

LOS CONTROLES BIOMÉTRICOS

En la edición anterior de Estr@tegia Magazine habíamos comenzado a ver algunos métodos de autenticación e identificación de personas y decíamos que estos métodos suelen ser divididos en tres grandes categorías, en función de lo que utilizan para la verificación de identidad. Algo que la persona sabe (una clave por ejemplo), algo que la persona posee (una tarjeta magnética por ejemplo) y por último, una característica física o comportamiento propio de la persona a lo que se denomina autenticación biométrica.

A pesar de que los dos primeros métodos son los más utilizados hoy en día, incluso en forma combinada, parece que en un futuro no muy lejano los sistemas de autenticación biométrica serán los métodos que se van a imponer en la mayoría de situaciones en las que se haga necesario autenticar un usuario, debido principalmente a que quien lo utilice no va a necesitar recordar claves o números de identificación complejos, no necesitará llevar consigo algún objeto y además son sistemas mucho más difíciles de falsificar; las principales razones por la que no se han impuesto ya en nuestros días es su elevado precio, fuera del alcance de muchas organizaciones, y su dificultad de mantenimiento.

El reconocimiento de formas, la inteligencia artificial y el aprendizaje son las ramas de la informática que desempeñan el papel más importante en los sistemas de autenticación biométricos; la criptología, ciencia muy utilizada dentro de las técnicas actuales, se limita aquí a un uso secundario, como el cifrado de una base de datos de patrones retinales, o la transmisión de una huella dactilar entre un dispositivo analizador y una base de datos.

La autenticación basada en características físicas existe desde que existe el hombre y, sin darnos cuenta, es la que más utiliza cualquiera de nosotros en su vida cotidiana: a diario identificamos a personas por los rasgos de su cara o por su voz. Obviamente aquí el agente reconocedor es una persona, pero en el modelo aplicable a redes o sistemas el agente ha de ser un dispositivo que, basándose en características del sujeto a identificar, le permita o deniegue acceso a un determinado recurso.

Aunque la autenticación de usuarios mediante métodos biométricos es posible utilizando cualquier característica única y medible del individuo (esto incluye desde la forma de teclear ante un ordenador hasta los patrones de ciertas venas, pasando por el olor corporal), tradicionalmente ha estado basada en cinco grandes grupos que van a ser desarrollados más adelante. La siguiente es una tabla comparativa de las características generales de los distintos métodos.

Tabla Comparativa de métodos biométricos

	Voz	Escritura Firma	Huellas Dactilares	Ojo Retina	Ojo Iris	Geometría de Mano
Fiabilidad	alta	alta	alta	muy alta	muy alta	alta
Facilidad de Uso	alta	alta	alta	baja	media	alta
Prevención de Ataques	media	media	alta	muy alta	muy alta	alta
Aceptación	alta	muy alta	media	media	media	alta
Estabilidad	media	media	alta	alta	alta	media
Identificación	no	si	si	si	si	
Autenticación	si	si	si	si	si	si
Interferencias	ruidos, resfriados	firmas fáciles	suciedad, heridas	irritación	gafas	artritis, reumatismo

Generalmente, los dispositivos utilizados para la autenticación biométrica están compuestos de tres partes principales:

- un mecanismo automático que captura una imagen o sonido de la característica a analizar.
- una entidad que procesa y extrae ciertas características de la muestra.
- un proceso que realiza el almacenamiento o la comparación de tales características con las guardadas en una base de datos para decidir si el usuario es válido o no

Es en esta decisión donde principalmente entran en juego las dos características básicas de la fiabilidad de todo sistema de autenticación y en especial de los sistemas biométricos: las *tasas de falso rechazo* y de *falsa aceptación*.

Tasa de falso rechazo (*False Rejection Rate, FRR*): probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente.

Tasa de falsa aceptación (*False Acceptance Rate, FAR*): probabilidad de que el sistema autentique correctamente a un usuario ilegítimo.

Evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada genera un grave problema de seguridad: estamos proporcionando acceso a un recurso a personal no autorizado a acceder a él.

VERIFICACIÓN DE VOZ

En los sistemas de reconocimiento de voz no se intenta, como mucha gente piensa, reconocer lo que el usuario dice, sino identificar una serie de sonidos y sus características para decidir si el usuario es quien dice ser. Para autenticar a un usuario utilizando un reconocedor de voz se debe disponer de ciertas condiciones para el correcto registro de los datos, como ausencia de ruidos, reverberaciones o ecos; idealmente, estas condiciones han de ser las mismas siempre que se necesite la autenticación.

Cuando un usuario desea acceder al sistema pronunciará unas frases en las cuales reside gran parte de la seguridad del protocolo; en algunos modelos, los denominados de *texto dependiente*, el sistema tiene almacenadas un conjunto muy limitado de frases que es capaz de reconocer: por ejemplo, imaginemos que el usuario se limita a pronunciar su nombre, de forma que el reconocedor lo entienda y lo autentique.

Como veremos a continuación, estos modelos proporcionan poca seguridad en comparación con los de *texto independiente*, donde el sistema va "*proponiendo*" a la persona la pronunciación de ciertas palabras extraídas de un conjunto bastante grande. De cualquier forma, sea cual sea el modelo, lo habitual es que las frases o palabras sean características para maximizar la cantidad de datos que se pueden analizar (por ejemplo, frases con una cierta entonación, pronunciación de los diptongos, palabras con muchas vocales, etc). Conforme va hablando el usuario, el sistema registra toda la información que le es útil; cuando termina la frase, ya ha de estar en disposición de facilitar o denegar el acceso, en función de la información analizada y contrastada con la de la base de datos.

El principal problema del reconocimiento de voz es la inmunidad frente a *replay attacks*, un modelo de ataques de simulación en los que un atacante reproduce (por ejemplo, por medio de un magnetófono) las frases o palabras que el usuario legítimo pronuncia para acceder al sistema. Este problema es especialmente grave en los sistemas que se basan en textos preestablecidos. Por otro lado, en modelos de texto independiente, más interactivos, este ataque no es tan sencillo porque la autenticación se produce realmente por una especie de desafío-respuesta entre el usuario y la máquina. Otro grave problema de los sistemas basados en reconocimiento de voz es el tiempo que el usuario emplea hablando delante del analizador, al que se añade el que éste necesita para extraer la información y contrastarla con la de su base de datos; aunque actualmente en la mayoría de sistemas basta con una sola frase, es habitual que el usuario se vea obligado a repetirla porque el sistema le deniega el acceso (una simple congestión hace variar el tono de voz, aunque sea levemente, y el sistema no es capaz de decidir si el acceso ha de ser autorizado o no; incluso el estado anímico de una persona varía su timbre).

A su favor, el reconocimiento de voz posee la cualidad de una excelente acogida entre los usuarios, siempre y cuando su funcionamiento sea correcto y éstos no se vean obligados a repetir lo mismo varias veces, o se les niegue un acceso porque no se les reconoce correctamente.

VERIFICACIÓN DE ESCRITURA

Aunque la escritura -generalmente la firma- no es una característica estrictamente biométrica, se suele agrupar dentro de esta categoría; de la misma forma que sucedía en la verificación de la voz, el objetivo aquí no es interpretar o entender lo que el usuario escribe, sino autenticarlo basándose en ciertos rasgos característicos.

Existe una diferencia fundamental entre el uso de las firmas que hacemos en nuestra vida cotidiana y los sistemas biométricos; en los segundos se utiliza además la forma de firmar, las características dinámicas de la firma (por eso se les suele denominar *Dynamic Signature Verification*, DSV): el tiempo utilizado, las veces que se separa el bolígrafo del papel, el ángulo con que se realiza cada trazo, etc.

Para utilizar un sistema de autenticación basado en firmas se solicita en primer lugar a los futuros usuarios un número determinado de firmas ejemplo, de las cuales el sistema extrae y almacena ciertas características; esta etapa se denomina de *aprendizaje*, y el principal obstáculo a su correcta ejecución son los usuarios que no suelen firmar uniformemente. Contra este problema la única solución es relajar las restricciones del sistema a la hora de *aprender* firmas, con lo que se decrementa su seguridad.

Una vez que el sistema conoce las firmas de sus usuarios, cuando estos desean acceder a él se les solicita tal firma, con un número limitado de intentos. La firma introducida es capturada por un lápiz óptico o por una lectora sensible (o por ambos), y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el verificador es capaz de distinguir como auténtica.

VERIFICACIÓN DE HUELLAS

Típicamente la huella dactilar de un individuo ha sido un patrón bastante bueno para determinar su identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona. Por tanto, parece obvio que las huellas se convertirían antes o después en un modelo de autenticación biométrico: desde el siglo pasado hasta nuestros días se vienen realizando con éxito clasificaciones sistemáticas de huellas dactilares en entornos policiales, y el uso de estos patrones fue uno de los primeros en establecerse como modelo de autenticación biométrica.

Cuando un usuario desea autenticarse ante el sistema sitúa su dedo en un lector, este toma una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos, y es de esta imagen normalizada de la que el sistema extrae las minucias (ciertos arcos, bucles o remolinos de la huella) que va a comparar contra las que tiene en su base de datos; es importante resaltar que lo que el sistema es capaz de analizar no es la huella en sí sino que son estas minucias, concretamente la posición relativa de cada una de ellas. Está demostrado que dos dedos nunca pueden poseer más de ocho minucias comunes, y cada uno tiene al menos 30 o 40 de éstas. Si la comparación de las posiciones relativas de las minucias leídas con las almacenadas en la base de datos es correcta, se permite el acceso al usuario, denegándosele obviamente en caso contrario.

Los sistemas basados en reconocimiento de huellas son relativamente baratos comparados con otros sistemas biométricos; sin embargo, tienen en su contra la incapacidad temporal de autenticar usuarios que se hayan podido herir en el dedo a reconocer. Otros elementos como la suciedad, la presión ejercida sobre el lector o el estado de la piel pueden ocasionar lecturas erróneas.

VERIFICACIÓN DE PATRONES OCULARES

Los modelos de autenticación biométrica basados en patrones oculares se dividen en dos tecnologías diferentes: los que analizan patrones de retinas, y los que analizan el iris. Estos métodos se suelen considerar los más efectivos: para una población de 200 millones de usuarios la probabilidad de

coincidencia es casi 0, y además una vez muerto el individuo los tejidos oculares degeneran rápidamente, lo que dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver.

La principal desventaja de los métodos basados en el análisis de patrones oculares es su escasa aceptación; el hecho de mirar a través de un binocular (o monocular), necesario en ambos modelos, no es cómodo para los usuarios, ni aceptable para muchos de ellos: por un lado, los usuarios *no se fían* de un haz de rayos analizando sus ojos, y por otro, un examen de este órgano puede revelar enfermedades o características médicas que a muchas personas les puede interesar mantener en secreto, como el consumo de alcohol o de ciertas drogas. Aunque los fabricantes de dispositivos lectores aseguran que sólo se analiza el ojo para obtener patrones relacionados con la autenticación, y en ningún caso se viola la privacidad de los usuarios, mucha gente no cree esta postura oficial. Por si esto fuera poco, se trata de sistemas demasiado caros para la mayoría de organizaciones, y el proceso de autenticación no es todo lo rápido que debiera en poblaciones de usuarios elevadas. De esta forma, su uso se ve reducido casi sólo a la identificación en sistemas de alta seguridad, como el control de acceso a instalaciones militares.

- Retina: la forma de los vasos sanguíneos de la retina humana es un elemento característico en cada individuo, por lo que numerosos estudios en el campo de la autenticación de usuarios se basan en su reconocimiento. En los sistemas de autenticación basados en patrones retinales el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia interocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. En ese momento se escudriña la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

- Iris: el iris es el anillo visible de color que rodea a la pupila. Es una estructura muscular que controla la cantidad de luz que ingresa a los ojos, con detalles intrincados que pueden ser medidos, tal como las estrías, incisiones, y surcos. El iris no debe ser confundido con la retina la cual recubre por dentro la parte de atrás de los ojos. No existen dos ojos iguales, no hay incluso correlación entre los patrones de dos personas gemelas idénticas, o entre el ojo izquierdo y el derecho de una misma persona. La cantidad de información que puede ser extraída de un único iris es mayor que la que puede encontrarse en las huellas dactilares, y la exactitud mayor que la de un ADN.

Una cámara de reconocimiento de iris toma una fotografía en blanco y negro de entre 5 y 24 pulgadas, dependiendo del tipo de cámara. Las cámaras, certificadas por los estándares internacionales de iluminación segura, utiliza un método no invasivo de rayos cercanos al infrarrojo (similar al utilizado en los controles remotos) que es escasamente visible y muy seguro. La imagen del ojo es primeramente procesada por un programa que localiza los bordes interiores y exteriores del iris, y el contorno de los párpados con el objeto de extraer solamente la porción que corresponde al iris. Pestañas y reflejos que pueden estar cubriendo partes del iris son también detectados y eliminados. Luego, un sofisticado programa matemático codifica los patrones del ojo en un proceso que se denomina *Demodulación*. Este proceso crea un código para la secuencia de textura en el iris similar al código de secuencia utilizado para el ADN. El proceso de Demodulación realiza una muy compacta pero completa descripción de los patrones del iris. Esta secuencia se denomina IrisCode®, y captura las características únicas de un iris de una manera robusta que permite una comparación muy rápida y fácil contra una gran base de datos de patrones. En sólo algunos segundos, incluso con una base de datos de millones de registros, el IrisCode® generado desde la imagen en vivo será comparado con los previamente almacenados para ver si coincide con alguno de ellos. El umbral de decisión se ajusta automáticamente al tamaño de la base de datos de búsqueda para asegurar que no ocurran falsos positivos.

VERIFICACIÓN DE LA GEOMETRÍA DE LA MANO

Los sistemas de autenticación basados en el análisis de la geometría de la mano son sin duda los más rápidos dentro de los biométricos: con una probabilidad de error aceptable en la mayoría de ocasiones,

en aproximadamente un segundo son capaces de determinar si una persona es quien dice ser.

Cuando un usuario necesita ser autenticado sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura. Una vez la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos -anchura, longitud, área y determinadas distancias-. Transformando estos datos en un modelo matemático que se contrasta contra una base de patrones, el sistema es capaz de permitir o denegar acceso a cada usuario.

Quizás uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es que éstos son capaces de aprender: a la vez que autentican a un usuario, actualizan su base de datos con los cambios que se puedan producir en la muestra -un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida-; de esta forma son capaces de identificar correctamente a un usuario cuya muestra se tomó hace años, pero que ha ido accediendo al sistema con regularidad. Este hecho, junto a su rapidez y su buena aceptación entre los usuarios, hace que los autenticadores basados en la geometría de la mano sean los más extendidos dentro de los biométricos a pesar de que su tasa de falsa aceptación se podría considerar inaceptable en algunas situaciones: no es normal, pero sí posible, que dos personas tengan la mano lo suficientemente parecida como para que el sistema las confunda. Para minimizar este problema se recurre a la identificación basada en la geometría de uno o dos dedos, que además puede usar dispositivos lectores más baratos y proporciona incluso más rapidez.

A PRUEBA DE ENGAÑOS

Por último, quizás es conveniente desmentir uno de los grandes mitos que existen sobre este tipo de sistemas de autenticación: la vulnerabilidad a ataques de simulación. Suele verse en películas o leerse en libros que en algunos casos se consigue "engañar" a autenticadores biométricos para conseguir acceso a determinadas instalaciones o sistemas: se simula la parte del cuerpo a analizar mediante un modelo o incluso utilizando órganos amputados a un cadáver o al propio usuario vivo. Evidentemente, esto sólo sucede en la ficción: hoy en día cualquier sistema biométrico - con excepción, quizás, de algunos modelos basados en voz - son altamente inmunes a estos ataques. Los analizadores de retina, de iris, de huellas o de la geometría de la mano son capaces, aparte de decidir si el miembro pertenece a un usuario legítimo, de determinar si éste está vivo o se trata de un cadáver.

Fuentes: Red española de I + D (<http://www.rediris.es/>)

Eyedentify.com (<http://www.eyedentify.com/>)

Iridian® Technologies (<http://www.iriscan.com>)