e-Ciencias de la Información
Revista electrónica publicada por la
Escuela de Bibliotecología y Ciencias de la Información,
Universidad de Costa Rica, 2060 San José, Costa Rica

e-Ciencias de la Información
Revista electrónica semestral, ISSN-1659-4142
Volumen 4, número 2, ensayo 1
Junio - Diciembre, 2014
Publicado 1 de julio, 2014
http://revistaebci.ucr.ac.cr/

CAPTCHA: ¿UNA SOLUCIÓN PARA LA SEGURIDAD INFORMÁTICA O PROBLEMA PARA LA ACCESIBILIDAD/USABILIDAD WEB?

Omar Antonio Vega
Ronald Eduardo Vinasco-Salazar

CAPTCHA: ¿solución para la seguridad informática o problema para la accesibilidad/usabilidad web?

CAPTCHA: a solution for computer security or a problem to access/ use the web?

Omar Antonio Vega[1] y Ronald Eduard Vinasco-Salazar[2]

RESUMEN

Los CAPTCHA, las pruebas humanas interactivas más utilizadas, aparecen como un método de diferenciación entre usuarios humanos y máquinas para brindar seguridad a la información en internet y evitar el *spam*, especialmente. Por ello, se hace una presentación introductoria de las pruebas humanas interactivas, para luego profundizar en los CAPTCHA, donde se trata su evolución, su clasificación, especificando sus técnicas de generación, algunas de sus aplicaciones y los tipos de ataques a los que se ven sometidos. Después, se tratan algunas repercusiones que han tenido sobre la usabilidad/accesibilidad de servicios de internet para usuarios humanos, lo que lleva a plantearse la inquietud de si los CAPTCHA, más que una solución, se han convertido en un nuevo problema por resolver.

Palabras clave: CAPTCHA, seguridad de información, pruebas humanas interactivas, usabilidad/accesibilidad.

ABSTRACT

CAPTCHAs, which constitute the most widely used human interactive proofs (HIP), appear as a method of differentiation between human computer users and machines to provide security for information on the Internet and avoid spam, especially. Therefore, this paper makes an introductory presentation of HIPs, and then delves into CAPTCHAs, their evolution and classification, specifying their generation techniques, some of its applications and types of attacks to which they are subjected. It then discusses some implications that CAPTCHAs have had on usability/accessibility to the Internet services for human users, which leads to the question of whether they become a new problem, rather than a solution.

Keywords: CAPTCHA, security for information, interactive human proof, usability/accessibility.

Fecha de recibido: 26 de marzo del 2014 **Fecha de aprobado:** 12 de mayo del 2014

Fecha de corregido: 21 de mayo del 2014

[1]Universidad de Manizales, Facultad de Ciencias e Ingeniería. COLOMBIA. oavega@umanizales.edu.co
[2]Universidad de Manizales, Oficina de Tecnologías de la Información. COLOMBIA. rvinasco@umanizales.edu.co

1. INTRODUCCIÓN

La creciente oferta de servicios en internet y la acogida de ellos por parte de un número cada vez mayor de usuarios, ha llevado a establecer diversas técnicas para proteger la información de los ataques, especialmente aquellos de programas automatizados (conocidos como *bots*) que fungen como usuarios humanos.

Ante esta situación, aparecen las pruebas humanas interactivas, entre las cuales destacan los CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*, por sus siglas en inglés). Estos parten de la inteligencia artificial, y proponen retos -basados en texto o imágenes, y últimamente sonidos- aptos para ser rápidamente resueltos por seres humanos, pero difíciles para las computadoras. Sin embargo, esta solución ha implicado limitaciones para la accesibilidad/usabilidad de la web por parte de diversos usuarios, ante la complejidad de algunos CAPTCHA.

Es por ello que se pretende realizar un acercamiento a esta estrategia de seguridad de la información, y algunas de sus repercusiones sobre la accesibilidad/usabilidad de sitios web, no desde una posición terminante, sino como una incitación al debate académico sobre la efectividad integral de los CAPTCHA.

El documento se plantea en tres partes: inicialmente, explica de manera breve las pruebas humanas interactivas (HIP); luego aborda los CAPTCHA desde su evolución, clasificación, aplicaciones y ataques a los que están expuestos; finalmente, se hace una corta presentación de algunas repercusiones de estos sistemas sobre la usabilidad/accesibilidad para los usuarios en general (no solo aquellos con incapacidades, por ejemplo), debido al aumento de dificultad en su lectura para enfrentar los avances de los *bots*.

2. PRUEBAS HUMANAS INTERACTIVAS

En el marco de la utilización masiva de las tecnologías de la información y las comunicaciones (TIC), y debido a la cantidad de información personal e institucional en internet que requiere ser protegida, se han establecido técnicas para probar que se es humano al momento de ingresar o utilizar cierta información. Para ello, la biometría, en conjunto con otras disciplinas, tiene un interesante reto.

Tales técnicas se han denominado pruebas humanas interactivas, mejor conocidas como HIP, por sus siglas en inglés (*Human Interactive Proofs*), y permiten a una persona autenticarse como miembro de un grupo dado (por ejemplo, un humano en oposición a una máquina, una máquina determinada en oposición a otras, un adulto en oposición a un niño, etc.), mediante un desafío que el computador ofrece, el cual debe ser fácil de superar para el miembro, pero difícil para quien no lo sea (Areitio & Areitio, 2008, p. 62).

En otras palabras, el usuario humano demuestra su pertenencia a un grupo particular a través de un desafío/respuesta de protocolo, según lo expresan Shirali-Shahreza y Shirali-Shahreza (2008), quienes, además, señalan que la mayor parte de los HIP son de tipo gráfico (palabras, imágenes e inclusive videos). Esto les permite ser utilizados por personas con discapacidades, por ejemplo los sordos, a los que, cuando desean entrar en un sitio web específico para ellos, se les muestra una palabra a través de una película y ellos (que utilizan el lenguaje de signos) seleccionan la palabra que aparece en la lista.

3. CAPTCHA

Para Shirali-Shahreza y Shirali-Shahreza (2008), los métodos más utilizados para diferenciar automáticamente máquinas y humanos son los CAPTCHA (por sus siglas en inglés, *Completely Automated Public Turing test to tell Computers and Humans Apart*), los cuales están basados en inteligencia artificial. Son similares a la prueba de Turing, con la diferencia de que el juez es un equipo cuyo objetivo es hacer preguntas que los usuarios humanos podrán responder, pero las máquinas actuales no.

De acuerdo con Cabezas, Sabaté, Vendrell y Marcos (2014, párr. 1), los CAPTCHA son

> unos "puzzles" que los webmasters incluyen en su sitio web para asegurarse de que los visitantes que quieren interactuar con el contenido son personas, y no robots spam que tratan de registrarse en el sitio web, incluir comentarios en blogs, etc. (párr. 2)

Estos requieren inteligencia humana, por lo que "benefician al propietario de un sitio web porque filtran los no deseables robots spammers, y de paso pueden proporcionar mayor percepción de seguridad al usuario" (Cabezas et al, 2014, párr. 2).

Desde los inicios de internet, determinados usuarios han querido hacer el texto ilegible para los ordenadores. Los primeros fueron los hackers, que pensaban que los foros sobre temas sensibles eran supervisados automáticamente por ordenadores mediante palabras claves. Para evitar tales filtros, sustituían una palabra por caracteres idénticos. Por ejemplo, *HELLO* podría ser |-|3|_|_() ó)-(3££0. A este método se le conoció más adelante como *leet* o *leetspeak*, como lo manifiestan Martínez y Prieto (2009).

En 1996, según Hernández y Ribagorda (2010, pp. 141-142), Moni Naor se convierte en pionero al mencionar algunas técnicas para diferenciar remotamente máquinas y humanos; en 1997 se utiliza por primera vez el motor de búsqueda de Altavista, cuando Andrei Broder y sus colegas desarrollan un filtro, mediante la generación de una imagen de texto impreso al azar que el sistema de reconocimiento de caracteres de las máquinas no puede leer. Cinco años más tarde, reconocieron que el sistema había reducido más del 95% de correo basura en poco más de un año.

Sin embargo, el término CAPTCHA se comienza a utilizar en el año 2000 en la Universidad de Carnegie Mellon, y responde a un juego de palabras, ya que la pronunciación de la palabra recuerda a *catch ya*, una versión informal de *I catch you* (te cojo o te pillo), según señalan Martínez y Prieto (2009). Allí, informan Hernández y Ribagorda (2010, p. 142), Udi Manber de Yahoo! presenta los *bots*[3] y la necesidad de evitarlos en los chat, para lo que los profesores Manual Blum, Luis A. von Ahn y John Langford desarrollan un *gimpy*, con palabras en inglés, al azar, presentado como una imagen de texto impreso con una amplia variedad de deformaciones y distorsiones, incluyendo la imágenes superpuestas de palabras diferentes.

3.1 Tipos de CAPTCHA

Los CAPTCHA, de acuerdo con Shirali-Shahreza y Shirali-Shahreza (2008), se clasifican fundamentalmente en métodos basados y no basados en OCR (*Optical Character Recognition*, por sus siglas en inglés)[4]. En los primeros, los más conocidos y usados en la actualidad, se presenta la imagen de una palabra con una distorsión de diversos efectos, la cual debe ser escrita por el usuario y, debido a los efectos pictóricos, no podrá ser reconocida por el equipo. Para su creación, se acostumbra llevar a cabo un procedimiento general (elegir una palabra de un diccionario predefinido, aplicar un formato a la palabra y convertirla en imagen y degradar la composición mediante distorsión), en el que se diferencian los métodos de generación por medio de los algoritmos de elección de palabras/diccionarios, el formato aplicado a los caracteres y las degradaciones realizadas sobre las imágenes.

En el segundo grupo se presentan imágenes cuyos retos implican, para resolverlos, dar clic en una zona específica de la imagen, identificar una serie en las imágenes, mover algún componente de ella, o incluso formar cadenas de caracteres con las iniciales de los objetos representados. Una de las principales razones por las que los CAPTCHA basados en imágenes son vulnerables frente a ataques, es que en casi ninguna de las técnicas existentes estas son distorsionadas para evitar el reconocimiento de una máquina.

Adicionalmente, para Yan y Salah (2008), existen los sistemas basados en sonido (o los sistemas de audio), los cuales, por lo general, requieren de reconocimiento de voz para resolver una tarea.

En la tabla 1 se presentan algunas técnicas de generación de CAPTCHA separadas según si están basadas en texto o en imagen. De igual manera, en la tabla 2 se presenta una comparación realizada por Saquinaula (2013).

[3]Entendido como un programa informático que realiza distintos cometidos y que trata de simular a un humano.

[4]Vásquez (2010) los ha denominado como basados en texto y basados en imagen, respectivamente.

3.2 Aplicaciones de los CAPTCHA

Los CAPTCHA, como sistemas que diferencian personas de máquinas, tienen multiplicidad de aplicaciones relacionadas con la seguridad en diferentes sectores de la sociedad actual. Algunas de ellas, de acuerdo con von Ahn, Blum, Hopper y Langford (2003), son:

- Encuestas por internet. A partir de la experiencia de Slashdot[5] apareció la necesidad de crear un mecanismo para evitar que las encuestas por internet fueran amañadas mediante el uso *bots* y así asegurar que los votos provinieran de personas y no de máquinas.
- Servicios gratuitos de correo electrónico. Hoy en día muchas empresas proporcionan servicios de correo electrónico gratuito, y la mayoría de ellas son vulnerables a ataques de *bots*, que pueden solicitar miles de cuentas de correo en un minuto. Esta situación se soluciona fácilmente si se pide a los usuarios identificarse como humanos antes de obtener su cuenta.
- Motores de búsqueda. Los *bots* de indexación de los motores de búsqueda recorren internet para poder localizar páginas web y añadirlas a sus índices. Aunque algunos sitios web utilizan una etiqueta HTML para no ser incluidos en los motores de búsqueda, esto no asegura que no sean localizados ni que su código HTML no sea recorrido por un *bot*. Para evitar que la privacidad de esta página sea violada por *bots*, es necesario recurrir a un CAPTCHA.
- Correo electrónico en cadena y spam. Los retos CAPTCHA también son utilizados como solución para evitar el envío de cadenas de correo electrónico o *spam*. De esta forma, sólo son aceptados aquellos correos cuyo emisor haya probado que es una persona.
- Prevenir ataques de diccionario. Una aplicación algo más novedosa es el uso de CAPTCHA para prevenir los ataques de diccionario de sistemas de autenticación mediante contraseña. La idea es muy sencilla y se basa en evitar que una máquina pueda probar ilimitadamente todas las palabras clave que desee. Esta técnica la implementan sistemas tan populares como *Twitter*, y permite realizar tres intentos fallidos al introducir la contraseña, el resto de oportunidades deben ser validadas por un CAPTCHA.

[5]En noviembre de 1999, Slashdot realizó una encuesta online para conocer la opinión de los usuarios sobre cuál era la mejor universidad americana de informática. Como en casi todas las encuestas vía web, las direcciones IP de donde procedían los votos se almacenaron para prevenir que un usuario pudiera votar más de una vez; sin embargo, los estudiantes de la Universidad de Carnegie Mellon encontraron una forma para amañar las votaciones utilizando programas que realizaban miles de votaciones a favor de su universidad, y así subieron su puntuación rápidamente. Al día siguiente, estudiantes de MIT implementaron su propio programa para conseguir votos y la encuesta se convirtió en una competición entre los *bots* de ambas universidades. La MIT consiguió 21,156 votos y Carnegie Mellon 21.032, mientras el resto de universidades no superaron los 1000 votos, de acuerdo con lo expresado por von Ahn, Blum, Hopper y Langford (2003).

3.3 Ataques contra CAPTCHA

Tal y como sucede con cualquier tipo de aplicación usada para prevenir el uso ilícito de un servicio, los CAPTCHA son susceptibles a ataques, y dado su uso principal en la protección en el registro a correo web mediante formularios, la mayor cantidad de ataques proviene de los *spammers,* quienes sostienen una constante búsqueda de registro y uso gratuito de múltiples cuentas de correo. Aunque aquí se mencionarán algunos de los ataques más conocidos, es importante tener en cuenta que estos se mantienen en constante desarrollo, al igual que los esfuerzos por prevenirlos, por lo que "realmente siempre ha sido claro para los creadores de captchas que estos tendrán una vida útil determinada y solo un alto porcentaje (se espera que muy alto) de efectividad" (Elizondo, 2008, p. 77).

3.3.1 Romper un CAPTCHA resolviéndolo automáticamente

La firma de seguridad Websense (2012) ha informado sobre una nueva versión del troyano *Cridex* que permite vulnerar el servicio CAPTCHA ubicado por *Yahoo* en su formulario de registro, y así acceder a múltiples cuentas de correo electrónico para usarlas como cuentas de envío masivo. En el informe se muestra cómo, luego de cinco intentos fallidos, el troyano logra solucionar el desafío CAPTCHA. Sin embargo, es pertinente señalar que, además de la nueva variante de *Cridex*, existen múltiples programas destinados a solucionar los caracteres que aparecen en un CAPTCHA de forma automática.

3.3.2 Método de resolución semiautomático

Baquia (2008) informa que una investigación elaborada por TrendLabs alerta de la aparición de un método semiautomático empleado por ciberdelincuentes para sortear estos controles de seguridad, cuyo proceso consiste en que, primero, un programa robot visita la página de inscripción de un *webmail* y diligencia el formulario con datos aleatorios y cuando aparece la verificación CAPTCHA, el programa envía el mensaje a un terminal informático ubicado en India, donde los trabajadores introducen la combinación correcta de letras y números y vuelven a enviar la información al programa robot. Este introduce la clave y completa el proceso de registro, permitiendo así a los creadores de *spam* el acceso gratuito a las cuentas de correo, desde las cuales comienzan a distribuir los mensajes entre miles de cuentas de correo legítimas.

3.3.3 Vulnerar el algoritmo de generación de CAPTCHA

El algoritmo ejecutado para generar los CAPTCHA puede ser vulnerado con el fin de conocer el texto antes de que sea presentado al usuario; sin embargo, este tipo de ataque es difícil de completar debido a que los algoritmos modernos están muy bien desarrollados, son de código abierto y revisados por múltiples personas, lo cual implica invertir gran cantidad de recursos para romper este tipo de lógica. La probabilidad de la vulneración se

incrementa cuando un proveedor de servicio usa un sistema de generación de CAPTCHA muy antiguo, a diferencia de los reCAPTCHA[6], muy seguros en este aspecto.

3.3.4 Resolver el CAPTCHA manualmente

Este tipo de ataque puede sonar contradictorio, ante la siguiente pregunta: ¿si se tiene la opción de atacar un CAPTCHA de manera automática, para qué se pretendería realizar un ataque que lo resuelva manualmente? La razón es sencilla: si los CAPTCHA son creados para ser resueltos por humanos, la forma más sencilla de solucionarlo es por un humano, cuyas opciones para conseguirlo son:
- Embeber el CAPTCHA que se quiere romper dentro de otro servicio web, el cual es ejecutado por el atacante; por ejemplo, un atacante puede tomar un CAPTCHA del formulario de registro de *Gmail*, presentarlo a un usuario y pedirle que lo resuelva para puede tener acceso a cierto tipo de contenido. En este caso, el usuario resuelve la prueba por el atacante y este puede completar el resto del formulario automáticamente y así tener acceso a una cuenta de correo que puede usar para *spam*.
- Resolver los CAPTCHA mediante la contratación de personas para descifrar tantos como puedan. Por ejemplo, *spammers* pueden pagar a un programador para agregar imágenes y alimentar una a una a un operador humano, y estas fácilmente podrían ser verificadas por cientos de usuarios cada hora. La eficacia de sistemas de verificación visuales es baja, y su utilidad es anulada una vez que son explotados (May, 2005).

Luego de realizar un estudio experimental sobre los CAPTCHA sonoros para descubrir la diferencia entre el nivel de comprensión del ser humano en distintas pruebas con sonidos que los usuarios deben descrifrar, y el de un reconocedor de voz automático, García (2013, p. 85) señala que:
- la tecnología actual de reconocimiento de voz está bastante lejos de poder resolver CAPTCHA sonoros con garantías;
- los CAPTCHA sonoros son algo más complicados de resolver que los gráficos, aunque, a la vez, son bastante más seguros;
- el reconocedor de voz no fue capaz de reconocer ninguno de los CAPTCHA con ruido de fondo, y de los que se les eliminó el ruido, no reconoció ninguno completo;
- como los CAPTCHA son un sistema seguro que resuelve la mayoría de usuarios, se presenta gran cantidad de errores en las pruebas con usuarios;
- los parámetros que provocan en mayor medida los fallos son la combinación de una menor distancia entre la pronunciación de los números y la velocidad de pronunciación.

[6]reCAPTCHA consiste básicamente en el reto de reconocer dos palabras, de las cuales una es desconocida (no obtenida de una imagen de OCR) y la otra, conocida para el sistema.

4. CAPTCHA Y ACCESIBILIDAD/USABILIDAD

A manera de aclaración sobre los términos accesibilidad y usabilidad, se recurre a De Óleo y Rodríguez (2013):

> La accesibilidad web permite que un sitio web pueda ser visitado y utilizado de forma satisfactoria por el mayor número posible de personas. De acuerdo con Nielsen (2001), la accesibilidad no sólo implica la necesidad de facilitar acceso, sino también la necesidad de facilitar el uso. Es difícil separar la usabilidad (facilidad de uso) de la accesibilidad (facilidad de acceso); y no sólo es difícil, sino en muchos casos, innecesario. En efecto, un diseño accesible debe aumentar la facilidad de uso para más personas en más situaciones o contextos (Henry, 2006). Y en sentido general, los principios de usabilidad y accesibilidad tienen como objetivo que el diseño de un sitio web permita que éste pueda ser accedido y usado por el mayor número posible de personas, independientemente de las limitaciones propias del individuo o de las derivadas del contexto de uso (Nielsen, 2001). (p. 102)

Es innegable que, a medida que se usan técnicas en los CAPTCHA para disminuir la posibilidad de que métodos automatizados puedan fungir como humanos, aumentando el ruido y las deformaciones de la imagen, como efecto colateral aumenta la dificultad para los usuarios, se conduce a altas tasas de error y, con ello, a mucha frustración.

A manera de confirmación de esto, Cabezas et al. (2014) citan la prueba a 318.000 CAPTCHA de 21 tipos (13 basados en textos, números o imágenes, y ocho sonoros), llevada a cabo a través de la plataforma *Amazon Mechanical Turk*, con un mínimo de tres personas por cada uno, donde se detectó la dificultad para resolverlos, especialmente los de audio, cuya dificultad aumenta para quienes no son hablantes nativos del idioma utilizado. Los autores aseguran, además, que diversas razones llevan a los usuarios a rendirse o a no tener una buena experiencia:

> - Los usuarios no siempre entienden qué acción se debe acometer, - Les resulta difícil o imposible visualizar el captcha, como en el caso de los re-captchas, que proponen al usuario que transcriba una serie de letras y/o números, y en ocasiones están tan distorsionados que es muy complicado, y - a menudo desconocen su utilidad.(Cabezas et al., 2014, párr. 5)

Cabezas et al. (2014) realizaron una prueba que consistía en resolver diez CAPTCHA, responder la pregunta de facilidad y contestar un test de veinte preguntas para valorar la satisfacción percibida en cuanto a la usabilidad y la utilidad de este sistema. En los resultados resaltan aspectos como:
- los usuarios inicialmente perciben como más fáciles aquellos CAPTCHA con los que están más familiarizados (los llamados reCAPTCHA), que en realidad han resultado ser los peor resueltos;

- otros tipos de CAPTCHA, concretamente los que están basados en imágenes y en los que los usuarios deben identificar elementos o conceptos, no se perciben como fáciles de resolver en un inicio; tras enfrentarse a ellos esta percepción cambia radicalmente, en unos casos, de forma muy positiva y se mantiene negativa en otros;
- los CAPTCHA de creación propia son percibidos como más difíciles, a pesar del grado de acierto mayor respecto de los re-CAPTCHA, resultado acorde con la idea de que los usuarios perciben como fácil aquello que ya conocen;
- las mayores puntuaciones en percepción de eficacia y facilidad, las tienen dos pruebas basadas en la identificación de imágenes, lo cual indica que este tipo de sistemas es más eficaz y se percibe como fácil de resolver por parte de los usuarios;
- el CAPTCHA semiótico (interpretación de imagen: manos), resuelto por el 100% de los participantes, debería de explorarse más, dado el alto grado de eficacia que presenta.

Por ello, para Gossweiler, Kamvar y Baluja (2009), la creación de un CAPTCHA sugiere la necesidad de evaluaciones de usabilidad, para garantizar que las personas puedan resolverlo en una cantidad de tiempo y con tasas de éxito razonables. Por ejemplo, al evaluar un CAPTCHA que requiere de los usuarios ajustar las imágenes con giro aleatorio en su orientación vertical, se encontró resulta familiar para muchas personas que usan cámaras digitales, teléfonos celulares con cámaras, e incluso que clasifican fotografías físicas.

Entre algunos ejemplos sobre los inconvenientes en la usabilidad de los CAPTCHA, se encuentran:
- Un informe del Grupo de Trabajo del W3C indica que los CAPTCHA pueden suponer un importante problema de accesibilidad para usuarios ciegos, con baja visión, o que tienen una discapacidad de aprendizaje como la dislexia, pero no se discutió cómo mejorar la usabilidad de los CAPTCHA, aunque se reconoció que deben ser 'amigablemente humanos' (Yan y Salah, 2008).
- Desde la aparición de los CAPTCHA, resultó claro que excluían de contestar correctamente no solo a las computadoras, sino también a los ciegos. Esto va en contra de la tendencia de volver la computación cada vez más accesible para los diferentes tipos de personas con discapacidad, lo que llevó al desarrollo de CAPTCHA auditivos, los cuales presentan una grabación de letras y números a los que se sobreponen ruidos (Elizondo, 2008, p. 76).
- La distorsión tiene un claro impacto en la usabilidad de letras cifradas, ya que para los usuarios humanos sería difícil o imposible reconocer el exceso de caracteres distorsionados. Según señalan Yan y Salah (2008), algunos casos típicos que llevan a confusiones al estar distorsionadas, se presentan al tratar de diferenciar S de 0, 6 de G y B, 5 de S/s o de 6, 2 de Z/z, 1 de l, 7 de 1, 8 de 6 o 9, 'vv' de 'w', 'cl' de 'd', 'nn' o 'rn' de 'm', 'rm' de 'nn', 'cm' de 'an', así como un arco de J. En los CAPTCHA de audio también se presentan confusiones, como en los casos de 'p' y 'b'; 'g' y 'j'; 'a' y '8'.

5. CONCLUSIONES

No hay desacuerdo alguno sobre la imperante necesidad de proporcionar seguridad a la información personal e institucional colocada en internet, que se incrementa exponencialmente día a día, ante la gran cantidad y constante posibilidad de ataques informáticos. Sin embargo, con soluciones como los CAPTCHA se han logrado resultados en relación con esto, aunque, de manera paralela y quizás insospechada, los CAPTCHA dificultan la accesibilidad/usabilidad de los usuarios a diversos servicios en el marco de la sociedad de la información y el conocimiento, situación que agrava la brecha digital existente. Lo anterior, antes que desvirtuar tal solución, pretende servir de aliciente para el debate académico sobre su efectividad integral, a partir de la pregunta que sirve de título al presente documento.

6. REFERENCIAS

Areitio, J. y Areitio, T. (2007). Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación. *Revista española de electrónica*, (630), 52-67.

Baquía (2008). *Romper un captcha sale barato* [Blog]. Recuperado de http://www.baquia.com/posts/romper-un-captcha-sale-barato

Cabezas, V., Sabaté, A., Vendrell, A. y Marcos, M. C. (2014). Experiencia de usuario y captchas, explorando la semiótica visual. *No Solo Usabilidad*, *13*. Recuperado de www.nosolousabilidad.com/articulos/usabilidad_captchas.htm

De Oleo, C. y Rodríguez, L. (2013). Pautas, métodos y herramientas de evaluación de accesibilidad web. *Ventana Informática,* (28), 99-115.

Elizondo, F. J. (2008). Enredándose, CAPTCHA. *Ingenierías*, *11*(38), 74-78.

García, F.J. (2013). *Experimentación con CAPTCHA sonoros* (Tesis de grado). Universidad de Valladolid, Valladolid, España.

Gossweiler, R., Kamvar, M. y Baluja, S. (2009). What's Up CAPTCHA?: A CAPTCHA Based On Image Orientation [¿Qué pasa CAPTCHA:? Un CAPTCHA basado en orientación de imagen]. En *18th international conference on World wide web WWW'09* [18va Conferencia internacional en World Wide Web] (pp. 841-850). Nueva York, NY, EE.UU.: ACM. doi: 10.1145/1526709.1526822

Hernández, C. J. y Ribagorda, A. (2010). Pitfalls in CAPTCHA design and implementation: The Math CAPTCHA, a case study [Errores en el diseño e implementación CAPTCHA: El CAPTCHA de Matemáticas, un estudio de caso]. *Computers & Security*, *29*(1), 141-157.

Martínez, D. y Prieto, O. (2009). Servicios Accesibles de Acceso Exclusivamente Humano. En *Segunda Conferencia Internacional sobre brecha digital e inclusión social* 9 (pp. 1-12). Universidad Carlos III de Madrid y Universidad de Costa Rica. Leganés, Madrid, España. Recuperado de http://orff.uc3m.es/bitstream/10016/10622/1/servicios_accesibles_CIBD_09.pdf

May, M. (2005). *Inaccessibility of CAPTCHA: Alternatives to Visual Turing Tests on the Web* [La inaccesibilidad del CAPTCHA: Alternativas a las pruebasvisuales de Turing en la Web]. W3C Working Group Note. Recuperado de http://www.w3.org/TR/turingtest

Mori, G. y Malik, J. (2003). Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA [Reconociendo objetos en Clutter adversario: Fracturando un CAPTCHA visual]. En *IEEE Computer Society Conference on Computer Vision and Pattern Recognition, CVPR'03* [IEEE Conferencia de la Sociedad en Computación en Visión por Computadora y Reconocimiento de Patrones]. IEEE. Recuperado de http://www.cs.sfu.ca/~mori/research/papers/mori_cvpr03.pdf

Saquinaula, G.R. (2013). *Análisis del CAPTCHA: caracyerísticas, problemática y aplicaciones*. (Tesis de grado). Universidad Tecnológica Israel, Quito, Ecuador.

Shirali-Shahreza, M. y Shirali-Shahreza, S. (2008). Encouraging persons with hearing problem to learn sign language by Internet websites [Alentar las personas con problemas de audición para aprender el lenguaje de signos por los sitios web de Internet]. *Eighth IEEE International Conference on Advanced Learning Technologies, ICALT '08* [Octava Conferencia Internacional IEEE sobre Tecnologías Avanzadas de Aprendizaje]. IEEE. Recuperado de http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-345/paper8.pdf

Vázquez, A. M. (2010). *Diseño e implementación de un protocolo seguro de intercambio de mensajes con un dispositivo seguro* (Proyecto final de graduación). Universidad Carlos III de Madrid, Madrid, España.

Von Ahn, L., Blum, M., Hopper, N. J. y Langford, J. (2003). CAPTCHA: Using hard AI problems for security [CAPTCHA: Usando problemas duros de la IA para la seguridad]. En *22nd international conference on Theory and applications of cryptographic techniques EUROCRYPT'03* [22a Conferencia Internacional sobre Teoría y Aplicaciones de las Técnicas Criptográficas]. International Association for Cryptologic Research (IACR).

Websense. (2012). *Trojan caught on camera shows CAPTCHA is still a security issue* [Trojan captado por la cámara muestra CAPTCHA es todavía un tema de seguridad] [Blog]. Recuperado de http://community.websense.com/blogs/securitylabs/archive/2012/01/30/trojan-caught-on-camera-shows-captcha-is-still-a-security-issue.aspx

Yan, J. y Salah El Ahmad, A. (2008). Usability of CAPTCHAs or usability issues in CAPTCHA design [Usabilidad de CAPTCHAs o problemas de usabilidad en el diseño de CAPTCHA]. En *4th symposium on Usable privacy and security, SOUPS '08* [Cuarto simposio sobre la privacidad utilizable y la seguridad]. ACM.

7. TABLAS, CUADROS Y FIGURAS

Tabla 1
Técnicas de generación de CAPTCHA más populares, clasificadas por tipo

Tipo	Técnica de generación	Observaciones
Técnicas basadas en texto	Gimpy	Primera implementación con usos comerciales que apareció en la Web. Las distorsiones más comunes son la inclusión de fondos con degradaciones y líneas tipo parrilla, aplicación de deformaciones no lineales, difuminación de la imagen total e inclusión de pixeles de ruido de fondo. El método Gimpy original consiste en un reto formado por siete palabras, que pueden repetirse, repartidas por la imagen de forma aleatoria, normalmente superpuestas dos a dos; el usuario debía reconocer tres de ella para superarlo. Debido a no cumplir los requisitos mínimos de usabilidad y seguridad se evoluciona hacia EZ-Gimpy[7], que se simplifica al aparecer una única palabra. Los CAPTCHA generados con está técnica pronto fueron rotos, debido a su limitado diccionario constituido por 860 palabras en inglés, y la poca variedad de fuentes aplicadas a los caracteres o las distorsiones aplicadas a las imágenes.
	Pessimal Print	Se basa en los defectos que aparecen en los textos cuando se realizan múltiples copias, escaneos o impresiones por imprentas antiguas. Algunas de las distorsiones que aplica son: la aparición de letras; los contornos discontinuos de los elementos; la fragmentación de caracteres o la desaparición de ciertos fragmentos del carácter; la aparición de pequeñas manchas que no corresponden a ningún elemento del texto; y la utilización de fuentes de letras condensadas y/o cursivas. Estas modificaciones suponen un reto para la inteligencia artificial, pero también conllevan restricciones a las personas que deben conocer el alfabeto Latino, la lengua inglesa y tener experiencia en la lectura de esta lengua, ya que la fragmentación de los caracteres puede llevar a equívocos. Se ha demostrado que cuando el atacante conoce de antemano la fuente de letra utilizada, la probabilidad de éxito es del 40%, además, es vulnerable a métodos de restauración de imágenes usados por los OCR actuales. Una versión más moderna de esta técnica es utilizada por reCaptcha.
	MSN CAPTCHA	Se utilizó en servicios on-line de Microsoft (como Hotmail, MSN y Windows Live), muy popular hasta que fue roto en el 2006 y sus deficiencias fueron divulgadas en el ámbito científico. No se conoce exactamente el algoritmo de generación del CAPTCHA, ya que Microsoft protegió sus implementaciones con varias patentes. El esquema se basa en un reto formado por ocho caracteres, en los que se incluye tanto dígitos como letras, siempre en mayúsculas, con una fuente de tipografía serif y color azul oscuro junto con un fondo de imagen liso de color gris claro para asegurar una lectura fácil. Se aplican distorsiones de curvatura sobre el texto tanto a nivel local, en forma de pequeñas olas y las deformaciones elásticas a lo largo de los píxeles del carácter, como a nivel global con deformaciones elásticas de la palabra, deformaciones que tratan de frustrar las técnicas en las que se basan los algoritmos detección, además, incrementa la seguridad añadiendo de forma aleatoria arcos de diferentes espesores para generar ruido en la imagen y evitar así los ataques por segmentación.
	Baffle Text	En primer lugar, se genera una palabra pronunciable, ya que así, un usuario humano tendrá mayor facilidad para responder al reto, pero sin que esta pertenezca al diccionario, para evitar que se produzcan ataques basados en el léxico, para ello, se hace uso de un generador fonético basado en el modelo de Markov. Una vez conseguida la palabra, a la que se le aplica una fuente, que elegida de forma aleatoria

Continúa

[7]Ya en 2003 se presentaban algoritmos que identificaban una imagen EZGimpy con una tasa de éxito del 92%, y de Gimpy, el 33% de las veces (Mori y Malik, 2003).

Tipo	Técnica de generación	Observaciones
		entre de un amplio rango de ellas, y se genera una imagen con un fondo simple que no contenga degradaciones. El sistema generará una segunda imagen formada por un conjunto de círculos, cuadrados y/o elipses que se superpondrá a modo de máscara sobre la imagen de la palabra aplicando una operación de suma, substracción o diferencia de contrastes de forma aleatoria entre las dos imágenes. Aunque la metodología resulta muy robusta frente a ataques de segmentación de caracteres, su baja usabilidad supone un grave problema en la implantación.
	Scatter Type	Diseñado para resistir ataques por segmentación de caracteres. Los retos se generan de forma pseudoaleatoria sintetizando una cadena de caracteres junto con un formato de letra en una imagen. Dentro de cada imagen, los caracteres de la imagen son fragmentados usando cortes horizontales y verticales, cada uno de los fragmentos generados se dispersan desplazándolos por los ejes de coordenadas x e y. La técnica de dispersión de caracteres se ha diseñado de forma rigurosa para frustrar los ataques por segmentación de caracteres mediante cualquiera de las técnicas que se conocen en la actualidad. No aplica complejas modificaciones sobre las imágenes favoreciendo la usabilidad, siendo los textos altamente reconocibles para las personas aunque el nivel de distorsión aplicado sea muy alto. A pesar de que los recientes esfuerzos para automatizar las habilidades perceptivas de los humanos han supuesto un progreso en el campo, los métodos más conocidos todavía no constituyen una amenaza para Scatter Type. Los datos experimentales muestran también que la calificación subjetiva de dificultad está fuertemente relacionada con la ilegibilidad.
Técnicas basadas en imagen	Bongo	Uno de los primeros proyectos del Instituto de Ciencias Computacionales de la Universidad Carnegie Mellon University, cuyo grupo de Inteligencia Artificial, en la actualidad, es puntero en la materia y las tecnologías aplicadas en ella. El reto se inspira en el conjunto de puzles de reconocimiento de patrones visuales creados por M.M. Bongard en 1967. Proporciona dos conjuntos de imágenes: las imágenes de la izquierda pertenecen a una categoría y los de la derecha a otra. El reto consiste en determinar a cuál de los dos grupos pertenecen una serie de imágenes sin clasificar (izquierda o derecha). Sólo necesita que se solucionen correctamente cuatro imágenes para superar el reto lo que implica que un ataque con respuesta aleatorias tiene un acierto de alrededor del 6%. Por lo tanto, una máquina sólo tendría que probar, como máximo, 17 veces antes de superar el reto.
	PIX	Basa su potencia en una base de datos que contiene imágenes etiquetadas por conceptos. Dado que a una misma imagen pueden asociarse distintos conceptos, la técnica desarrollada por L. von Ahn genera un reto que contiene cuatro imágenes distintas sobre una misma idea y el usuario deberá o bien escribir el nombre de la idea mostrada o bien elegir la palabra que mejor describe las imágenes de una lista de opciones lo suficientemente larga para minimizar los aciertos por azar.
	IMAGINATION	Diseñado para ser robusto frente a ataques automatizados ofreciendo a su vez una interfaz amigable para los usuarios. El reto consta de dos pasos que permite reconocer con claridad y rapidez a los humanos: El primer reto consiste en una imagen compuesta, es decir, un mural de imágenes, para superarlo el usuario deberá localizar uno de los límites entre las subimágenes por las que está compuesto y hacer clic sobre él. El algoritmo escoge aleatoriamente de una base de datos ocho imágenes que ejemplifican conceptos simples u objetos, cada uno de estas imágenes se escala e inserta en una de las ocho particiones aleatorias realizadas con anterioridad en el área de la imagen final. Una vez que se han acoplado todas las imágenes formando una nueva composición, esta será distorsionada aplicando distintos difuminados de colores por regiones seleccionadas de forma aleatoria. La distorsión consigue difuminar los límites entre las imágenes ya que los pixeles adyacentes, aún perteneciendo a imágenes distintas, comparten gama de colores lo que hace más complejo identificar los límites

Continúa…

Tipo	Técnica de generación	Observaciones
		entre las imágenes para una máquina pero no para las personas. El segundo reto que compone el sistema es un ejemplo típico de CAPTCHA visual, la interfaz consta de una imagen y una lista de palabras de las cuales tan sólo una describirá el objeto o concepto que se muestra. A diferencia de otros CAPTCHA, la imagen se encuentra distorsionada mediante una combinación de difuminados, particionamientos de la imagen, quantización de los colores, inclusiones de líneas, puntos o mayas de ruido, desdibujamiento de contornos y modificaciones en las gamas de colores.
	Simplified 3D to 2D	El esquema de generación de CAPTCHA de imágenes de 3D a 2D requiere un algoritmo de transformación algo complejo y una amplia base de datos de imágenes, con estos recursos es sencillo encontrar un algoritmo que genere retos sin mucho costo computacional. El test de Turing, implementado para diferenciar a las personas de las máquinas, se basa en la capacidad humana para transformar una imagen de 3D a 2-, por ejemplo, relacionar un cubo con un cuadrado o conocer que la base de un cilindro es un círculo y su lado un rectángulo.

Fuente: Construida a partir de Vázquez, 2010.

Tabla 2
Comparación de los diez mejores CAPTCHA

CAPTCHA	Características			
	Seguridad alta	**Tecnología soportada**	**Sonido**	**Imagen**
TheCAPTCHA	X	PHP		X
Securimage	X	PHP	X	X
ReCAPTCHA	X	PHP	X	X
JCAPTCHA	X	JAVA	X	X
NuCAPTCHA	X	JavaScript, HTML5, Flash	X	X
ProtectedWebForm.com	X	PHP	X	X
Free CAPTCHA-Service	X	Multi-platdform	X	X
CAPTCHA Confident	X	Multi-platdform	X	X
IronClad CAPTCHA	X	PHP	X	X
BotDetect CAPTCHA	X	ASP, PHP, Perl	X	X

Fuente: Saquinaula, 2013, p. 43.