Sistemas De Autenticación Biométricos

Seguridad Y Protección De La Información

Ricardo Llopis Nebot

Índice General

1. Introducción.

Desde el principio de los tiempos, la búsqueda de un medio de identificación no ambiguo ha sido uno de los objetivos de la humanidad.

En la vida cotidiana como en el mundo tecnológico, la importancia de la privacidad y la seguridad de los datos obligan a establecer medidas de identificación y autentificación con el fin de asegurar que ninguna otra persona accede a datos ajenos o servicios privados.

En la llamada era de la tecnología, cada vez mas actividades que hasta entonces se realizaban en papel han pasado a realizarse mediante aplicaciones informáticas, como el comercio electrónico, o el acceso a datos bancarios, operaciones en las que se necesita garantizar la confidencialidad y seguridad.

Hasta ahora podíamos observar continuamente métodos sencillos para conseguir resolver estos problemas como, por ejemplo, el uso de las tarjetas plásticas de identificación, en las que incluso se solía incorporar una foto o una firma a modo de identificación entre personas. En el mundo de la tecnología de la información este planteamiento debe ser modificado ya que no existe una persona que te identifique. Es por ello que se requieren otras técnicas que resuelvan dicho problema, como el uso de passwords o diferentes protocolos de seguridad que existen.

Dichas técnicas se pueden agrupar en:

- Las de uso de información confidencial.
- Las de medida de características biológicas.

En la primera opción, el usuario debe dar su beneplácito y ayudar para que la técnica funcione, pero su desarrollo en diferentes ámbitos puede llegar a ser muy complejo para él.

El uso de la segunda opción, mediante la utilización de tecnología suficiente, puede resolver fácilmente estos problemas, siempre que se utilice del modo correcto.

Actualmente el uso de la memorización de información esta muy extendido en casi todas las aplicaciones que requieren seguridad al acceder a datos, servicios, u otros productos. Algunos ejemplos son:

- Teléfonos móviles: Uso del PIN.
- Cajeros automáticos: Memorización de una clave personal.
- Sistemas Multiusuario: Memorización de un login y un password.

Pero la memorización de información puede llegar a ser muy molesta cuando se usan varias de estas aplicaciones al mismo tiempo, o, por otro lado, cuando una de ellas se utiliza con poca frecuencia. En estos casos resultaría interesante la utilización de otros métodos de identificación que facilitaran al usuario su utilización, y es ahí donde entran en juego los métodos biométricos.

Podemos definir métodos biométricos como técnicas automáticas de reconocimiento de personas mediante el análisis de características físicas o de comportamiento que definen al usuario por ser exclusivas del mismo, como pueden ser, las huellas dactilares, el timbre de voz, la firma... Características que identifican al usuario sin ningún tipo de dudas y que son imposibles de falsificar.

A pesar de la enorme ventaja que estos métodos ofrecen, también presentan inconvenientes que deben tenerse en cuenta:

- La implementación de éstas técnicas suele tener un coste muy alto. Para resolverlo se debe mejorar las prestaciones de los terminales que se utilicen, ya que son los encargados de procesar de modo adecuado lo datos recibidos. Esto requiere una fuerte inversión que no todas las empresas están dispuestas a llevar a cabo.

- Las técnicas no son absolutamente seguras, pudiendo producirse ciertos errores. Este problema se aborda a través de la investigación y mejora de las técnicas actuales, lo cual permitiría mejorar el nivel de certeza.

Cuando estos condicionantes se satisfagan completamente, el uso de la memorización de información pasará a un segundo plano.

2. Métodos biométricos.

2.1 Aceptación del Usuario.

El problema básico en la implantación de los métodos biométricos es la aceptación del usuario. Varias teorías al respecto están hoy enfrentadas. Parte de la sociedad rechaza de entrada la idea de identificarse mediante sus huellas o algún sistema que controle su anatomía porque creen que su intimidad es invadida, sienten que se les está espiando o controlando de algún modo, o simplemente creen que se les está tratando como criminales. Por otro lado, como vino a demostrar un estudio de la Universidad de Columbia, cada vez hay mas gente (el 83%) que confía en la comodidad de no llevar cada vez más tarjetas diferentes, ni en tener que recordar diversos códigos de seguridad para cada una de ellas.

Lo cierto, básicamente, es que si nos centramos en el aspecto de la comodidad, más de una vez nos puede ocurrir que nos dejemos olvidada una tarjeta en casa, pero raro es que nos dejemos la mano o el ojo.

Otro punto de vista para la no aceptación de ciertos sectores es el de la salud. Los problemas médicos que pueden producir las técnicas de medida, tanto por un contagio como por una lesión, también influye sobre la aceptación de los métodos.

En todos estos aspectos se requiere una mejora del proceso de medida y una fase de información al usuario que elimine cualquier sombra de duda que pueda tener ya que todo proceso de medida siempre debe incluir un consentimiento expreso por parte del usuario.

2.2 Seguridad de la Medida.

Por definición, los procesos de medida no son fiables completamente, sino que presentan cierta incertidumbre inherente que debe ser considerada. Dicha incertidumbre resulta proporcional a la complejidad del propio proceso de medida, que suele ser bastante alta en la medida de características humanas.

La probabilidad de que una medida se ajuste a su valor real se representa mediante una campana de Gauss. Para resolver esta problemática, el valor de referencia se obtiene como la media de una serie de mediciones de la característica. Posteriormente, la identificación se produce mediante la comparación de una medida con el valor de referencia.

Debido a la incertidumbre de la medida, la comparación debe admitir como correctas medidas con un cierto nivel de error. Es por ello que se debe definir un umbral ,que varía con la aplicación y con la técnica de identificación utilizada.

2.3 Características y clasificación.

Una técnica biométrica se fundamenta en una característica biológica que debe cumplir las siguientes premisas.

- Identifica de modo único a una persona.
- Su falsificación resulta imposible.
- El envejecimiento de la persona no modifica su valor.
- Su evaluación es viable, tanto por el método utilizado como en el coste computacional y monetario.
- El método y la característica seleccionados serán adecuados para sus usuarios futuros.

Las características puede agruparse en:

- Características Fisiológicas: Incluyen las relacionadas con el cuerpo humano y las que no se refieren a un patrón de comportamiento consciente.

- Características de Comportamiento: Se refieren a las que se refieren al comportamiento consciente, y que por tanto pueden variar dentro de unos límites.

2.4 Tipos de sistemas biométricos.

2.4.1 Sistemas fisiológicos.

La elección de una característica fisiológica es compleja, ya que sus valores no deben variar a lo largo de la vida del usuario.

Ejemplos de características cuyo valor es fijo son las huellas digitales o los vasos sanguíneos de la retinas. En cambio, la imagen facial de la cara puede sufrir varios cambios, entre los cuales aparecen el volumen del cabello y su peinado, así como la existencia de bigote y barba.

2.4.1.1 Características Faciales.

Externamente la imagen de la cara de una persona puede variar sobremanera, pero aún así puede ser utilizado en este contexto. Se puede demostrar que el procesamiento de la fotografía bien iluminada de una persona puede generar una serie de parámetros que la identifiquen de modo único. En la actualidad, el desarrollo de las técnicas asociadas no son muy seguras, por lo que su uso no está muy extendido, aunque lo estarán en el futuro próximo.

El procesamiento requiere la utilización de ordenadores de altas prestaciones, así como técnicas específicas como lógica difusa o redes neuronales.

Las técnicas actuales comienzan realizando un análisis en 3 dimensiones de la cara completa, que previamente el usuario habrá apoyado en el lugar adecuado enfrente de una pantalla que oculta multitud de escáneres. Posteriormente el sistema extrae cientos de pequeñas imágenes del usuario, a modo de celdillas, cada una con varias posiciones y con luz diferente, guardando dicha información. La velocidad de este proceso suele ser bastante rápida, de un segundo aproximadamente.

Para salvar el problema antes mencionado de los posibles cambios corporales, estas técnicas van actualizando valores a medida que el sujeto sufre alguno de dichos cambios, como pudieran ser, heridas, barba...

2.4.1.2 Características de la Retina.

Los modelos de autenticación biométrica basados en patrones oculares se suelen considerar los más efectivos: para una población de 200 millones de potenciales 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 su ojo, 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 (aparte del hecho de que la información es procesada vía *software*, lo que facilita introducir modificaciones sobre lo que nos han vendido para que un lector realice otras tareas de forma enmascarada).

Otro inconveniente es la utilización de lentes de contacto, ya que modifica los valores de la medida obtenida.

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.

La vasculatura de la retina (forma de los vasos sanguíneos) es un elemento característico de cada individuo, por lo que numerosos estudios en el campo de la autenticación de usuarios se basan en el reconocimiento de esta vasculatura.

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 escanea 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.

2.4.1.3 Utilización del Iris.

El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es igual que la vasculatura retinal una estructura única por individuo que forma un sistema muy complejo – de hasta 266 grados de libertad – , inalterable durante toda la vida de la persona. El uso por parte de un atacante de órganos replicados o simulados para conseguir una falsa aceptación es casi imposible con análisis infrarrojo, capaz de detectar con una alta probabilidad si el iris es natural o no.

La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retinales. Desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios. Para ello, se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado; esta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos suficiente para los propósitos de autenticación.

Esa muestra, denominada *iriscode* es comparada con otra tomada con anterioridad y almacenada en la base de datos del sistema, de forma que si ambas coinciden el usuario se considera autenticado con éxito.

La probabilidad de una falsa aceptación es la menor de todos los modelos biométricos.

2.4.1.4 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, determinadas distancias. . .) en un formato de tres dimensiones. 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 autentificadores 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 suficiente-
mente 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.

2.4.1.5 Huellas Digitales.

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 área determinada (área de lectura, no se necesita en ningún momento una impresión en tinta). Aquí se 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 (en comparación con otros biométricos, como los basados en patrones retinales). Sin embargo, tienen en su contra la incapacidad temporal de autenticar usuarios que se hayan podido herir en el dedo a reconocer (un pequeño corte o una quemadura que afecte a varias minucias pueden hacer inútil al sistema). También elementos como la suciedad del dedo, la presión ejercida sobre el lector o el estado de la piel pueden ocasionar lecturas erróneas.

Otro factor a tener muy en cuenta contra estos sistemas es psicológico, no técnico: hemos dicho en la introducción que un sistema de autenticación de usuarios ha de ser aceptable por los mismos, y generalmente el reconocimiento de huellas se asocia a los criminales, por lo que muchos usuarios recelan del reconocedor y de su uso.

2.4.2 Sistemas de comportamiento.

Una de las propiedades básicas de estas características es su evolución a lo largo de la vida de una persona. Dicha evolución debe ser considerada en el desarrollo de la técnica, de modo que se pueda identificar a una persona aún cuando se hayan producido ciertos cambios. Es por ello, que habitualmente se desarrollan procedimientos adaptativos que detectan y corrigen los cambios producidos.

2.4.2.1 Ritmo de Escritura.

El modo en el que cada persona escribe sobre un teclado es diferente. Estas técnicas se fundamentan en el análisis de todas las peculiaridades que muestra el usuario al teclear un patrón, que puede ser una palabra o una frase. Peculiaridades como son: las pausas producidas cuando se presionan diferentes teclas, el tiempo de presión de cada una, la misma presión, la velocidad de escritura, el nivel de error...

Como puede apreciarse, es una técnica muy simple que ni siquiera requiere hardware específico, hasta el punto de que, si donde queremos acceder es un sistema informático, no hay que realizar ningun tipo de modificación del mismo.

2.4.2.2 Características de la voz.

De igual modo que las características faciales permiten identificar una persona, también es posible utilizar su voz. La voz humana es simplemente un sonido, por lo que puede ser tratada como una señal más, sobre la cual es posible aplicar un análisis de Fourier.

Como resultado de este análisis se obtiene el espectro característico de una persona que puede ser almacenado para una posterior identificación. Este análisis requiere una potencia de cálculo bastante importante, así como herramientas adicionales como la lógica difusa y las redes neuronales.

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 autentificar 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 autentificación.

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 autentifique. 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. . .).

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: volviendo al ejemplo anterior, el del nombre de cada usuario, un atacante no tendría más que grabar a una persona que pronuncia su nombre ante el autentificador y luego reproducir ese sonido para conseguir el acceso. Casi la única solución consiste en utilizar otro sistema de autenticación junto al reconocimiento de voz. Por contra, 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, de forma que la cantidad de texto grabado habría de ser mucho mayor – y la velocidad para localizar la parte del texto que el sistema propone habría de ser elevada –.

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. A pesar de sus problemas técnicos, será una de las más utilizadas en el futuro.

2.4.2.3 Firma Dinámica.

Aunque la escritura (generalmente la firma) no es una característica estrictamente biométrica, como hemos comentado en la introducción 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 en el lector, sino autenticarlo basándose en ciertos rasgos tanto de la firma como de su rúbrica.

La verificación en base a firmas es algo que todos utilizamos y aceptamos día a día en documentos o cheques; no obstante, existe una diferencia fundamental entre el uso de las firmas que hacemos en nuestra vida cotidiana y los sistemas biométricos; mientras que habitualmente la verificación de la firma consiste en un simple análisis visual sobre una impresión en papel, estática, en los sistemas automáticos no es posible autenticar usuarios en base a la representación de los trazos de su firma.

En los modelos biométricos se utiliza además la forma de firmar, las características dinámicas (por eso se les suele denominar *Dynamic Signature Verification*, DSV): el tiempo utilizado para rubricar, las veces que se separa el bolígrafo del papel, el ángulo con que se realiza cada trazo. . .

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 (aparte de una concienciación de tales usuarios) 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 (generalmente más que los sistemas que autentican mediante contraseñas, ya que la firma puede variar en un individuo por múltiples factores). 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.

2.5 Tabla general.

	Iris	**Retina**	**Huellas**	**Mano**	**Firma**	**Voz**
Fiabilidad	Muy Alta	Muy Alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy Alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy Alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación / autentificación	Ambas	Ambas	Ambas	Autentificación	Ambas	Autentificación
Estándares	---	---	ANSI/NIST, Fbi	---	---	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas...	Artritis, reumatismo...	Firmas fáciles o cambiantes	Ruido, resfriados...
Uso en	Instalaciones nucleares, servicios médicos, centros penitenciarios	Instalaciones nucleares, servicios médicos, centros penitenciarios	Policía, industrial	General	Industrial	Accesos remotos en bancos o bases de datos
Precio por nodo en 1997 (Dolares)	5,000	5,000	1,200	2,100	1,000	1,200

3. Aplicaciones.

El uso de contraseñas de seguridad está fuertemente ligado al acceso a datos, servicios personales, o sistemas informáticos en todo el mundo, por ello, es aconsejable que el manejo de estas contraseñas sea efectivo y seguro. El avance que multitud de universidades y empresas están consiguiendo en la investigación y el desarrollo de nuevas técnicas o en el perfeccionamiento de las existentes, ha hecho que el mundo se plantee la gran utilidad que los métodos biométricos van a representar en un futuro no muy lejano.

Paulatinamente nuevos usos se están encontrando en la aplicación de estas técnicas de autentificación, que, con el paso del tiempo, todavía se ampliarán más, dado que el éxito que están teniendo y a medida que se vaya confiando aún mas en ellos.

Algunas aplicaciones de biométricos actuales las encontramos en:

- **La seguridad financiera:** Cajeros automáticos, transferencias electrónicas, el reciente comercio electrónico...
- **El control de acceso de personas:** Aeropuertos, zonas de seguridad de empresas, zonas de defensa gubernamentales...
- **El control demográfico:** Inmigración, pasaportes, visados...
- **El sistema de votaciones:** Maquinas automáticas de recogida de votos electorales...
- **Las telecomunicaciones:** Telefonía móvil, control de acceso a sistemas de comunicaciones...
- **La Medicina:** Historiales clínicos, registro de medicaciones a pacientes con enfermedades duraderas o terminales...

Como curiosidad, en España, más concretamente en la EXPO de Sevilla se implementó un sistema de identificación basado en huellas digitales, que se utilizó en las tarjetas de los empleados y en los pases de visita semestrales. La idea de los pases semestrales fue impedir el bloqueo de la venta de pases diarios, lo que permitiría un mayor número de visitantes. Resultaba fundamental que estos pases fueran utilizados únicamente por su propietario, por lo que se introdujo este sistema de identificación. El problema fue el coste de la identificación, cuyo valor debía ser 8 segundos siendo su valor inicial de 30 segundos llegando hasta 15.

En otra ocasión, en Barcelona '92 se utilizó un sistema basado en la firma dinámica para el acceso a la torre de control del tráfico aéreo de su aeropuerto. El proceso de identificación se basaba en la comparación de la firma introducida por el usuario con el valor medio de los parámetros de tres firmas almacenadas en la tarjeta. Tras una identificación correcta, se sustituía la firma más antigua por la nueva, con el objeto de tener una batería de firmas actualizada. El número de intentos del usuarios se limitaba para impedir un proceso de prueba y error.

4. Bibliografía y enlaces.

[1] Charles P. Pfleeger. ***Security In Computing***. Englewood Cliffs, 1989.

[2] Deborah Russell & G.T. Gangemi. ***Computer Security Basics***. Sebastopol, Clif. O'Reilly & Associates, 1991.

[3] Simson Garfinkel & Gene Spafford. ***Practical Unix & Internet Security***. O'Reilly & Associates, 1996.

[4] Antonio Villalón Huerta. ***Seguridad En Unix Y Redes***. 2000

[5] José Ignacio Aliaga. ***Nuevas Tecnologías Aplicadas A La Gestión***. 2001

[5] Página web de **Avanti**
http://homepage.ntlworld.com/avanti

[6] Página web de **Biometric Consortium**.
http://www.biometrics.org

[7] Página web de **AcSys Biometrics**.
http://www.acsysbiometrics.com

[8] Página web de **Biometric Domain**.
http://www.biometricdomain.com