contraseña en un lienzo o sobre una imágen. El usuario reproduce en forma de dibujo lo que ha establecido en el proceso de registro.

El método Draw a Secret (DAS) Jermyn et˜al. (1999) fué el primero dentro de esta categoría. El sistema interpretaba el dibujo a partir de sus coordenadas según el trazo. El espacio de claves era mayor que el de contraseñas alfanuméricas. Si las dimensiones de la cuadrícula son pequeñas, se reduce el espacio de claves y de lo contrario haría difícil el proceso de dibujar correctamente la clave. Esta restricción determina que el sistema sea útil solamente en el ambiente de dispositivos pequeños como celulares y PDA's. En Van˜Orschot and Thorpe (2005) se demuestran que las contraseñas seleccionadas por los usuarios para este sistema reducen drásticamente el espacio de claves. En Dunphy and Yan (2007) se propone la utilización de un fondo para motivar al usuario a crear patrones mas complejos.

[3]El atacante mira sobre el hombro del usuario mientras este introduce su clave.

Revista Cubana de Ciencias Informáticas
Vol. 12, No. Especial UCIENCIA, Septiembre 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 13-27
http://rcci.uci.cu

Pass-Doodle Varenhorst (2004) es parecido al DAS. Los usuarios dibujan sin la existencia de una cuadrícula. Se pueden usar varios punteros, diferentes grosores, velocidades y colores en el trazo.

El método Pass-Shape Weiss and Luca (2008) es similar al Pass-Doodle. Las contraseñas son traducidas a caracteres alfanuméricos mediante 8 direcciones distintas del trazo a intervalos de 45^o. Es sencillo de recordar pero su espacio de claves es reducido pués en cada cambio de ángulo solo existen 8 posibles direcciones.

Pass-Go Tao (2006) trata de erradicar las deficiencias de DAS. Se basa en un juego chino llamado "Go". El usuario selecciona las intersecciones en una cuadrícula como su clave secreta. El espacio de claves de 256 bits (374 bits si se tienen en cuenta la distinción por colores). Se demostró por Nali and Thorpe (2004); Orschot et˜al. (2008) que el 40 % de las claves caen en un subespacio definido por su simetría con respecto a los ejes central, vertical y horizontal. Además que el 72 % de las claves tienen 4 o menos intersecciones. Este sistema es la base de los modelos de autenticación de patrones en sistemas operativos para celulares. Otros como BPass-Go(Background Pass-Go) parecido a BDAS y MGBPG(Multi Grid Pass-Go) parecido a MGDAS(Multi Grid DAS) buscan ampliar el espacio de claves y ayudar al usuario a recordar patrones de claves mas complejos.

En el método GrIDsure Brostoff (2009) se muestran números en una cuadrícula de 5 x 5. Los usuarios deben seleccionar y memorizar el patrón realizado por un sub-conjunto de los 25 números mostrados. Para registrase se introducen por teclado los números que conforman el patrón. Para autenticarse el usuario debe recordar el patrón e introducir la nueva secuencia de números que lo conforman.

1.3 Técnicas basadas en la memorización de puntos claves

En esta categoría se requiere que el usuario memorice un conjunto de puntos en áreas predeterminadas de una imagen o conjuntos de ellas. En la idea original de Blonder, el usuario debía clickear con un mouse o un lapicero en determinados puntos de una imagen, si lo hacía de forma correcta este sería aceptado por el sistema de lo contrario sería rechazado.

Passlogix Autores (b), ha desarrollado varios SAG que se encuentran dentro de esta categoría y que básicamente buscan repetir una secuencia de acciones. Uno de sus ejemplos más significativos es el vGo en el que los usuarios pueden mezclar un cóctel virtual y usar la combinación de ingredientes como una contraseña. Otras opciones de claves secretas incluyen seleccionar una mano de cartas, o preparar una cena en una cocina virtual. Estas propuestas poseen un espacio de claves pequeño y no existe forma de prevenir que el usuario escoja claves fáciles de adivinar.

PassPoints Wiedenbeck et˜al. (2005) extiende el funcionamiento del trabajo inicial de Blonder. En este método cualquier imagen puede ser utilizada (pinturas, fotos naturales, fotos familiares, fotos de arquitectura, etc.)

Revista Cubana de Ciencias Informáticas
Vol. 12, No. Especial UCIENCIA, Septiembre 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 13-27
http://rcci.uci.cu

lo que hace al sistema más flexible. Las imágenes podían ser seleccionadas por el usuario o proveídas por el sistema. Las imágenes más deseadas para el proceso debían tener contenido que tuviera significado para el usuario por lo que estas debían contener escenas concretas. También era un requisito adicional que las imágenes seleccionadas fueran intrincadas en el contenido y que tuvieran cientos de puntos memorables diseminados de forma homogénea. El usuario podía seleccionar en estas imágenes cualquier conjunto de puntos para crear su secreto. Luego en el proceso de autenticación este debe seleccionarlos en el orden preciso, con un margen de error (tolerancia) alrededor de cada punto. Como una imagen puede contener cientos de miles de puntos, el espacio teórico de este sistema es suficientemente grande. No se necesitarían muchos puntos para hacer la clave segura, con 5 o 6 se pueden lograr mas claves que con 8 caracteres dentro de un alfabeto estándar de 64 letras. Para que el proceso de autenticación fuera efectivo y rápido para el usuario debía existir una tolerancia asociada a cada punto (aproximadamente $0,25cm$). Además de que por razones de seguridad requiere que el sistema no almacene la clave de forma explícita.

Principales elementos negativos de esta técnica:

- Algunas regiones de la imagen son mas probables de ser seleccionadas para conformar la clave Renaud and Angeli. (2004).
- Para que la clave sea efectiva debe contener varios puntos, esto puede extender el proceso de autenticación y de registro mucho más que en un sistema de introducción de caracteres alfanuméricos por lo que lo hace más vulnerable a los ataques de tipo Shoulder-Surfing.
- No guardar la clave de forma explicita provoca un problema a la hora de aplicar el resumen la clave. Puesto que es muy difícil para el usuario volver a seleccionar exactamente los mismos puntos en la imagen, el resumen de la clave sería siempre diferente. Esto conlleva a la utilización de un mecanismo de discretización para establecer la tolerancia alrededor de cada punto lo que reduce el espacio de clave y aporta información relevante para ataque de diccionario Zhu et˜al. (2013). Una discusión acerca de la importancia del proceso de discretización en los esquemas de password grafica puede verse en Birget et˜al. (2003); Chiasson et˜al. (2008); Bicakci (2008); Patra et˜al. (2016).

Cued Click Points (CCP) Patra et˜al. (2016) se propone por los autores como una alternativa más eficiente que el PassPoints. Sugiere la utilización de una secuencia de imágenes (total de 5) y de un solo punto en cada una de ellas. La secuencia de imágenes variaría dependiendo de los puntos que el usuario seleccione. Cuando el usuario se registra, selecciona un punto en cada una de un grupo de 5 imágenes que se le muestran de forma consecutiva. Para el proceso de autenticación este debe seleccionar correctamente los puntos que estableció en el proceso de registro. Si selecciona en cada imagen el punto correcto se le notificará de manera instantánea

que va por el camino adecuado mostrándole la imágenes siguiente en la secuencia que él escogió en el proceso de registro (algo que solo él conoce). De lo contrario se le guiará por un grupo de imágenes distinto hasta que al finalizar el proceso de autenticación sería fallido. Al aumentar el número de imágenes y solo un punto en cada una de ellas aumenta considerablemente el espacio de claves. El sistema debe funcionar en una arquitectura cliente-servidor. Las imágenes se almacenan del lado del servidor y la comunicación debe ser cifrada mediante SSL o TLS. Se utilizaría un mecanismo de discretización para permitirán los fallos y aciertos. Según los estudios de usabilidad de la investigación original la mayoría de los usuarios prefieren el CCP antes que el PassPoints alegando que cada imagen ayudaba a recordar los puntos seleccionados.

Principales elementos negativos de este esquema:

- Si se obtiene el usuario y la secuencia de imágenes que este ha utilizado para conformar su clave, el atacante tiene toda la información que necesita para ejecutar un ataque.
- Para que el sistema sea eficiente se recomienda un grupo inicial de 1200 imágenes, aún con este límite pueden repetirse imágenes en el proceso de autenticación, aumentar la base de datos de imágenes podría afectar el almacenamiento.
- El sistema básicamente es también vulnerable a los ataques de tipo Shoulder-Surfing, incluso más que el PassPoints.
- Se debe utilizar un mecanismo de discretización lo que reduce el espacio de clave y aporta información relevante para ataque de diccionario Zhu et˜al. (2013).

Persuasive Cued Click-Points (PCCP) Chiasson and Oorschot (2008) Se propone como mejora al CCP y busca persuadir al usuario en la selección de puntos más aleatorios. En principio es muy parecido al CCP, solo que en el proceso de creación de la contraseña en la imagen se muestra un cuadro que resalta un área aleatoria limitando el espacio donde el usuario puede seleccionar el punto. Existirá un botón que variará a selección del usuario la localización del cuadro. Para el proceso de autenticación se mantiene la idea original, son el recuadro.

1.4 Esquemas híbridos

A partir de las vulnerabilidades detectadas en cada uno de los sistemas se hace evidente la aparición de técnicas que puedan tomar lo mejor de algunos de ellos y combinarlas para darles mayor seguridad. Dentro de esta categoría se pueden agrupar propuestas como la de Jiminy Renaud and Smith (2001), CAPTCHA (Completely

Revista Cubana de Ciencias Informáticas
Vol. 12, No. Especial UCIENCIA, Septiembre 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 13-27
http://rcci.uci.cu

Automated Public Turing tests to tell Computer and Humans Apart) Gao et˜al. (2009) Wang et˜al. (2010), Inkblot Stubblefield and Simon (2004) , Zhao and Li Zhao and Li (2007), Click-a-secret Éluard et˜al. (2011), Gao et al. Gao et˜al. (2010), PassHands Gao et˜al. (2011) y GBFG Liu et˜al. (2011).

Resultados y discusión

1.5 Valoración de la seguridad de las Contraseñas Gráficas

Son muchos los aspectos que se deben tener en consideración a la hora de diseñar un sistema de autenticación, estos van desde la codificación y almacenamiento de las contraseñas hasta la capacidad para resistir ataques. González˜Nahón et˜al. (2014).

Almacenamiento de la contraseña: en el diseño de un sistema de autenticación es importante la forma en la que se vaya a almacenar la información de los usuarios registrados en el sistema y sus contraseñas. Estos datos, sobretodo la contraseña, no se deben almacenar en texto claro. La forma más segura es almacenando los datos luego de aplicarle una función hash (Función Resumen), nunca en texto claro. En un sistema online, cuando se envía la solicitud de ingresar en el sistema se debe enviar la información además por un canal cifrado. En un sistema local no existe ese problema al no existir una comunicación mediante una red de datos; aun así la base de datos donde se almacena la información sensible debe estar cifrada. Los únicos métodos que aplican seguridad mediante funciones HASH son Dhamija y Pering con sus recomendaciones, PassFaces, PassPoints, CCP y PCCP.

Espacio de claves: El espacio teórico de claves de una contraseña es el número total de contraseñas posibles que se pueden generar. Este espacio teórico asume una distribución equiprobable de las contraseñas. El tamaño de este conjunto depende del número total de caracteres posibles y de la longitud de la contraseña. En las Contraseñas Gráficas, los caracteres posibles son los puntos donde se puede pulsar en la imagen. Cuanto más grande es el espacio de claves, más seguro es el sistema ya que será más resistente a cierto tipo de ataques como el de fuerza bruta. En los sistemas de autenticación con contraseña numérica, tiene un espacio de claves muy pequeño en comparación con otros sistemas con CA o CG. En sistemas de autenticación con CA el espacio de claves varía mucho ya que depende de los caracteres permitidos. En los sistemas de CG el espacio de claves depende íntegramente de las zonas donde se pueda pulsar. Dependiendo de la técnica de autenticación gráfica y de su implementación este posee una dimensión variable. En Zhu et˜al. (2013) demuestran que en las CG las técnicas que utilizan discretización, se reduce significativamente su espacio de clave, aplicando Ataques de Diccionario al PassPoints y al PCCP logran obtener para la Discretización Centrada, el 62 % de las claves, y el 39 % para la Discretización Robusta. Todos los métodos dentro de la categoría Cued-Recall based Technique destacan por su espacio de clave considerablemente grande.

Revista Cubana de Ciencias Informáticas
Vol. 12, No. Especial UCIENCIA, Septiembre 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 13-27
http://rcci.uci.cu

Resistencia a ataques: Para que una contraseña alfanumérica se considere segura debe ser larga, aleatoria y no debe guardar relación con el usuario [4]. Si una contraseña es larga, la hace más resistente a ataques como los de fuerza bruta o Shoulder Surfing. Si una contraseña alfanumérica es aleatoria la hace más resistente a ataques como los de diccionario o la ingeniería social. Todos los métodos consultados poseen debilidades que los pueden hacer vulnerables a los diferentes ataques. Dentro de estos destacan en la primera categoría las propuestas de Birget y Man (Resistentes a Shoulder Surfing) y el método PassPoints con sus variantes puesto que aplicándole restricciones resiste los Ataques de Diccionario Basados en Patrones y detección de HotSpots.

1.6 Valoración de la usabilidad de las Contraseñas Gráficas

Aunque el sistema posea muchas características que lo hacen seguro, si no es cómodo o relativamente fácil de usar por el usuario nunca se utilizará en escenarios reales. González˜Nahón et˜al. (2014) define la usabilidad como la unión de 3 factores:

- Efectividad: Precisión y grado de éxito en las tareas que realiza un usuario.
- Eficiencia: Relación entre el grado de éxito en las tareas que realiza un usuario y los recursos utilizados para conseguirlo.
- Satisfacción: Evaluación positiva del usuario hacia el sistema.

Todos los sistemas de la primera categoría poseen problemas de efectividad y eficiencia. La cantidad de imágenes suele ser grande para garantizar un espacio de claves adecuado y esta restricción afecta en primer lugar la rapidez y el éxito con que el usuario puede culminar el proceso de registro-autenticación. En segundo lugar muchas imágenes pueden afectar la eficiencia aumentando el espacio de almacenamiento en el servidor. En general para cada técnica es evidente que un proceso de autenticación extenso por la utilización de muchas imágenes conduciría a incomodidades para el usuario en el proceso de autenticación.

En la segunda categoría, las técnicas propuestas como base (DAS, PassGo y GrIDsure) cumplen con los parámetros de efectividad y eficiencia dado que sus restricciones iniciales los conciben solo para escenarios específicos [5]. Destacan las propuestas BDASH, Pass-Doodle, PassShape y Background Pass-Go por contribuir a mejorar las deficiencias de sus métodos originales para escenarios diversos pero los hace predecibles y vulnerables a ataques. Entre ellos resalta el Pass-Go para el cuál existen en la actualidad muchas implementaciones de variantes de este sistema para dispositivos móviles.

[4] No deben ser nombres de familiares, mascotas, cumpleaños, números de identidad personal, aniversarios ni fragmentos u combinaciones de estos.

[5] Escenarios donde el tamaño de la cuadrícula sea pequeño.

En la tercera categoría todos los métodos cumplen con el parámetro de efectividad y satisfacción. En los estudios se abunda sobre la rapidez con la que los usuarios comprenden el procedimiento y son capaces de reproducir sus claves de forma efectiva y exitosa a partir de la región de tolerancia. Solo es señalable la influencia de la discretización en la eficiencia de las implementaciones.

Conclusiones

A partir de la discusión realizada de los SAG se concluye:

- Las técnicas de Birget, el PassGo, PassPoints, CCP y el PCCP, son fuertes ante ataques de fuerza bruta, de diccionario, Spayware e ingeniería social. Estos tres últimos solo son vulnerables a los de tipo Shoulder Surfing.
- Las mejoras a SAG deben tener en cuenta: el almacenamiento de la clave, el espacio de claves, la resistencia a ataques y la usabilidad como medidas de eficiencia. Siempre tener en perspectiva que la mejoría en uno puede atentar contra el detrimento de otro.
- La técnica PassPoints, CCP y PCCP que se encuentran dentro de la categoría Cued-Recall Based Techniques destacan por cumplir con todos los parámetros que definen la seguridad y la mayoría que definen la usabilidad en los sistemas de autenticación.
- El procedimiento de discretización aplicado para almacenar la contraseña en los SAG aporta información relevante para ataques de diccionario.
- Se recomienda el empleo de PassPoints por su flexibilidad, comodidad para el usuario y resistencia a la grán mayoría de los ataques.
- El Passpoint posee importantes características que ayudan al usuario en el recuerdo de la contraseña. Es simple en su concepto y soporta combinación de estrategias para mejorar sus vulnerabilidades. **?**

Referencias

Akula, S. and Devisetty, V. (2004). *Image based registration and authentication system*, volume Vol. 4.

Autores, V. Passfaces: Two factor authentication for the enterprise. www.realuser.com.

Autores, V. Passlogix graphical password schemes. http://www.passlogix.com.

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.

Bicakci, K. (2008). Optimal discretization for high-entropy graphical passwords. In *Computer and Information Sciences, 2008. ISCIS'08. 23rd International Symposium on*, pages 1–6. IEEE.

Birget, J.-C., Hong, D., and Memon, N. D. (2003). Robust discretization, with an application to graphical passwords. *IACR Cryptology ePrint Archive*, 2003:168.

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

Brostoff, S., I. P. S. A. M. (2009). Evaluating the usability and security of a graphical one-time pin system. In *24th BCS Conference on Human Computer Interaction.*

Bulganmaa, T. and Junxing, Z. (2017). New graphic password scheme comntaining questions-backgroung/pattern and implementation. *International Congress of nformation and Comunication Technology(ICICT 2017)*, page 148/156.

Chiasson, S., F. A. B. R. and Oorschot, V. (2008). Influencing users towards better passwords: Persuasive cued click-points. In *In Proceedings of the BCS Conference on Human Computer Interaction (HCI).*

Chiasson, S., Srinivasan, J., Biddle, R., and van Oorschot, P. C. (2008). Centered discretization with application to graphical passwords. In *UPSEC*. Citeseer.

Daf, S. S., Mhaiskey, T. M., Hadke, A. A., Khadke, S. K., and Jogekar, R. N. (2017). A review on image based graphical user authentication. *International Journal of Engineering Science and Computing*, Vol. 7.

Davis, D., Monrose, F., and Reiter, M. K. (2004). On user choice in graphical password schemes. In *USENIX Security Symposium*, volume 13, pages 11–11.

Dhamija, R. and Perrig, A. (2000). Deja vu : A user study using images for authentication. *Proceedings of 9th USENIX Security Symposium.*

Dunphy, P. and Yan, J. (2007). Do background images improve draw a secret graphical passwords? In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 36–47. ACM.

Éluard, M., Maetz, Y., and Alessio, D. (2011). Action-based graphical password:"click-a-secret". In *Consumer Electronics (ICCE), 2011 IEEE International Conference on*, pages 265–266. IEEE.

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.

Gao, H., Liu, X., Wang, S., and Dai, R. (2009). A new graphical password scheme against spyware by using captcha. In *SOUPS*.

Gao, H., Ma, L., Qiu, J., and Liu, X. (2011). Exploration of a hand-based graphical password scheme. In *Proceedings of the 4th international conference on Security of information and networks*, pages 143–150. ACM.

Gao, H., Ren, Z., Chang, X., Liu, X., and Aickelin, U. (2010). A new graphical password scheme resistant to shoulder-surfing. In *Cyberworlds (CW), 2010 International Conference on*, pages 194–199. IEEE.

González Nahón, M. et al. (2014). Estudio de mecanismos de autenticación basados en contraseñas visuales en dispositivos móviles android. B.S. thesis.

Jansen, W. (2004). Authenticating mobile device users through image selection. *WIT Transactions on Information and Communication Technologies*, Vol. 30.

Jermyn, I., Mayer, A. J., Monrose, F., Reiter, M. K., Rubin, A. D., et al. (1999). The design and analysis of graphical passwords. In *Usenix Security*, pages 1–14.

Kirkpatrick, E. A. (1894). An experimental study of memory. *Psychological Review*, 1(6):602.

Lashkari, A. H., Gani, A., Sabet, L. G., and Farm, S. (2010). A new algorithm on graphical user authentication (gua) based on multi-line grids. *Scientific Research and Essays*, 5(24):3865–3875.

Liu, X., Qiu, J., Ma, L., Gao, H., and Ren, Z. (2011). A novel cued-recall graphical password scheme. In *Image and Graphics (ICIG), 2011 Sixth International Conference on*, pages 949–956. IEEE.

Man, S., H. D. and Mathews, M. (2003). A shoulder surfing resistant graphical password scheme. In *in Proceedings of International conference on security and management.*

Nali, D. and Thorpe, J. (2004). *On predictive models and user-drawn graphical passwords.*

Nikhil, T. A. and Arati, D. (2015). Graphical passwords authentication: A survey. *International Journal of Computer Science and Mobile Computing*, Vol. 4.

Orschot, V., P.C, and Thorpe, J. (2008). *On predictive models and user-drawn graphical passwords*, volume Vol. 10(4).

Patra, K., Nemade, B., Mishra, D. P., and Satapathy, P. P. (2016). Cued-click point graphical password using circular tolerance to increase password space and persuasive features. *Procedia Computer Science*, 79:561–568.

Patrick, A. S., Long, A. C., and Flinn, S. (2003). Hci and security systems. In *CHI'03 Extended Abstracts on Human Factors in Computing Systems*, pages 1056–1057. ACM.

Radhika and Biswas, S. S. (2014). Comparative study of graphical user authentication approaches. *International Journal of Computer Science and Mobile Computing*, Vol. 3.

Rejman-Greene, M. (2001). Biometrics—real identities for a virtual world. *BT Technology Journal*, 19(3):115–121.

Renaud, K. and Angeli., A. D. (2004). My password is here! an investigation into visio- spatial authentication mechanisms. In *Interacting with Computers 16*, pages 1017–1041.

Renaud, K. and Smith, E. (2001). Jiminy: helping users to remember their passwords. In *Annual conference of the south african institute of computer scientists and information technologists. saicsit*, pages 73–80.

Shepard, R. N. (1967). Recognition memory for words, sentences, and pictures. *Journal of verbal Learning and verbal Behavior*, 6(1):156–163.

Sobrado, L. and Birget, J. (2002a). Graphical passwords. *The Rutgers Scholar, RutgersUniversity, Camden New Jersey*, Vol. 4.

Sobrado, L. and Birget, J.-C. (2002b). Graphical passwords. *The Rutgers Scholar, an electronic Bulletin for undergraduate research*, 4:12–18.

Stubblefield, A. and Simon, D. (2004). Inkblot authentication. *Microsoft Research*.

Sunil, S. S., Prakash, D., and Shivaji, Y. R. (2014). Cued click points: Graphical password authentication technique for security. *(IJCSIT) International Journal of ComputerScience and Information Technologies*, Vol. 5(2).

Suo, X. (2006). A design and analysis of graphical password.

Takada, T. and Koike, H. (2003). Awase-e: Image-based authentication for mobile phones using users favorite images. *Human-computer interaction with mobile devices and services*, pages 347–351.

Tao, H. (2006). *Pass-Go, a new graphical password scheme*. PhD thesis, University of Ottawa (Canada).

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

Varenhorst, C. (2004). Passdoodles: A lightweight authentication method. *MIT Research Science Institute*.

Walkup, E. (2016). The password problem. Technical report, Sandia National Laboratories (SNL-NM), Albuquerque, NM (United States).

Wang, L., Chang, X., Ren, Z., Gao, H., Liu, X., and Aickelin, U. (2010). Against spyware using captcha in graphical password scheme. In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, pages 760–767. IEEE.

Weiss, R. and Luca, A. D. (2008). Passshapes - utilizing stroke based authentication to increase password memorability. *In NordiCHI*, pages 383–392.

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.

Zhao, H. and Li, X. (2007). S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. In *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*, volume 2, pages 467–472. IEEE.

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.