II Conferencia Internacional sobre Brecha Digital e Inclusión Social
(Leganés, Madrid, del 28-30 de octubre de 2009)

SERVICIOS ACCESIBLES DE ACCESO EXCLUSIVAMENTE HUMANO

Oscar Prieto Gordo
Departamento de Ingeniería y Arquitecturas Telemáticas, Universidad Politécnica de Madrid, España
oprieto@diatel.upm.es
Daniel Martínez Ávila
Departamento de Biblioteconomía y Documentación, Universidad Carlos III de Madrid, España
daniel.martinez@uc3m.es

RESUMEN: En la Sociedad de la Información surgen nuevos servicios que se ofrecen a través de Internet, en los que es necesario realizar un registro previo antes de utilizarlo. En este punto entra en juego la forma de restringir el acceso a las máquinas para que no realicen un uso masivo del servicio. La forma más extendida de permitir el acceso exclusivamente humano son los denominados CAPTCHA, pero este sistema llega a convertir los servicios en inaccesibles. Por lo tanto, es necesario ofrecer distintas alternativas para conseguir servicios accesibles de acceso exclusivamente humano.

PALABRAS CLAVE: Accesibilidad, Web, CAPTCHA, Acceso humano, Integración tecnológica, Sociedad de la Información.

1. introducción

En la llamada Sociedad de la Información, la accesibilidad es una cuestión que incumbe a todas las personas ya que no es una cuestión de sensibilidad sino de derecho y por lo tanto es necesario hacer llegar a la mayor cantidad de usuarios la posibilidad de acceder a Internet para facilitar la integración tecnológica.

Con la aparición de herramientas que automatizan el acceso a servicios web surge la necesidad de que las máquinas no puedan realizar ciertas acciones, tales como registrar cuentas de correo o consultar precios de vuelos por Internet, para no hacer un uso masivo de este servicio.

Los sitios web que ofrecen servicios en los que hay que registrarse (clientes de correo, foros, etc.) han tomado medidas para asegurar que dan sus servicios a usuarios humanos y que no están siendo explotados por robots.

Un método común de limitar el acceso a los servicios disponibles en la web es la verificación visual de una imagen. El sitio web verifica que el usuario es humano pidiéndole que lea un conjunto de caracteres distorsionados, que aparecen en una imagen, para después introducir estos caracteres en un formulario. Esta prueba recibe el nombre de CAPTCHA. Naturalmente, esta imagen no tiene el equivalente en texto acompañándola, ya que si lo tuviera podría ser tratado por una máquina. En la actualidad, esto es un problema para los usuarios con visibilidad reducida, personas ciegas o que tienen algún problema de aprendizaje, como la dislexia.

En este trabajo se explica en detalle qué son los CAPTCHA, en qué se basa su funcionamiento, su origen, sus características y las aplicaciones que tienen. También se describen los ataques que pueden sufrir por parte de las máquinas para evitar el grado de seguridad que proporcionan. A continuación, se exponen los

problemas de acceso que tienen los CAPTCHA para las personas y se detallan las posibles soluciones existentes para evitar esta barrera, como son la salida de sonidos, la identificación única, etc. Además, siguiendo la experiencia docente de los autores, el trabajo se centra en la integración de la tecnología dentro de un aula. Se recogen las diferentes dificultades con las que se han encontrado personas con distinto bagaje cultural, edad y dominio de un ordenador y se exponen los resultados obtenidos de esta experiencia.

2. OBJETO DE ESTUDIO: LOS CAPTCHA

CAPTCHA es el acrónimo de *Completely Automated Public Turing test to tell Computers and Humans Apart* (Prueba de Turing pública y automática para diferenciar máquinas y humanos).

Se trata de una prueba "desafío-respuesta" utilizada en computación para determinar cuándo el usuario es o no humano. El término se comenzó a utilizar en el año 2000 en la universidad de Carnegie Mellon y responde a un juego de palabras, ya que el sonido de la palabra al ser pronunciada recuerda a "*catch ya*", una versión informal de "*I catch you*" ("te cojo" o "te pillo")

La prueba típica consiste en que el usuario introduzca un conjunto de caracteres que se muestran en una imagen distorsionada que aparece en pantalla, tal y como muestra el ejemplo de la Figura 1. Se supone que una máquina no es capaz de comprender e introducir la secuencia de forma correcta, por lo que solamente un humano podría hacerlo.

Figura 1: Ejemplo típico de un CAPTCHA

En la figura se muestra una secuencia de caracteres que dificulta el reconocimiento de la máquina rotando y distorsionando las letras. Como el test es controlado por una máquina en lugar de por un humano, como en la prueba de Turing, también se les denomina Prueba de Turing inversa. La prueba de Turing es un procedimiento desarrollado por Alan M. Turing (A. M. Turing, 1950, p.433-460) para identificar la existencia de inteligencia en una máquina. La máquina debe hacerse pasar por humana en una conversación con un hombre a través de una comunicación de texto estilo chat. Al sujeto no se le avisa si está hablando con una máquina o una persona. Si el sujeto es incapaz de determinar si la otra parte de la comunicación es humana o máquina, entonces se considera que la máquina ha alcanzado un determinado nivel de madurez: es, en cierta forma, inteligente.

2.1. Origen de los CAPTCHA

Desde los primeros días de Internet determinados usuarios han querido hacer el texto ilegible a los ordenadores. El primer grupo de gente fueron los hackers, que pensaban que los foros sobre temas sensibles eran supervisados automáticamente por ordenadores utilizando 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*".

La primera discusión sobre las pruebas automatizadas que distinguen a seres humanos de las computadoras en la web aparece en un artículo de 1996 de Moni Naor del instituto de Weizmann (M. Noar, 1996) de la ciencia titulado "Identificación a través del test de Turing".

Los CAPTCHA primitivos se desarrollaron sobre el año 1997 en AltaVista por Andrei Broker para prevenir que las máquinas añadan URL (*Uniform Resource Locator*) a su motor de búsqueda. Se buscó hacer las

imágenes resistentes a los ataques de sistemas OCR (Reconocimiento Óptico de Caracteres), que extraen de una imagen los caracteres que componen un texto para almacenarlos en un formato con el que puedan interactuar programas de edición de texto. De esta forma, se crearon los primeros puzzles.
En el año 2000, Luis von Ahn y Manuel Blum (L. von Ahn y M. Blum, 2000) desarrollaron y publicaron la definición de CAPTCHA, que incluyó cualquier programa que pudiera distinguir a seres humanos de las computadoras. Además, inventaron múltiples ejemplos, incluyendo el primer CAPTCHA propiamente dicho, que fue muy utilizado en Yahoo.

Los CAPTCHA tienen las siguientes características por definición, incluidas también en las siglas del nombre:

- Son completamente automatizados (*automated*), es decir, no es necesario ningún tipo de mantenimiento o intervención humana para su producción. Esto supone grandes beneficios en cuanto a fiabilidad y coste. Sería inimaginable que tuviera que existir una persona generando el CAPTCHA.
- El algoritmo utilizado es público (*public*). De esta forma la ruptura de un CAPTCHA pasa a ser un problema de inteligencia artificial y no la ruptura de un algoritmo secreto.

2.2. Aplicaciones de los CAPTCHA

Los CAPTCHA son utilizados para evitar que los robots puedan utilizar ciertos servicios. Por ejemplo, para que no puedan participar en chats, registrarse para usar cuentas de correo electrónico o más recientemente, para evitar que el correo basura (*spam*) pueda ser enviado por una máquina (ya que el remitente debe pasar el test antes de que se entregue al destinatario)

Los servicios de acceso exclusivamente humano se han extendido muy rápidamente, de forma que ahora se encuentran en cualquier servicio de Internet que pueda ser objeto de un ataque masivo por parte de máquinas con intenciones maliciosas. Por ejemplo, en el uso de encuestas por Internet, la página web pide superar un CAPTCHA antes de mandar el voto del usuario, ya que esa encuesta podría ser fácilmente falseada con un robot. Otros casos son las consultas de precios de vuelos por Internet o la introducción de comentarios en blogs y foros.

3. ATAQUES CONTRA SISTEMAS CAPTCHAS

Un ataque contra un CAPTCHA consiste en intentar, de forma automatizada, realizar el trabajo que realizaría un humano: resolver el problema que se plantea, ya sea visual, acústico u otros.

Un CAPTCHA no es más que un desafío compuesto a partir de un dato fuente. El objetivo del atacante es realizar el proceso de forma inversa y encontrar la fuente a partir del desafío.

En los últimos años se vienen estudiando técnicas y desarrollando tecnologías que, aunque en principio no tenían como fin romper los CAPTCHA, se pueden utilizar de una u otra manera para ello. Estas tecnologías son diferentes en función del sistema que se haya implementado en el CAPTCHA y son, básicamente, las siguientes.

3.1. Sistemas de reconocimiento de caracteres (OCR)

Su mayor uso ha sido el de la digitalización de documentos escritos y previamente digitalizados en forma de imagen. Hoy en día la mayoría de los CAPTCHA muestran una serie de caracteres en forma de imagen que el usuario debe escribir en un cuadro de texto. Normalmente estas imágenes deforman algunas letras o incorporan líneas y otros “impedimentos” a la imagen para evitar la interpretación automatizada.

Por otro lado, estos "imperfectos" se presentan también en los documentos digitalizados y los programas de OCR, que tenían como fin la digitalización de documentos, han incorporado distintas líneas de investigación en el procesado digital de imágenes para conseguir interpretar correctamente estos caracteres.

3.2. Sistemas de reconocimiento del habla

Uno de los mitos de la evolución de la informática y la computación ha sido desde siempre la comprensión del habla: que la interfaz de los humanos con las máquinas sea la voz. La parte de la comprensión del texto es algo que ya está bien conseguido y más o menos logrado; el problema de estas tecnologías es la definición de un interfaz comprensible para manejar el ordenador completamente con la voz.

Uno de los sistemas de CAPTCHA alternativo a las imágenes con textos es el de archivos de audio con letras habladas y sintetizadas por un software específico. Por tanto, se podría utilizar el software de comprensión de voz para resolver el desafío.

3.3. Analizadores sintácticos

Permiten buscar las funciones de las palabras dentro de un texto para mejorar la traducción automatizada. Mediante el uso de esta tecnología podría buscarse, por ejemplo, la respuesta a una pregunta de aritmética simple expresada de forma textual, que es un mecanismo utilizado por algunos CAPTCHA.

Como en otros tipos de CAPTCHA, se pueden utilizar vías de investigación alternativas para complicar la resolución del desafío aunque, a diferencia de las imágenes y el sonido, es una tecnología desarrollada "con malos fines" la que se utiliza para complicar el desafío, no resolverlo, como por ejemplo la astucia utilizada por los generadores de correos basura para evitar ser detectados por los filtros de correo sin dejar de ser legibles: alteración de letras, mezcla de idiomas, caracteres de puntuación intermedios, etc.

3.4. ¿Cómo funciona la lucha contra estos ataques?

Como en otras muchas áreas, el proceso se convierte en crear sistemas de mayor complejidad. En principio los parámetros que dificultan la resolución son la aleatoriedad de los componentes del CAPTCHA y la existencia de un elemento lógico; por lo que es importante incorporar diferentes dificultades que se van añadiendo de forma aleatoria al sistema.

La evolución más notable y la vía más compleja de resolver hoy en día el problema de los ataques es la mezcla de varios sistemas básicos, normalmente aquellos que usan la lógica y las imágenes. Uno de estos sistemas avanzados está siendo desarrollado por Microsoft (J. Elson et al. 2007) dentro del proyecto ASIRRA (*Animal Species Image Recognition for Restricting Access*). Consiste en escoger las fotos de gatitos dentro de una serie de fotos de animales obtenidas de Petfinder.com.

4. PROBLEMÁTICA DE ACCESO PARA DIFERENTES DISCAPACIDADES

Como ya se ha indicado con anterioridad, los CAPTCHA basados en la verificación visual de una imagen son el método más cómodo y extendido a la hora de comprobar la humanidad del usuario que está accediendo a nuestro sistema. Aquellos sitios web con servicios gratuitos y atractivos para los usuarios, son los más propensos a sufrir los ataques de robots o "*spammers*" que no realizan ningún bien al servicio ofrecido. Es por ello que compañías de servicios por Internet y "*bloggers*" recurren al método más rápido para evitar estas agresiones: los CAPTCHA basados en la reproducción, en una imagen, de un texto distorsionado.

Este mecanismo es ampliamente usado desde hace ya varios años y es una respuesta buena en términos de usabilidad para el público general. Sin embargo, surge un problema claro a la hora de que determinados

grupos de personas con discapacidad accedan a estos servicios "securizados" mediante CAPTCHA tradicionales. Determinados grupos de usuarios nunca van a ser capaces de crear una cuenta de correo, comprar billetes de avión por Internet o escribir un comentario en un blog o foro por el simple de hecho de presentar una discapacidad claramente incompatible con estos sistemas de acceso exclusivamente humano. Estas personas serán, en primer lugar, y por razones evidentes, las personas ciegas, que no pueden ver las letras distorsionadas escritas en la imagen. Naturalmente, estos CAPTCHA no vienen acompañados por una reproducción equivalente del texto en formato HTML corriente (que podría ser leído por un programa de síntesis de voz para ciegos) ya que eso invalidaría por completo la propia definición de CAPTCHA y crearía un paso completamente libre para robots y otras amenazas.

A su vez, las personas con otro tipo de discapacidades visuales, aun no siendo tan severas como la ceguera total, también presentarán problemas a la hora de leer el texto del CAPTCHA. Estos problemas de visibilidad, que en muchas ocasiones pueden ser críticos a la hora de leer un texto normal en una web, se ven agravados en estas imágenes por el hecho de que las letras han sido distorsionadas por distintos métodos.

Las personas incluidas dentro de este grupo serían aquellas con visión reducida (miopía, cataratas…), que no pueden agrandar el tamaño de las letras porque se encuentran en formato de imagen, problema agravado por el hecho de que estos símbolos aparecen distorsionados. Otro grupo que tendría problemas son las personas con problemas para diferenciar colores (daltonismo, acromatopsia…) ya que, en ocasiones, estos CAPTCHA presentan falta de contraste entre letras y fondo, con el fin de hacerlos más complicados para los robots.

Cualquiera que haya hecho uso de un CAPTCHA en alguna ocasión, se habrá dado cuenta de que en ocasiones es incluso difícil reconocer algunas letras, aún cuando el usuario no tiene ningún problema visual grave. Se dan problemas especialmente entre letras minúsculas y mayúsculas que son muy similares (por ejemplo, la letra "y" o "s") o entre determinados caracteres que también son muy parecidos (por ejemplo, la letra "o" mayúscula y el número cero o la letra "ele" minúscula y el número uno) Si esto ya supone pequeños problemas a personas con visión correcta, no es de extrañar que aquellos con visión reducida tengan verdaderos problemas a la hora de acceder a los servicios protegidos por un CAPTCHA tradicional.

Por último, estos sistemas de acceso exclusivamente humano no sólo presentan problemas a aquellos con deficiencias visuales, también a las personas con problemas de aprendizaje como la dislexia o similares. Se llama dislexia a la incapacidad de algunas personas para leer y escribir correctamente, sin tener por otro lado, una deficiencia intelectual, ni motriz ni visual o en cualquier otro ámbito. Por lo tanto, al tratarse de una cierta dificultad a la hora de leer y asimilar los símbolos escritos del lenguaje, una persona disléxica encontrará problemas a la hora de enfrentarse a un CAPTCHA tradicional. Es importante hacer notar que una persona que es sólo disléxica, no presenta ningún otro problema psicológico ni tiene ninguna deficiencia mental, con lo que el uso de los servicios de Internet no presenta ningún problema (al margen evidentemente de la información escrita). En definitiva, se puede afirmar que el control de acceso exclusivamente humano tradicional falla a la hora de reconocer a las personas como humanos, convirtiendo en inaccesibles ciertos servicios que se ofrecen en la web.

5. POSIBLES SOLUCIONES

Existen otras posibilidades de controlar el acceso exclusivamente humano a parte de la tradicional distorsión de textos en imágenes. Estas posibilidades derivan en la creación de nuevos CAPTCHA, algunos de ellos tan efectivos como el tradicional de imágenes pero que presentan una mayor accesibilidad para personas con discapacidades.

Una buena "solución para todos" parte también de la combinación de dos o más de estos CAPTCHA a la hora de controlar el acceso humano. Si se ofrece la posibilidad de usar un sistema de reconocimiento humano a elegir entre varios, facilitamos una buena usabilidad para el público general, a la vez que se permite el acceso

a personas con discapacidad. Una persona sin problemas optará por el método más cómodo mientras que un ciego, por ejemplo, elegirá el único sistema compatible con su discapacidad.

A continuación se describen siete soluciones dadas hasta el momento como alternativas a la distorsión de textos en imágenes, todas ellas detalladas con sus pros y contras.

5.1. Puzzles lógicos

Una forma para diferenciar el comportamiento humano del comportamiento de una máquina es el uso de la lógica, ya que los robots pueden resolver operaciones matemáticas, pero nunca operaciones donde haya que usar la lógica. Ésta es, hoy por hoy, un terreno todavía totalmente humano.
De esta forma, se puede recurrir a puzzles lógicos, juegos de palabras o preguntas en las que haya que usar la lógica, dejando al margen la matemática. Esto permitiría dejar al margen a los robots. Para que fuera accesible para aquellas personas con discapacidad tendríamos que evitar los puzzles lógicos basados en imágenes o en relacionar imágenes.

Las principales desventajas de este sistema pasan por la flexibilidad que deberían tener las respuestas (si requieren entrada de textos) y el elevado número de posibles preguntas y/o juegos lógicos almacenados en la base de datos, para evitar intrusiones por parte de equipos automáticos que puedan aprender el orden de las respuestas. Otra solución sería no tener un gran número de preguntas pero variar aleatoriamente su orden, cosa que también es susceptible de ataque.
Pero el principal problema de estos puzzles lógicos sería que, al intentar permitir el acceso a personas con discapacidades visuales (evitando puzzles lógicos visuales), se estaría a su vez negando la entrada a individuos con discapacidad cognitivas que tienen mermadas sus capacidades de pensamiento lógico y que por lo tanto tendrían muchas dificultades a la hora de resolver estos puzzles lógicos.

5.2. Salida de sonidos

En términos de usabilidad de los CAPTCHA por parte del gran público, lo mejor es la utilización de elementos del lenguaje como las letras, las palabras o los números. Sin embargo, el uso de estos en forma de texto anula toda utilidad del sistema para prohibir la entrada de máquinas al mismo. Por lo tanto, lo más lógico sería la utilización de esos mismos elementos (letras, palabras, números) pero soportados por otro medio distinto al texto. La solución se encuentra en el uso del sonido para transmitir esa información: el contenido es el mismo pero el soporte es distinto y es, en principio, seguro frente a ataques de robots.

Algunos servicios de Internet ya utilizan CAPTCHA basados en la transmisión de sonidos para el control de acceso exclusivamente humano. Estos sistemas reproducen códigos o palabras, con cierta distorsión o ruido, que han de ser escuchados y posteriormente introducidos en una caja de texto, para comprobar el acceso humano.

La principal desventaja de este tipo de CAPTCHA es la misma que para los basados en imágenes, aunque trasladándose al terreno de las discapacidades auditivas. La sola utilización de este tipo de CAPTCHA permitiría el acceso a toda persona sana de oídos. Las personas sordas, con deficiencias auditivas o con algún tipo de trastorno cognitivo relacionado con la escucha, quedarían automáticamente fuera del servicio de Internet al que se desea acceder. Por lo tanto, al igual que los basados en reconocimiento visual, éstos no deberían ser utilizados de forma individual. Además, las máquinas están mucho más preparadas para el reconocimiento de voz que para el reconocimiento óptico de caracteres. Es por ello que el grado de distorsión relativa debe ser mayor en este tipo de CAPTCHA, pudiendo llegar hasta tal punto de que el código sea irreconocible.

5.3. Cuentas de uso limitado

Esta filosofía de trabajo, al no ser un sistema de control de acceso exclusivamente humano, queda ligeramente al margen de la definición estricta y ortodoxa de CAPTCHA. Se basa en el hecho de que cuando un usuario se da de alta en un servicio gratuito de Internet (webmail, compra de entradas, etc.), es raro que quiera hacer un uso masivo e inmediato de este servicio en un primer momento. Las necesidades de más utilidades y un uso más desarrollado se desarrollan con el tiempo de uso.

Partiendo de esta premisa, algunos servicios de Internet limitan, de forma explícita o implícita, la frecuencia de interacción del usuario con el servicio en sí. Por ejemplo, si un usuario quiere buscar entradas para un concierto, se le puede limitar a tres búsquedas diarias y una vez realizadas estas búsquedas se deshabilita su cuenta para el resto del día.

La creación de estos límites puede convertir en poco atractivos aquellos sitios web que en principio tenían gran valor para los robots.

La desventaja más importante pasa por el desarrollo de un proceso de prueba y error para conseguir el sistema de límites óptimo. Para ello, los diseñadores tendrán que dibujar una línea, a partir del estudio de las estadísticas, entre lo que sería un uso normal y lo que sería un uso excepcional. Además, esto puede conllevar que determinados usuarios por encima de la media queden insatisfechos con el servicio.

5.4. Comprobación no interactiva

Mientras que los CAPTCHA y otros acercamientos interactivos al control del *spam* son a veces eficaces, hacen que un sitio web sea más complejo. Esto es a menudo innecesario, ya que existen una gran cantidad de mecanismos no interactivos para comprobar si hay *spam* u otro contenido inválido. Este punto contiene dos acercamientos no interactivos: filtros de spam, en el cual una herramienta automatizada evalúa el contenido de una transacción, y estudios heurísticos, que evalúan el comportamiento del cliente.

En lo que respecta al filtrado anti-spam, se puede afirmar que en la actualidad está bastante desarrollado y extendido. Muchos blogs y chats recurren a estos sistemas para eliminar entradas y comentarios que han sido realizados por máquinas de forma automática. El uso de "*hot words*" o de filtros bayesianos es bastante popular. Son muy eficaces y quitan la carga cognitiva al usuario. Por lo general, eliminan mensajes calificados como *spam* (ya que superan un determinado umbral) y también marcan como "dudosos" otros mensajes para su posterior chequeo humano por parte del administrador del blog o chat.

De hecho, a pesar de que estos sistemas cometen errores en algunas ocasiones, se puede decir que un filtrado anti-spam bien diseñado es igual de efectivo que un CAPTCHA tradicional, con la ventaja de que evitamos al usuario el tener que hacer frente a éste.

El estudio heurístico, por su parte, se basa en la recolección de datos en el comportamiento de un determinado usuario, datos que pueden ayudar a llegar a una conclusión determinada (en este caso, que el usuario es un robot): páginas visitadas, volumen de datos, direcciones IP, tipo de entrada de datos, etc. La principal desventaja es que este sistema también requiere un estudio complejo del comportamiento de los usuarios "normales" y los "no normales".

Una última vuelta de tuerca a los CAPTCHA es el del uso de métodos heurísticos en los propios CAPTCHA con imágenes o con sonido: comprobar cómo el usuario ha respondido ante el test es tan importante como el hecho de si lo ha resuelto o no. Si, en la forma de actuar ante un CAPTCHA, nuestro sistema reconoce a un robot, el proceso de autenticación es eliminado automáticamente.

5.5. Sistemas de identificación únicos

Los sistemas de identificación generales, actualmente en desarrollo, son, como su propio nombre indica, sistemas que estarán presentes en todos los servicios web y en todas las páginas web y que permitirán conocer a un usuario de forma general, sin necesidad de identificarse tantas veces como servicios utilice.

El usuario sólo tendría que identificarse una vez, pero el gran reto de este sistema es que esté implantado en todos los recursos web, sin excepción, para que realmente sea útil y usable por todos. Este sistema resuelve, evidentemente, los problemas de accesibilidad a la hora de que una persona con discapacidad quiera entrar en un determinado servicio, ya que el usuario no tendrá que identificarse como humano, el propio sistema le reconocerá.

5.6. Biometría

Un sistema de acceso exclusivamente humano podría estar basado en los datos biométricos de los seres humanos. Los tests biométricos que se podrían utilizar son muy variados, aunque los más extendidos son los de reconocimiento de huella dactilar o los de retina.

Con la biometría no sólo se evita el uso abusivo de "*spammers*" y la creación de infinitas cuentas de usuario gracias a robots virtuales, sino que además permite la identificación de la persona de forma unívoca. Estos sistemas, combinados con el uso de sistemas de identificación únicos, permitirán un acceso totalmente humano a los servicios web y además de forma personal, sin riesgos de que nuestra identidad sea suplantada.

El principal obstáculo de esta tecnología es el desarrollo y la implantación de la infraestructura necesaria para que todo el sistema funcione; además de algunas cuestiones políticas y sociales que necesitan ser solucionadas. Sin embargo, Microsoft ya ha anunciado que tiene un sistema de reconocimiento biométrico instalado y funcionando y que podrá extenderse a gran escala en algunos años.

Estos sistemas solucionarían la problemática de las personas con minusvalías ya que cualquier persona podrá acceder a alguno de los métodos de reconocimiento humano, incluso las personas nacidas sin ojos pueden ser reconocidas por la huella dactilar, por ejemplo.

5.7. Tarjetas de crédito y DNI electrónico

El uso de las tarjetas de créditos y los DNI electrónicos para distinguir humanos de máquinas parece una solución rápida, sencilla y barata. Sin embargo, el principal problema con el que se encuentra es el de la inseguridad que generan estos sistemas aún hoy, un problema que no parece que será resuelto en un futuro cercano.

6. La Sociedad de la Información y la integración tecnológica

En la llamada Sociedad de la Información, la accesibilidad es una cuestión que incumbe a todas las personas ya que no es una cuestión de sensibilidad sino de derecho. Ningún ciudadano debe quedar excluido de los beneficios y ventajas que proporciona el avance tecnológico, ya que las TIC (Tecnologías de la Información y Comunicación) ofrecen nuevas perspectivas profesionales y de integración a las personas discapacitadas o no.

Si se centra el tema de la accesibilidad en las posibilidades que ofrece la web, es necesario nombrar uno de los organismos más relevantes en este ámbito, el *Web Accesibility Initiative* (WAI), perteneciente al W3C (WWW Consortium), que promueve la accesibilidad a través de una serie de directrices y estándares:

- Web Content Accesibility Guidelines 1.0 (WCAG 1.0) Mayo 1999.

•Web Content Accesibility Guidelines 2.0 (WCAG 2.0) Marzo 2004.
•Authoring Tool Accessibility Guidelines 2.0, 24 Febrero 2004.
•User Agent Accessibility Guidelines 1.0.

Es necesario considerar el intercambio científico y tecnológico, las posibilidades de acceso a la información, así como la capacidad de inter-relacionarse en forma inmediata y constante. El objetivo de la accesibilidad es hacer llegar a la mayor cantidad de usuarios la posibilidad de acceder a Internet para facilitar la integración tecnológica.

Se ha podido ver que un método común de limitar el acceso a los servicios disponibles en la web es la verificación visual de una imagen mediante la utilización de un CAPTCHA. En la actualidad, esto es un problema para los usuarios, no sólo para las personas con visibilidad reducida o que tienen algún problema de aprendizaje como la dislexia, sino para la mayoría de los interesados en los servicios que ofrece la web. Este problema acaba siendo un obstáculo para la accesibilidad y todo sistema que no sea accesible no podrá integrarse dentro del ámbito de la vida cotidiana.

Siguiendo la experiencia docente de los autores de este trabajo, se presenta a continuación un caso de estudio centrado en la integración de la tecnología dentro de un aula. Se recogen las diferentes dificultades con las que se han encontrado personas con distinto bagaje cultural, edad y dominio de un ordenador y se exponen los resultados obtenidos de esta experiencia.

6.1. Un caso de estudio: la integración tecnológica dentro de un aula

Resulta interesante evaluar el siguiente caso: el contexto se sitúa en la realización de un curso de formación de “Empleado de información al cliente” dirigido a personas mayores de cincuenta y cinco años y mujeres que han sufrido violencia de género. El grupo se encuentra formado por un total de treinta personas, de las cuales cinco tienen una edad comprendida entre 18 y 26 años y veinticinco personas son mayores de 55 años. El curso consta de 100 horas, de las cuales el 60% están destinadas a recibir formación de informática de usuario. Estas 60 horas se reparten en el manejo del sistema operativo Windows y de herramientas ofimáticas, así como la utilización de Internet. Hay que destacar que este grupo de personas poseen distinto bagaje cultural y dominio de un ordenador, habiendo cuatro personas que no han utilizado nunca un PC. Para facilitar la integración de la tecnología dentro del aula, cada uno de los alumnos dispone de un ordenador para seguir las explicaciones del profesor y realizar las prácticas propuestas.

Los resultados obtenidos en la utilización de buscadores de Internet o en la navegación de portales de información del tipo wikipedia (http://es.wikipedia.org) son muy positivos, consiguiendo un 100% de satisfacción en el aprendizaje y utilización de dichos portales, no entrañando ningún tipo de dificultad en su uso por parte de los alumnos. Los problemas llegan cuando se desea utilizar otros servicios que ofrece Internet como es el, ya indispensable, correo electrónico o la consulta de foros en los que es necesario registrarse previamente. Las dificultades se encuentran en la fase de registro, previa a la utilización del servicio. Si se desea crear una cuenta de correo electrónico, por ejemplo en el portal de Yahoo (http://es.yahoo.com), el último paso es la verificación de un CAPTCHA como el que se muestra en la Figura 2.

Figura 2: CAPTCHA ofrecido en el registro de una cuenta en Yahoo

En la Figura 2 pueden observarse distintos detalles: en primer lugar, la dificultad de descifrar el código; y en segundo lugar que no se ofrece una alternativa al CAPTCHA basado en imagen, excluyendo de esta forma a sectores de la sociedad que no podrán descifrar nunca el código.

Incluso viendo la imagen resulta difícil no equivocarse en ninguno de los caracteres, por lo que el siguiente paso se muestra en la Figura 3.

Figura 3: CAPTCHA ofrecido después de un intento

En la Figura 3 se propone la introducción de un nuevo código para poder seguir adelante en el registro de una cuenta de correo electrónico, previo fallo de la anterior imagen. El problema es que este proceso se repite varias veces hasta que se logra introducir correctamente uno de los códigos mostrados.

En el caso de estudio que se presenta en este trabajo ninguno de los alumnos consiguió pasar la prueba del CAPTCHA la primera vez y un total de dieciséis personas necesitaron más de cuatro intentos para poder registrar una cuenta de correo electrónico. Los resultados se muestran en el gráfico mostrado en la Figura 4. Es importante señalar que el número de intentos necesarios no depende de la edad de las personas que se enfrentan al desafío del CAPTCHA, ni al nivel de conocimientos informáticos ni al nivel de estudios, simplemente a la dificultad que entraña descifrar los caracteres que aparecen en las imágenes mostradas.

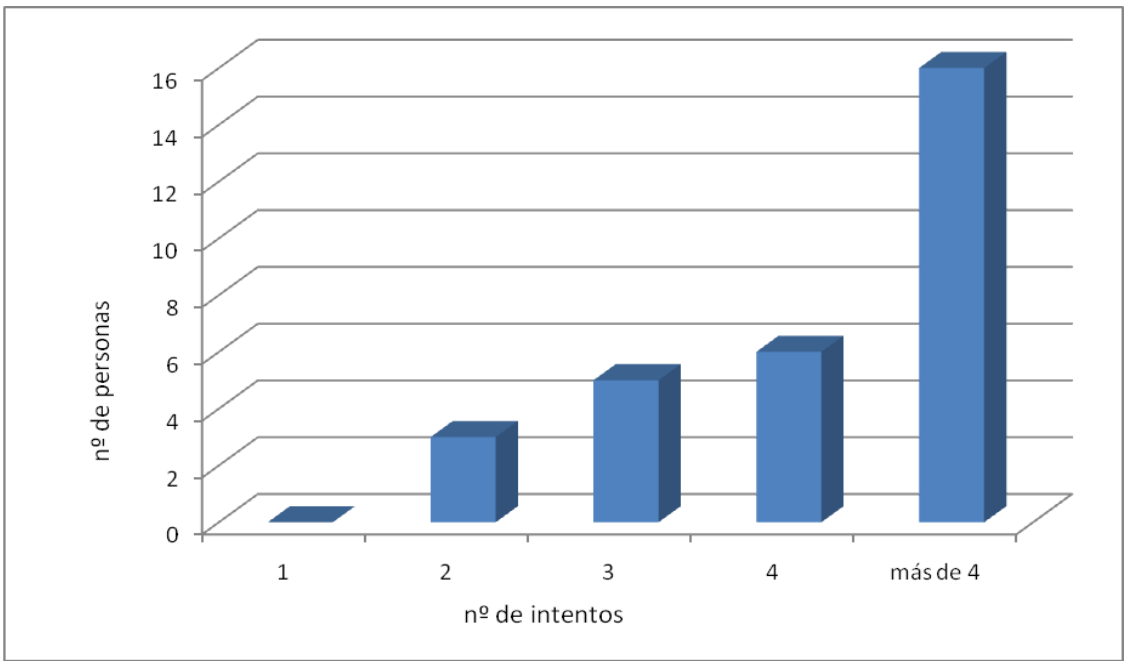

Figura 4: Número de intentos que necesitaron el total de 30 personas para crear una cuenta

Es necesario recordar que todo este proceso es sólo para crear una cuenta para la posterior utilización del correo electrónico, por lo que debe realizarse antes de poder hacer uso de un servicio que se ofrece en Internet. De estos resultados se desprende la frustración, la no satisfacción en el uso del correo electrónico, la pérdida de tiempo a la hora de registrar una cuenta, etc. Estos resultados serían similares en el uso de cualquier servicio que requiera de un registro previo, como puede ser la reserva de entradas o de vuelos, la utilización de foros, etc. Por lo tanto, se obtiene como conclusión que los servicios que se ofrecen en Internet en los que es necesario descifrar un CAPTCHA basado en imagen no son accesibles y por lo tanto se dificulta la integración tecnológica en todos los ámbitos de la persona, ya sea en la vida profesional o personal.

7. Conclusiones

El auge de Internet ha proporcionado una serie de nuevos e interesantes servicios. La mayoría de éstos requieren de la introducción de información por parte del usuario para poder tener acceso a ellos: creación de una cuenta de correo electrónico, consulta de precios de vuelos, reserva de entradas para espectáculos, etc. Dada esta necesidad de que el usuario introduzca información, estos servicios también se han hecho tremendamente atractivos para “personas virtuales” (máquinas que se hacen pasar por humanos), que atacan a los mismos accediendo miles de veces, creando una cantidad ingente de cuentas de correo, consultando información de manera indiscriminada, etc.

Esta problemática de acceso por parte de máquinas es una verdadera complicación para algunos servicios y los creadores buscan soluciones para hacer frente a un ataque cada vez mayor. Los CAPTCHA son una buena forma de resolver este problema ya que un CAPTCHA bien diseñado imposibilita la entrada a los robots que se hacen pasar por personas.

Sin embargo, los CAPTCHA tradicionales, los basados en imágenes, que por otro lado son los más extendidos, introducen verdaderos problemas de accesibilidad para las personas con problemas visuales o sin ellos. Todos aquellos sistemas que utilicen exclusivamente información visual van a ser muy buenos a la hora de discriminar robots y personas, pero también serán muy buenos a la hora de discriminar a los humanos con determinadas discapacidades o que sean incapaces de descifrar el desafío que propone un CAPTCHA.

Si bien los CAPTCHA tradicionales son una muy buena solución, en términos de usabilidad, para lo que fueron creados y no se recomienda que dejen de ser utilizados, sí se recomienda que se incorporen

alternativas en estas páginas de acceso a los servicios. Este trabajo propone la combinación de dos o más métodos de reconocimiento humano, de tal forma que sea el usuario el que pueda decidir qué desafío resolver a la hora de utilizar un servicio. El resultado final sería un servicio que cumple totalmente con sus funciones de acceso humano, que además sigua las pautas del diseño para todos y en el que se ofrezcan alternativas a la hora de resolver un problema. En la práctica, este tipo de implementaciones no resulta complicado y se consigue la satisfacción por parte del usuario a la hora de utilizar los servicios que se ofrecen.

REFERENCIAS BIBLIOGRÁFICAS

A. M. Turing. Computing machinery and intelligence. Mind: Vol. LIX. No.236, Octubre 1950, p.433-460.

Elson, J., Doceur, J.R., Howell, J., Saul, J. Asirra: A CAPTCHA that exploits Interest-Aligned Manual Image Categorization. Proceedings of 14th ACM Conference on Computer and Communications Security (CCS), Association for Computing Machinery, Inc., Octubre. 2007.

Festa, Paul. Spam-bot tests flunk the blind. 2003.

Mori, Greg. Breaking a Visual CAPTCHA. UC Berkeley Computer Vision Group, Simon Fraser University, 2003.

Naor, Moni. Identification via the Turing Test. Weizmann Institute of Science. 1996.

Raman, T.V. Audio CAPTCHAs when visual images are unusable. November 2006.

The CAPTCHA project: Can hard AI problems foil internet interlopers 2001. [Consulta: 09/09/2009]. Disponible desde Internet: www.captcha.net.

Von AHN, Luis, BLUM, Manuel. Developing CAPTCHA. 2000 Carneige Mellon University.

Von AHN, Luis, BLUM, Manuel, HOPPER, Hopper, LANGFORD, John. CAPTCHA: Using Hard AI Problems for Security. Advances in Cryptology, Eurocrypt 2003, p.294-311.

W3C Working Group. Inaccessibility of CAPTCHA. Alternatives to Visual Turing Tests on the Web. November 2005.

W3C Working Group. Web Content Accesibility Guidelines 1.0 (WCAG 1.0) Mayo 1999.

W3C Working Group. Web Content Accesibility Guidelines 2.0 (WCAG 2.0) Marzo 2004.

W3C Working Group. Authoring Tool Accessibility Guidelines 2.0, 24 Febrero 2004.

W3C Working Group. User Agent Accessibility Guidelines 1.0. Diciembre 2002.

Wikipedia, the Free Encyclopedia: Several articles. [Consulta: 09/09/2009]. Disponible desde Internet: www.wikipedia.org.

Yahoo. [Consulta: 09/09/2009]. Disponible desde Internet: http://es.yahoo.com